Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

01

Network Topology & Critical Vulnerabilities

- **Network Diagram**
- **Vulnerability Analysis**

02

Exploits Used

- **WPScan**
- **Weak Passwords**
- **Directory Browsing**
- **John the Ripper**
- **Privilege escalation**

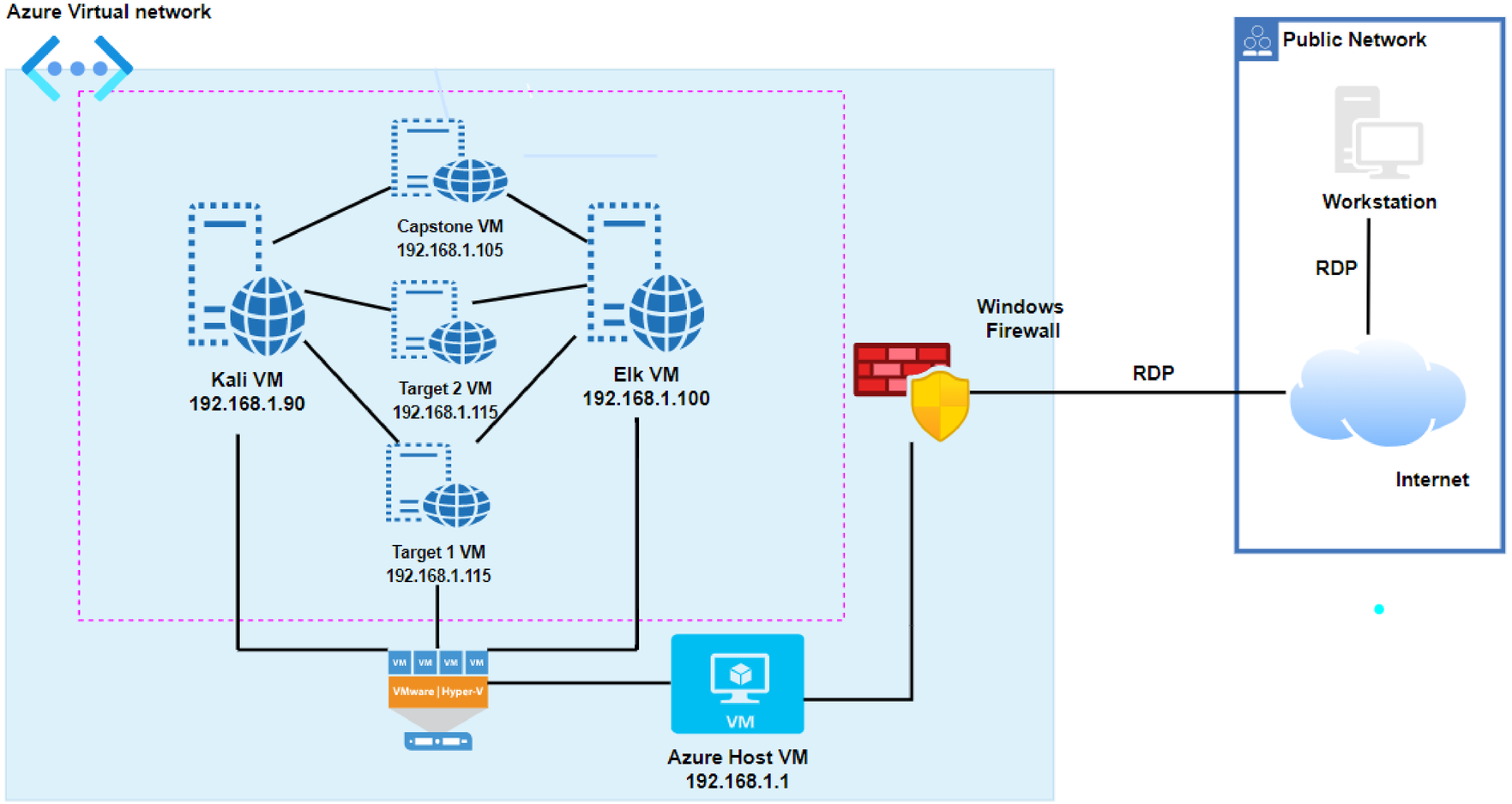
03

Methods Used to Avoiding Detect

- **Monitoring**
- **Stealth exploitation**

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.100
OS:Linux
Hostname: Elk

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target2

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Wordpress user enumeration	User enumeration returns usernames for wordpress users	Offer useful information for exploitation
Weak password	Simple usernames and password	Login access to server
Directory browsing	Directory and file searching is enabled for user would not need access to.	Critical information could be found through compromised user

