Cyber Kill Chain

Jay Chen, Ruben Ocana,
Senna Alsadam, Andrew Shi

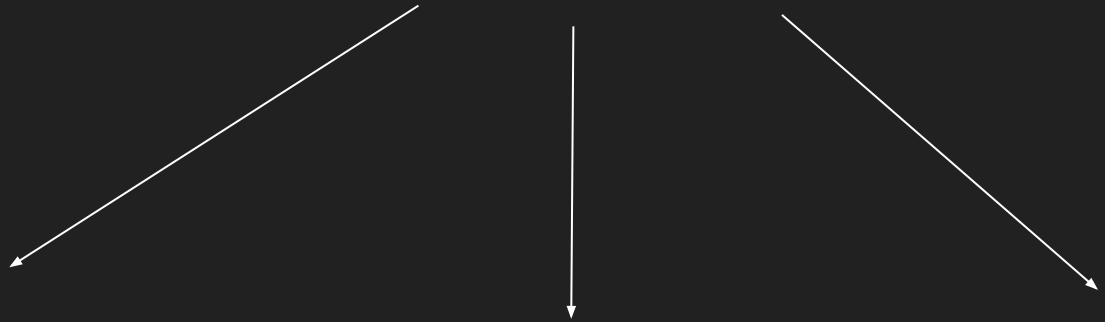
Modern Security Threats

- New class of threat actors called Advanced Persistent Threat (APT)
- Data compromised for economic or military advancement
- Conventional response methods don’t work
  - Response occurs *after* point of compromise

What is the “Kill Chain”

- Process that targets and engages attacker
- Intelligence driven threat focused approach separated into phases of an intrusion
- Provides a possibility of anticipating and mitigating future intrusions

Indicators



Atomic

-cannot be broken down into smaller parts
-retain meaning
-ex) IP addresses, email addresses, vulnerability identifiers

Computed

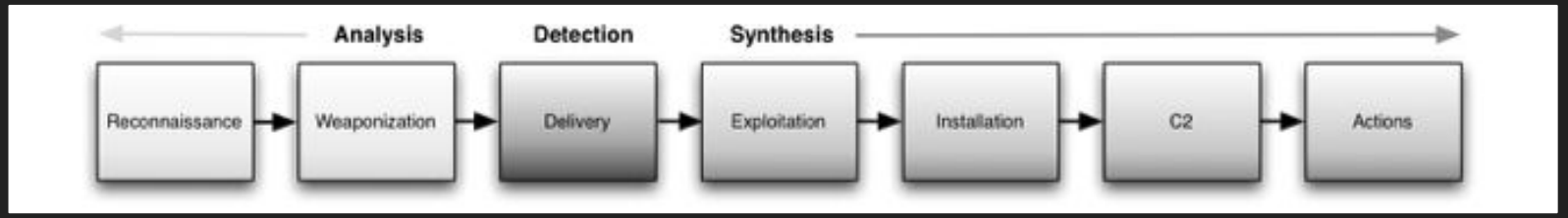
-derived from data of incident
-ex) hash values, regular expressions

Behavioral

-mix of computed and atomic

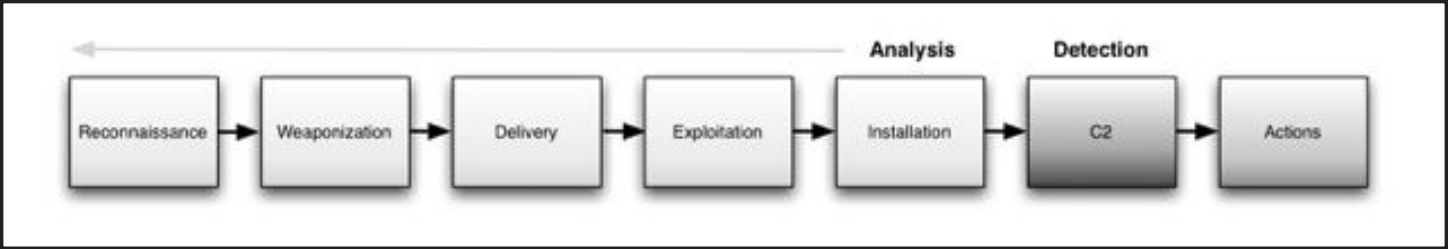
Earlier Phase Detection

- The intrusion is detected early on
- This allows predictions to be made about later phases
- Defenders want to analyze what happened so they are prepared for future intrusions



