Final Engagement

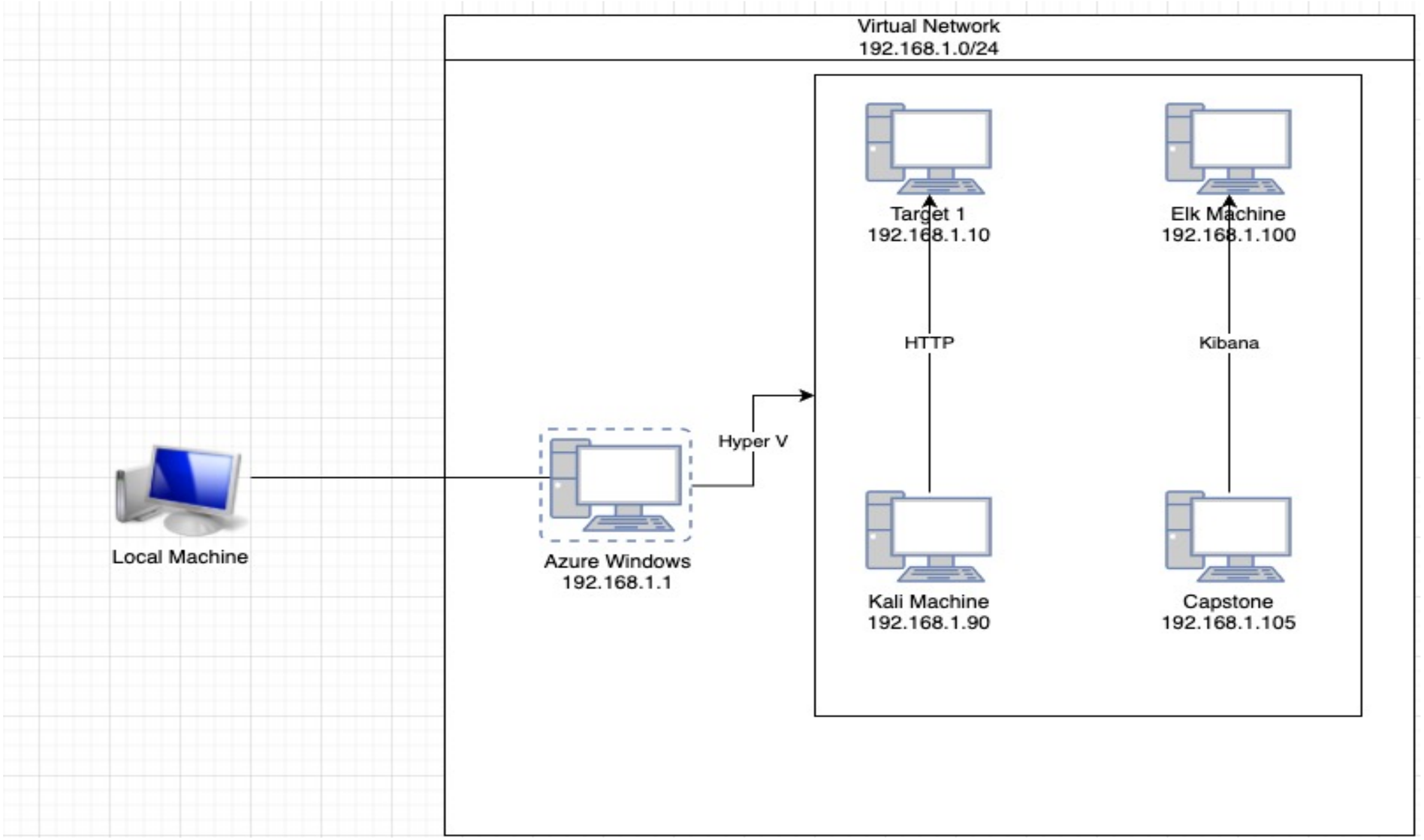
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

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: 192.168.1.1
OS: Windows
Hostname: ML-RefV-68 4427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Ubuntu
Hostname: Target 1