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

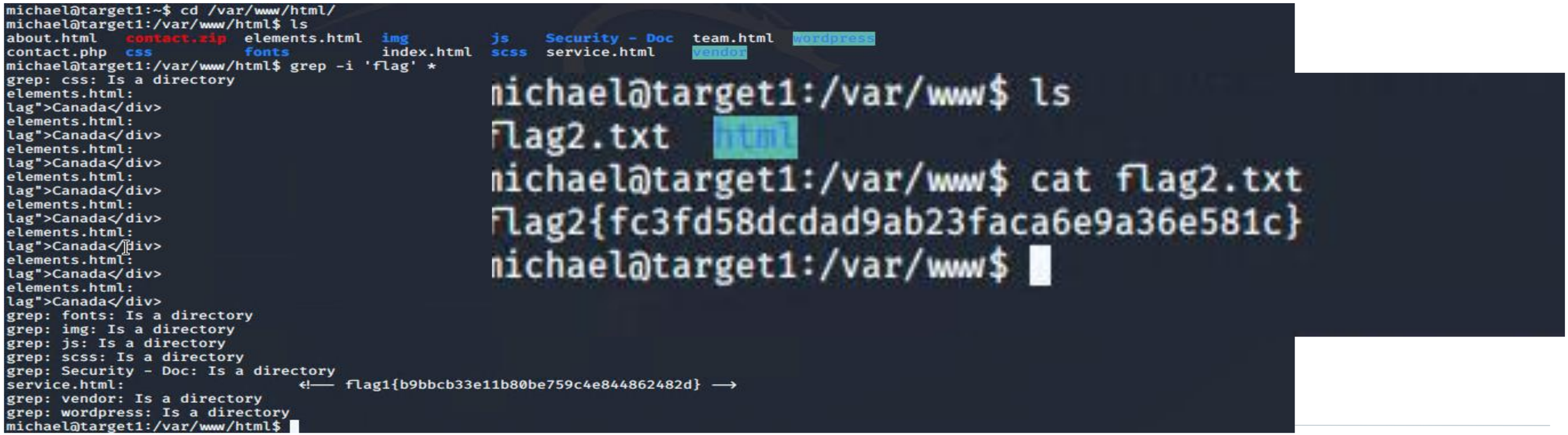
Vulnerability	Description	Impact
Access config file	Exposure of Sensitive Information to an unauthorized actor (wp-config.php)	Access config details – mysql database username and password were exposed
Crack password hash	Use of a One-Way Hash without a Salt	Abled to crack hash and uncover password
Privilege escalation	Provide elevated privileges	Full access to the system and more critical information were compromised

Exploits Used

Exploitation: [Open ports, Identify Users , Password guess]

Summarize the following:

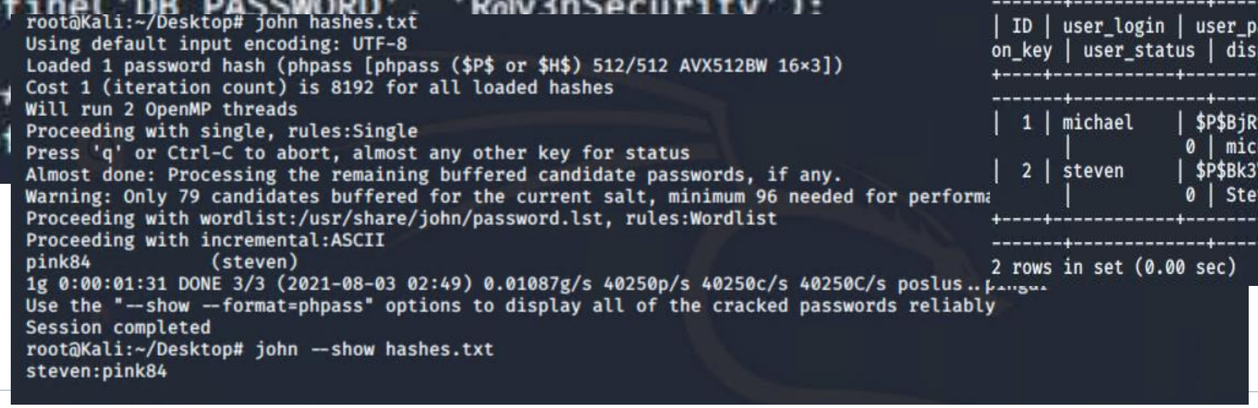
- Used nmap to identify the open ports and services.
- used wpscan to identify the users.
- Guessed the weak password for Michael and SSH into the system.
- Exploit granted user shell access to Michael’s account and found flag1 and flag2.

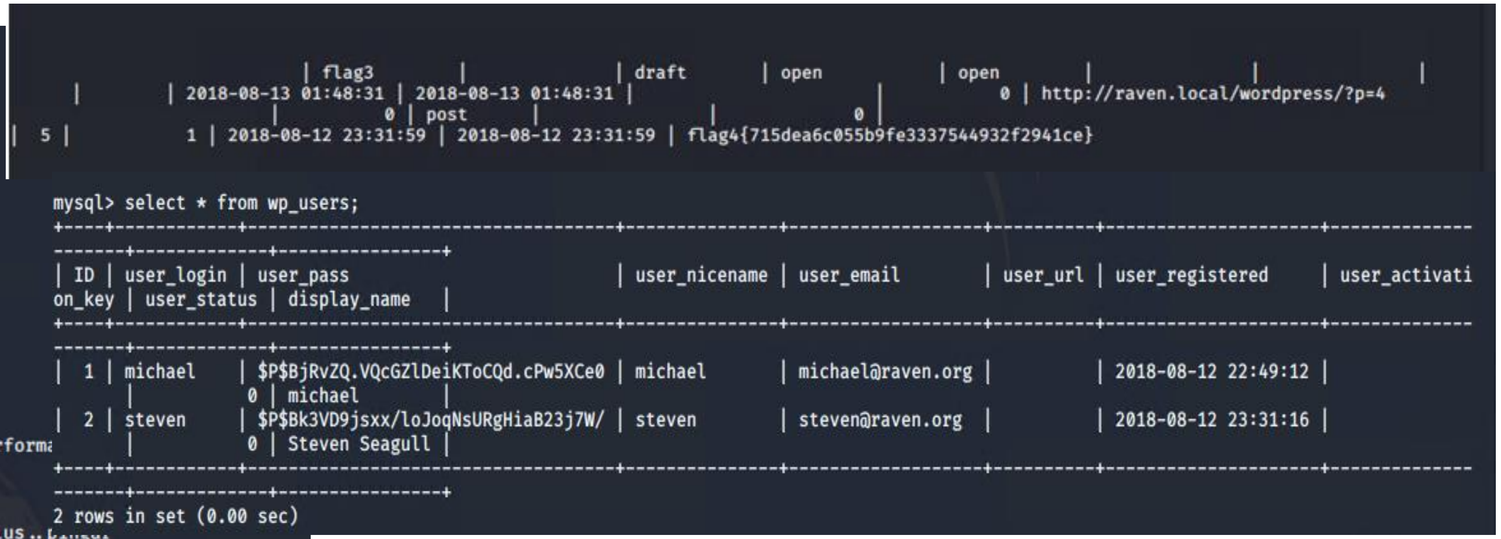


Exploitation: [access SQL database]

Summarize the following:

- Able to access WordPress config file (wp_config.php).
- Accessed the username and password of SQL database which is in readable text.
- This exploit granted the access to MySQL and found Steven's password hash and Flag3.