Late Phase Detection

- The intrusion is detected later
- Action taken in earlier phase was bypassed
- Defenders are too late
- Defenders must analyze what went wrong in order to prevent it from happening in future attacks

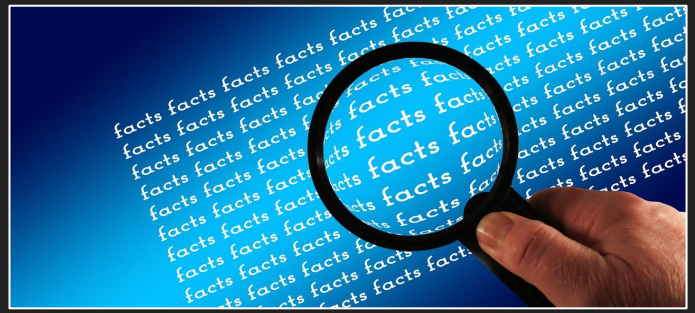


Cyber Kill Chain

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

Reconnaissance

- Reconnaissance consists of extensive research, identification, and selection of targets
- Done through browsing through the internet for information, looking through, but not limited to:
  - Mailing lists for email addresses
  - Social relationships
  - Information on specific technologies



Weaponization

- During weaponization, the goal is for the user to modify something a user will use or open in a way which would favor the attacker
- An example would be to compromise a Microsoft Office document to have a trojan on it

Delivery

- Delivery is defined as the transmission of the weapon to the targeted environment
- There are 3 delivery vectors that are most prevalent by APTs:

Delivery

- Delivery is defined as the transmission of the weapon to the targeted environment
- There are 3 delivery vectors that are most prevalent by APTs:
  - Email attachments
  - Websites
  - USB Removable Media

Exploitation

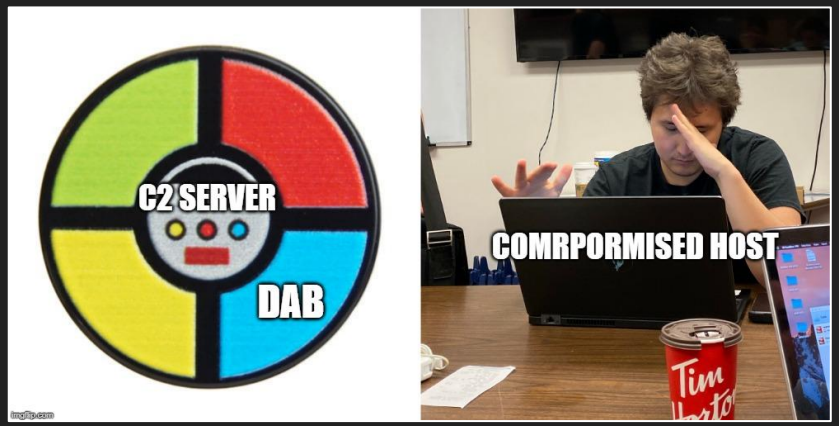
- Exploitation is the what happens after the weapon is delivered, it is the trigger phase
- Targets applications or operating systems vulnerabilities
- Sometimes this phase is meant to just exploit the users themselves or leverage a feature that would allow for auto-executing codes

Installation

- Once the weapon has intruded a system, they can begin installing remote access trojans or set up a back door
- This allows the adversary to maintain persistence inside the environment

Command and Control (C2)

- Command and Control is when intruders have their “hands on the keyboard” access inside the target environment
- Compromised hosts must beacon outbound to an Internet Controller server to establish a C2 channel



Actions on Objectives

- After successfully going through all previous 6 steps, an intruder can now take actions on their objectives
- Generally the objective is data exfiltration which could involve collecting, encrypting, and extracting information from the victim environment
- Potential objectives can include violations of data integrity or availability, or only using the victim environment as a hop point to compromise additional systems over time