IPv4: 192.168.105
OS: Ubuntu
Hostname: Capstone

Critical Vulnerabilities: Target 1

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

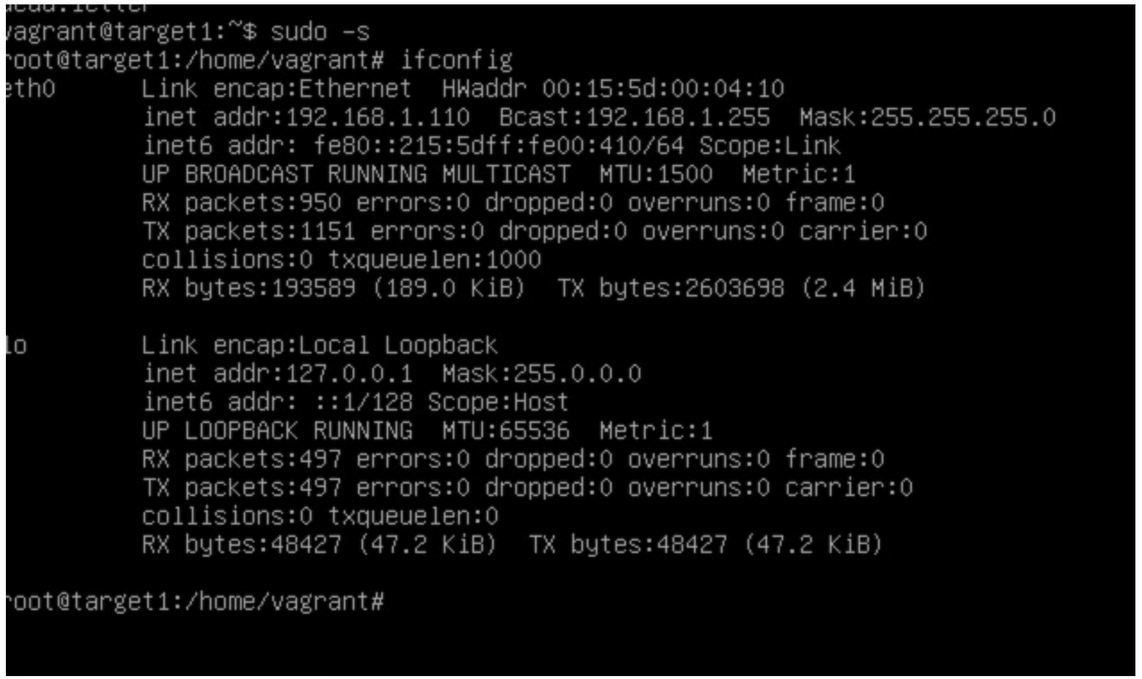
Vulnerability	Description	Impact
Nmap Port Scan	*Allows for attackers to scan for open ports in a network*	*This will show IP address of the servers and all open ports available for exploit*
WordPress Enumeration	*Allows attacker to gain access to user information*	*Gained access to the wp_config.php which gave access to the mysql database which gave access to user passwords and hashes*
Brute Force/Weak password policy	*Simple passwords all for easy Brute Force attack*	*Used brute force to gain unauthorized access by using Michael and Steven's passwords into the target 1 machine*
Python Privilege Escalation	*SSH'd into the target 1 machine using Steven's credentials*	*Gained root privledges*