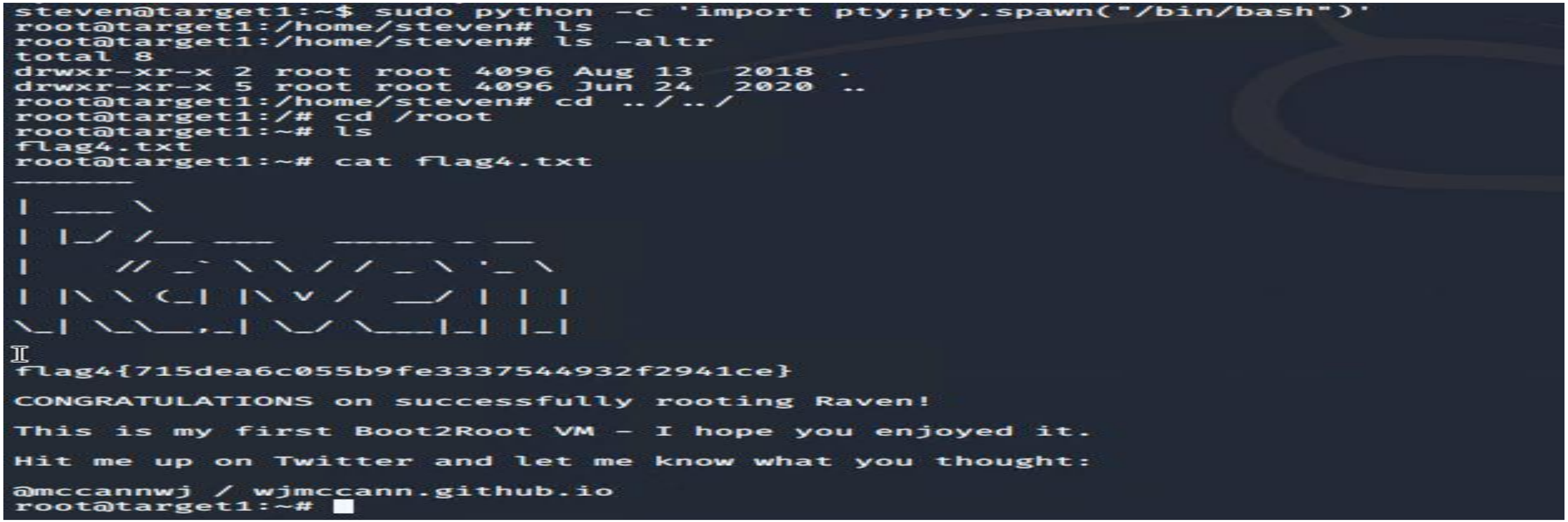




Exploitation: [gained privilege access]

Summarize the following:

- Using John, cracked the Steven’s password hash.
- Login into target1 using the Steven’s username and password.
- Using the python spawn shell, gained the root access and found Flag4.