Course of Action Matrix

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	“chroot” jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Cyber Kill Chain Case Study

Introduction to the case study

- Lockheed Martin Computer Incident Response Team (LM-CIRT) observed an attempt in March 2009
- LM-CIRT was able to mitigate the intrusions by leveraging the intrusion kill chain and attack indicators

Reconnaissance

- The adversary analyzed potential targets in an organization and created a recipient list
- The attacker also analyze potential events that will be of interest to the targeted individuals
- Presuming the identity of AIAA representative
- Sent a Targeted Malicious Email containing a benign pdf file

Weaponization

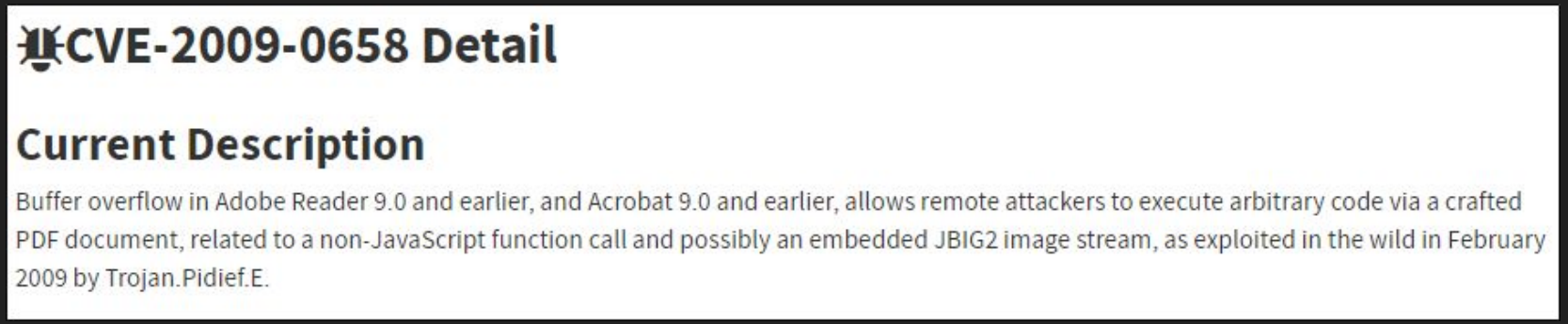
- TME attachment contained a weaponized PDF
- The weaponized PDF file contained two files
  - Benign PDF
  - Portable Execution (PE) backdoor installer
- The two files were encrypted using a trivial algorithm with an 8-bit key stored in the exploit shellcode

Delivery

- The delivery of the e-mail was from a yahoo mail server
- Adversary pretended to be an AIAA representative
- The email sent to five individuals contained the malicious pdf attachment

Exploitation

- If a user opens the PDF, shellcode exploiting CVE-2009-0658 will decrypt the installation binary
- The vulnerability was documented on February 19, 2009 and was patched on March 10, 2009
- The intrusion attempt took place on March 3, 2009



CVE-2009-0658 Detail

Current Description

Buffer overflow in Adobe Reader 9.0 and earlier, and Acrobat 9.0 and earlier, allows remote attackers to execute arbitrary code via a crafted PDF document, related to a non-JavaScript function call and possibly an embedded JBIG2 image stream, as exploited in the wild in February 2009 by Trojan.Pidief.E.

Installation

- By opening the PDF, the remote shellcode decrypted the encrypted PDF contents
- The shellcode will place a file called “fssm32.exe” on the user’s computer and start it
- The benign AIAA conference PDF will be displayed to the user
- “fssm32.exe” will extract the backdoor components embedded within itself, saving EXE and HLP file to the user’s computer