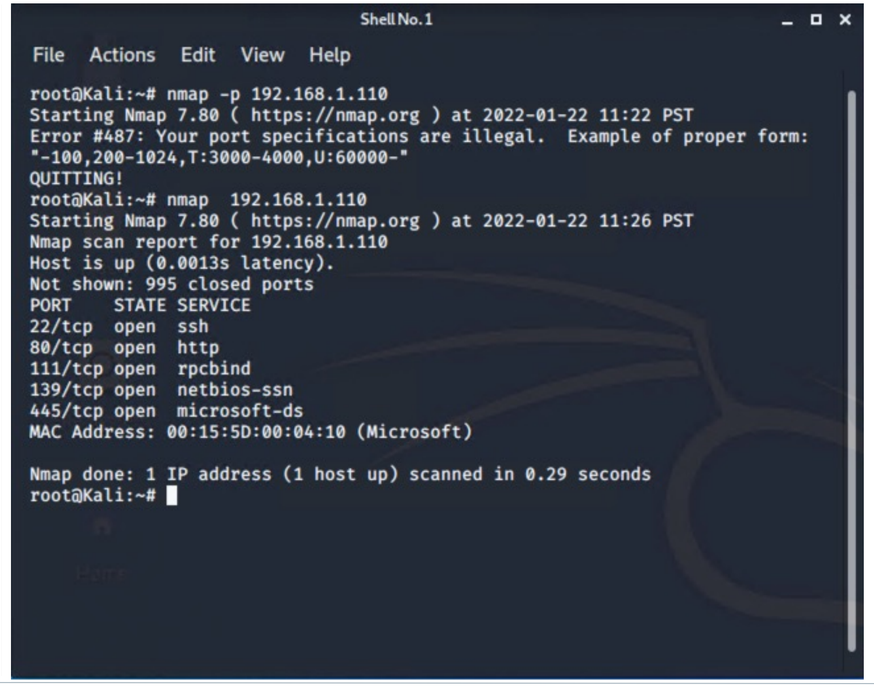
Exploits Used

Exploitation: [Nmap Scan]

Summarize the following:

- *Used ifconfig on target VM to find IP needed to use for Nmap scan.*
- *Used Nmap to scan IP address an check for open ports*
- *On IP address 192.168.1.110 of the target 1 server, ports 22 and 80 were open for exploitation.*

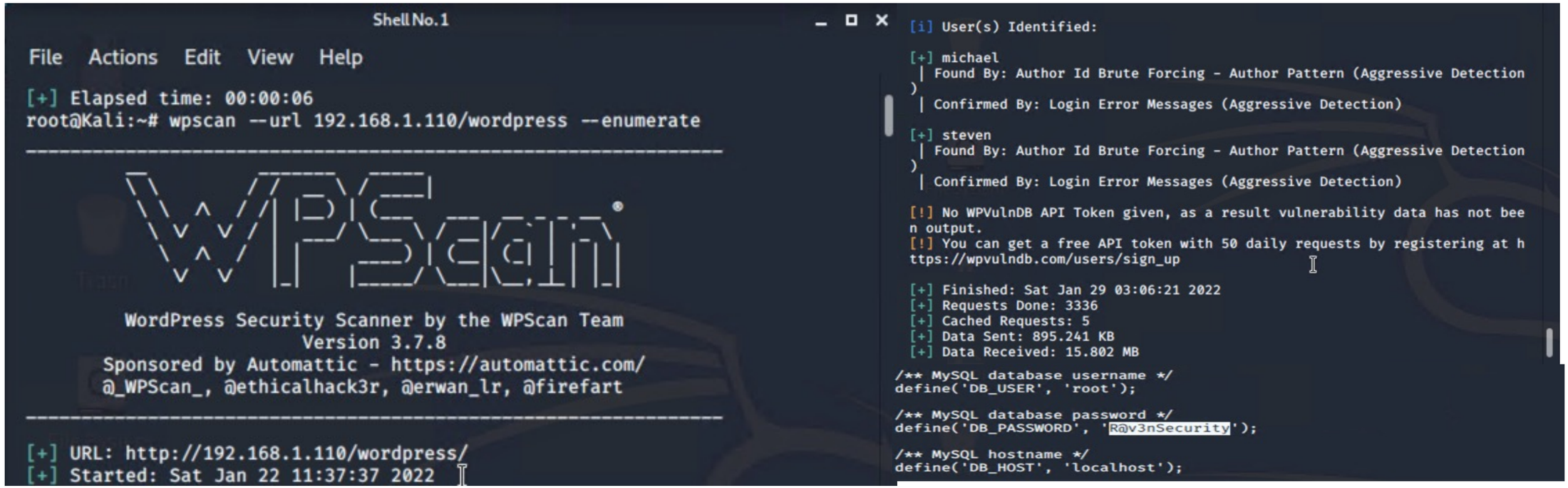




Exploitation: [Wordpress Enumeration]

Summarize the following:

- *Used WPScan to enumerate WP* ***wpscan –url http://192.168.1.110 –enumerate u***
- *Gained access to the wp_config.php file which gave access to the mysql database*