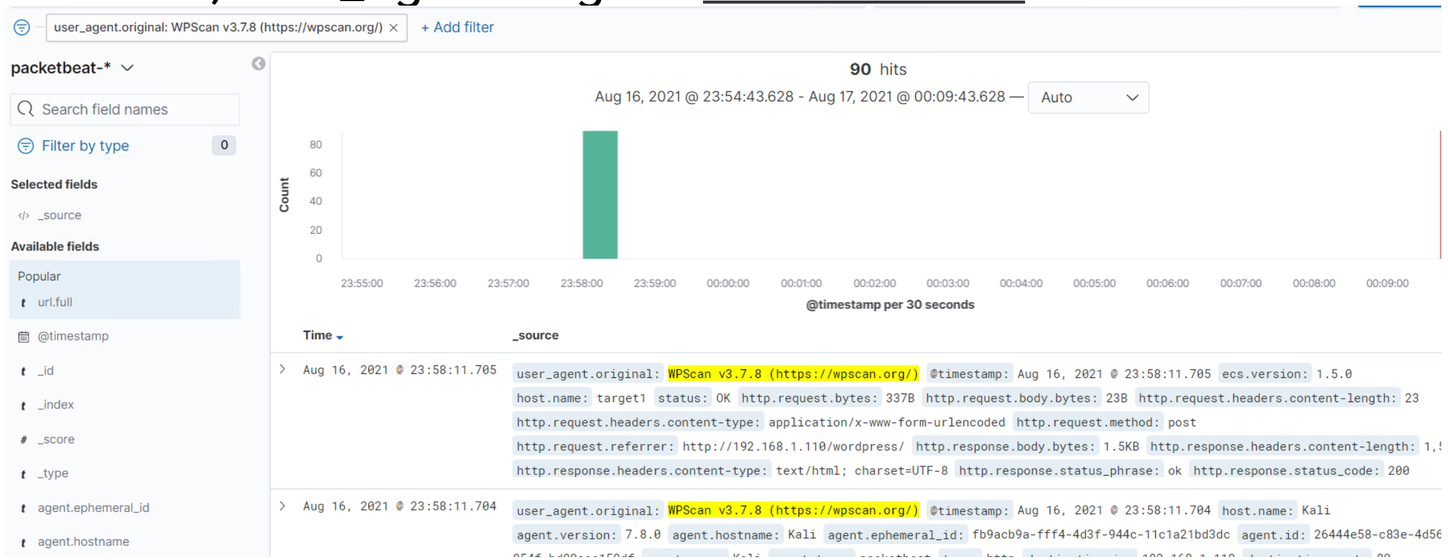


Avoiding Detection

Stealth Exploitation of WPScan

Monitoring Overview

- WordPress user enumeration detection metrics; user_agent.original:WPScan v3.7.8 (https://wpscan.org/)
- **Threshold**: 0



Mitigating Detection

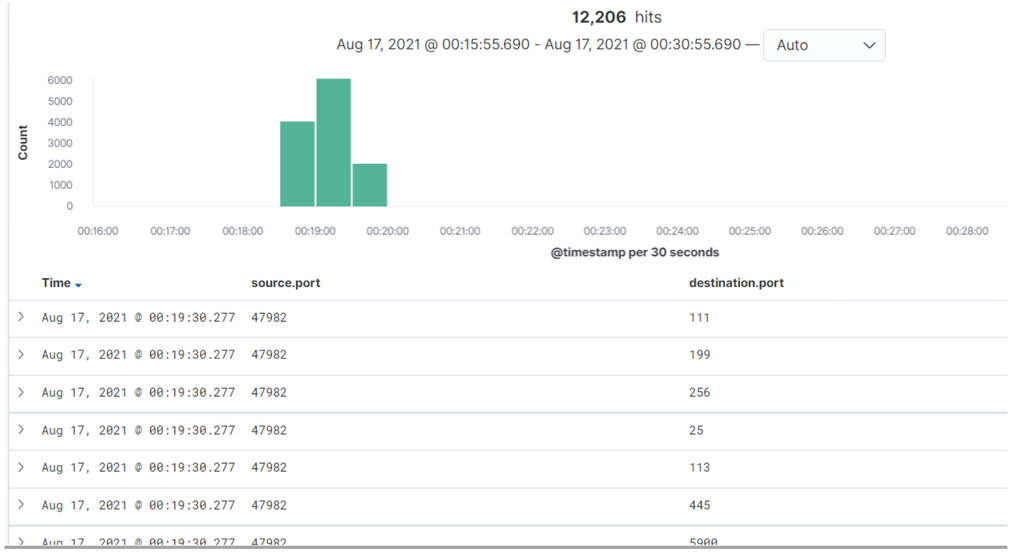
- Run stealthy/passive scan to avoid detection

Stealth Exploitation of Open ports

Monitoring Overview

- Set up an alert on Unauthorized Port scan detection.