C2

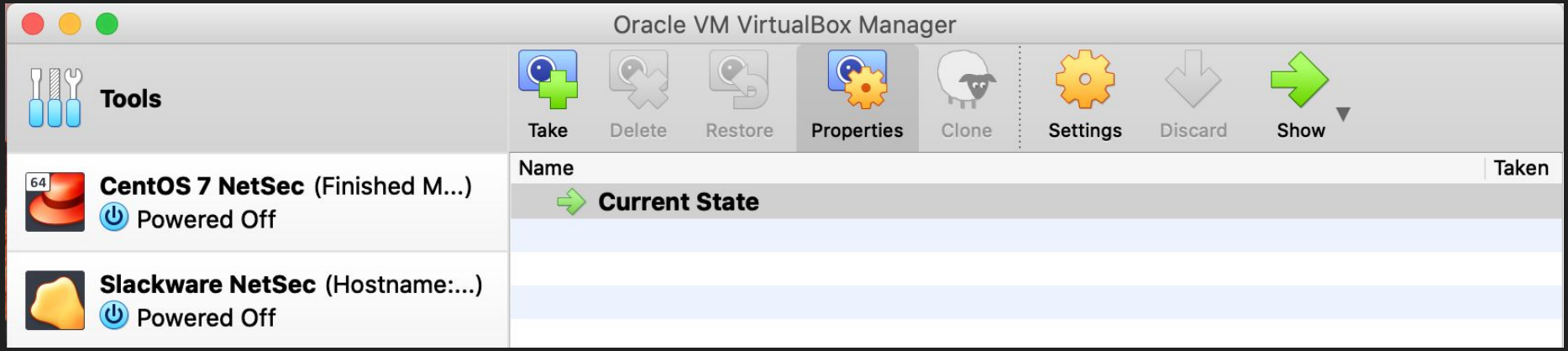
- If the installation phase is successful, the backdoor will send heartbeat data to the C2 server “202.abc.xyz.7 via HTTP requests.

Actions on Objectives

- Due to successful mitigations, the adversary never took actions on objectives
- The process was marked as “N/A”

Network Security

- This course exposes students to the tools and techniques used by information security professionals to analyze computer network traffic and identify suspicious and/or malicious activity within that traffic
- Compile open source network defense tools, and monitor legitimate network traffic over their new network
- Generate network traffic reports


Oracle VM VirtualBox Manager
Tools
Take
Delete
Restore
Properties
Clone
Settings
Discard
Show
Name
Taken
Current State
CentOS 7 NetSec (Finished M...)
Powered Off
Slackware NetSec (Hostname:...)
Powered Off

2019-08-20-traffic-analysis-exercise.pcap [Wireshark 1.10.14 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request Expression... Clear Apply Save

No.	Time	Source	Destination	Protoc	Lengt	Info
1680	2019-08-20 19:35:25	10.8.20.101	94.103.86.146	HTTP	314	GET /favicon.ico HTTP/1.1
1345	2019-08-20 19:34:41	10.8.20.101	172.217.9.132	HTTP	886	GET /images/branding/googlelogo/1x/googlelogo_color_150x54dp.png HTTP/1.1
1347	2019-08-20 19:34:41	10.8.20.101	172.217.9.132	HTTP	850	GET /images/errors/robot.png HTTP/1.1
1452	2019-08-20 19:35:24	10.8.20.101	94.103.86.146	HTTP	480	GET /images/h653rH6w/PilH9z95laHTcP4MnRhOF9A/GeqX26wnaS/8YsyasDcXWQnnOMko/S6uKPuADuGk1/GbwJRt1t6UV/9L7tclt9q8RKbN/nKvYej68gPCBsWo1AC8PG/zwuJ
1954	2019-08-20 19:35:27	10.8.20.101	94.103.86.146	HTTP	507	GET /images/jBsO54_2BSa5oBENEZ/EttkU7CFn/gj86aodttq4SGqKGzI8r/dkGLgHKXE_2BCYPc_2B/iz9iP_2FaGl7POu9Q7UWta/CDXs918WF_2BF/NgpZ3Loa/T7ptv50ZZZPV
1688	2019-08-20 19:35:26	10.8.20.101	94.103.86.146	HTTP	502	GET /images/uZD5Vn6mhixGDQdr/CNcGJS5C1Di8ksv/zwHUQAnlhtaYx_2FLC/6esXCGihE/bHH3S8sftmF6_2B9Ny2K/x48gu_2B14EZ7uhi8bQ/F_2B9mEQMX0NlsNC66yxvT/qz
1331	2019-08-20 19:34:41	10.8.20.101	172.217.6.174	HTTP	781	GET /images/wf_2BKr4G/FBs5faKhKo1Pnp08vMzq/zibGUzrNNpWqxTjIQAm/0UsHGbO79hlbB2A_2Fmfp7/oeErI2s2po_2F/Ew1zMmbp/HYA_2FMNo72ovThdaTAFCKZ/F_2Fgr5
2029	2019-08-20 19:36:47	10.8.20.101	23.200.143.72	HTTP	271	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab HTTP/1.1
413	2019-08-20 19:30:55	10.8.20.101	63.239.233.90	HTTP	151	GET /ncsi.txt HTTP/1.1
687	2019-08-20 19:31:33	10.8.20.101	94.103.87.160	HTTP	140	GET /qtra/ttqr.php?l=csuv3.j12 HTTP/1.1
6112	2019-08-20 19:49:57	10.8.20.101	185.183.98.232	HTTP	130	GET /samerton.png HTTP/1.1
16701	2019-08-20 19:53:49	10.8.20.101	185.183.98.232	HTTP	205	GET /samerton.png HTTP/1.1
7765	2019-08-20 19:50:22	10.8.20.101	185.183.98.232	HTTP	204	GET /tablone.png HTTP/1.1
3251	2019-08-20 19:46:43	10.8.20.101	206.189.74.47	HTTP	264	GET /wp-content/uploads/2019/08/3antifreeze.rar HTTP/1.1
2138	2019-08-20 19:41:39	10.8.20.101	139.198.5.65	HTTP	269	GET /wp-content/uploads/2019/08/4antifreeze.rar HTTP/1.1
12669	2019-08-20 19:51:42	10.8.20.101	68.183.185.221	HTTP	262	GET /wp-content/uploads/2019/08/antifreeze.rar HTTP/1.1
10374	2019-08-20 19:50:55	10.8.20.101	185.183.98.232	HTTP	130	GET /wredneg2.png HTTP/1.1

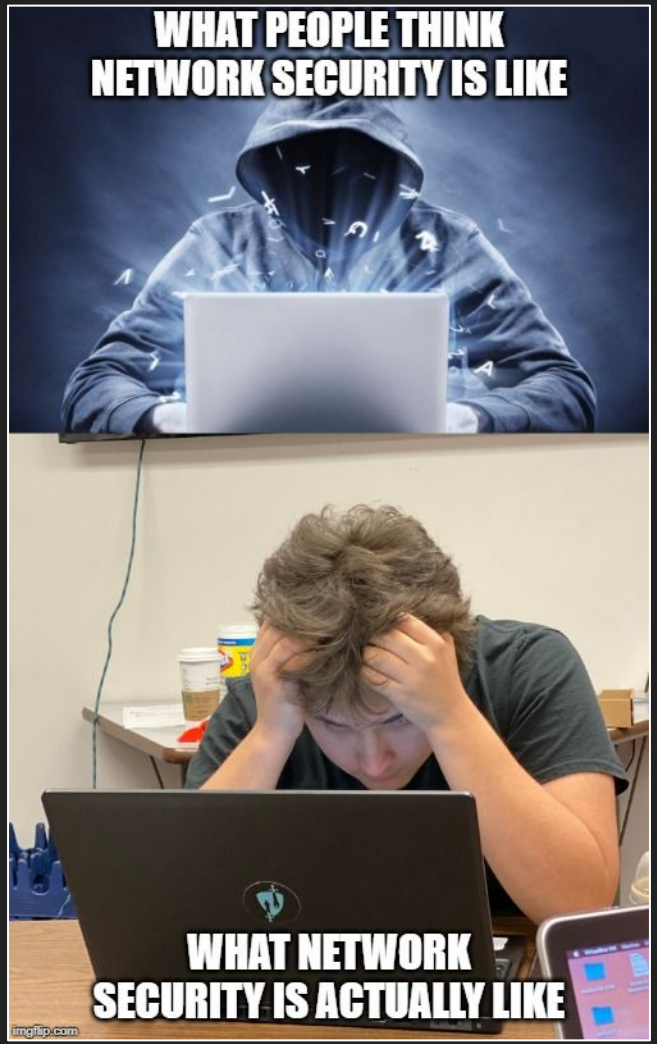
```
▸ Frame 12669: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits)
▸ Ethernet II, Src: AsustekC_a6:01:92 (00:18:f3:a6:01:92), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
▸ Internet Protocol Version 4, Src: 10.8.20.101 (10.8.20.101), Dst: 68.183.185.221 (68.183.185.221)
▸ Transmission Control Protocol, Src Port: 49564 (49564), Dst Port: http (80), Seq: 1, Ack: 1, Len: 208
▾ Hypertext Transfer Protocol
  ▸ GET /wp-content/uploads/2019/08/antifreeze.rar HTTP/1.1\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64)\r\n
    Host: boozzdigital.com\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://boozzdigital.com/wp-content/uploads/2019/08/antifreeze.rar]
    [HTTP request 1/1]
    [Response in frame: 13445]
```