  Threshold: 1000 per minute per given ip



Time	source.port	destination.port
Aug 17, 2021 @ 00:19:30.277	47982	111
Aug 17, 2021 @ 00:19:30.277	47982	199
Aug 17, 2021 @ 00:19:30.277	47982	256
Aug 17, 2021 @ 00:19:30.277	47982	25
Aug 17, 2021 @ 00:19:30.277	47982	113
Aug 17, 2021 @ 00:19:30.277	47982	445
Aug 17, 2021 @ 00:19:30.277	47982	5900

Mitigating Detection

- Port Scan: Performing slow rate port scan (--scan-delay <time>)

Exploitation of weak passwords

Monitoring Overview

- Implementing password policy and conducting audits to discover users having weak passwords

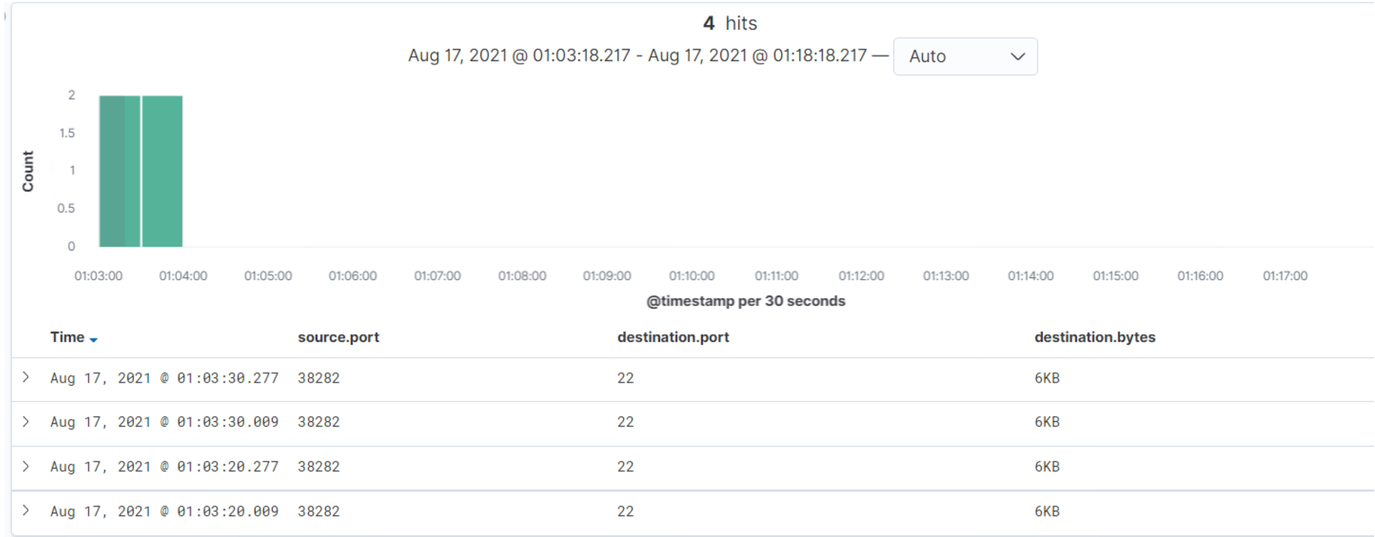
Mitigating Detection

- Use social engineering tactics to get information about passwords for password guessing.

Stealth Exploitation of SHH login

Monitoring Overview

- SHH login alerts through port 22 from external ip
- **Threshold**: 0



Time	source.port	destination.port	destination.bytes
Aug 17, 2021 @ 01:03:30.277	38282	22	6KB
Aug 17, 2021 @ 01:03:30.009	38282	22	6KB
Aug 17, 2021 @ 01:03:20.277	38282	22	6KB
Aug 17, 2021 @ 01:03:20.009	38282	22	6KB

Mitigating Detection

- ip address spoofing

Stealth Exploitation of gained privilege access

Monitoring Overview

- No Alerts triggered in as it is normal activity for user

Mitigating Detection

- Find other vulnerabilities to exploit for root access (use sudo exploits).
- Use reverse shell exploits


The End