Date	Time	Notes	Source	IP Source	IP Destination
20-08-2019	19:31:34	ET INFO EXE - Served Attached HTTP	Snort	94.103.87.160	10.8.20.101
20-08-2019	19:31:34	ET INFO Packed Executable Download	Snort	94.103.87.160	10.8.20.101
20-08-2019	19:31:34	ET POLICY PE EXE or DLL Windows file download HTTP	Snort	94.103.87.160	10.8.20.101
20-08-2019	19:31:34	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	Snort	94.103.87.160	10.8.20.101
20-08-2019	19:36:36	ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)	Snort	10.8.20.101	208.67.222.222
20-08-2019	19:36:47	ET DNS Query to a *.top domain - Likely Hostile	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:42:24	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	Snort	89.105.203.184	10.8.20.101
20-08-2019	19:49:09	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	Snort	185.117.75.41	10.8.20.101
20-08-2019	19:49:10	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	Snort	89.105.203.184	10.8.20.101
20-08-2019	19:49:19	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	Snort	89.105.203.184	10.8.20.101
20-08-2019	19:49:57	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:49:57	ET POLICY PE EXE or DLL Windows file download HTTP	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:49:57	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:50:22	ET USER_AGENTS Suspicious User-Agent (contains loader)	Snort	10.8.20.101	185.183.98.232
20-08-2019	19:50:22	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:50:22	ET POLICY PE EXE or DLL Windows file download HTTP	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:50:25	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)	Snort	89.105.203.184	10.8.20.101
20-08-2019	19:50:26	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:26	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:26	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:31	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:31	OS-WINDOWS Microsoft Windows raw WriteAndX InData pointer adjustment attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:31	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:31	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:31	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:36	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:36	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:41	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:41	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:46	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:46	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:51	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:51	OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags)	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010	Snort	10.8.20.8	10.8.20.101
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	OS-WINDOWS Microsoft Windows SMB remote code execution attempt	Snort	10.8.20.101	10.8.20.8
20-08-2019	19:50:55	ET INFO SUSPICIOUS Dotted Quad Host MZ Response	Snort	185.183.98.232	10.8.20.101
20-08-2019	19:50:55	ET POLICY PE EXE or DLL Windows file download HTTP	Snort	185.183.98.232	10.8.20.101

Snort Alerts | Wireshark | Bro DNS log | Bro HTTP log | Bro SSL log | +

Skills Learned/Sharpened

- Wireshark
- Splunk
- Snort
- Zeek
- Vagrant - create VMs
- Operating Systems: CentOS 7, Slackware
- ALL INSTALLATIONS DONE FROM SCRATCH


WHAT PEOPLE THINK
NETWORK SECURITY IS LIKE
WHAT NETWORK
SECURITY IS ACTUALLY LIKE
imgflip.com


WHEN A GIRL
NEEDS HELP PEN TESTING
AND YOU GIVE
HER THIS LOOK
imgflip.com