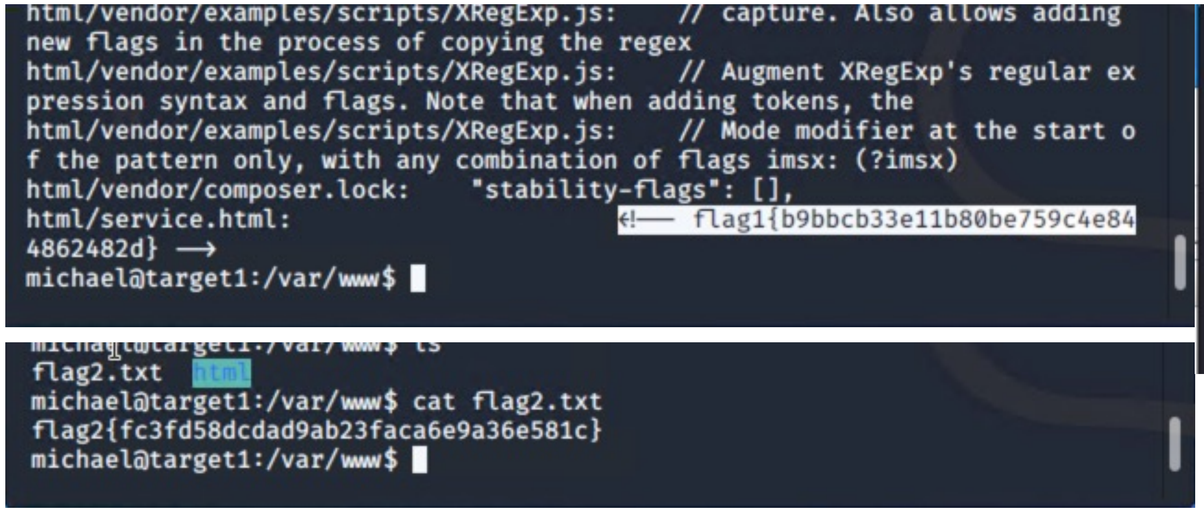


Exploitation: [Brute Force]/Weak Password Policy

Summarize the following:

We SSH'd into Target 1 machine because of Michael's weak password. Could have used Hydra on this but we actually guessed the password it was so weak. This is where we found Flag 1 and 2

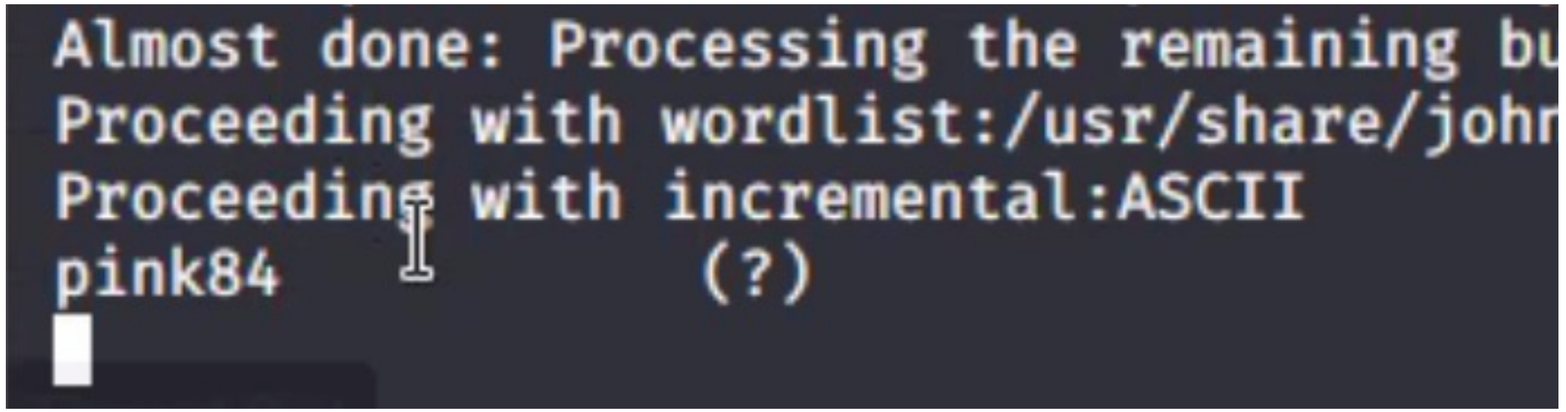
- *We used the command mysql –u root –p*
- *Saved the hashes to salts.txt*



Exploitation: [Brute Force]/Weak Password Policy/Continued

Summarize the following:

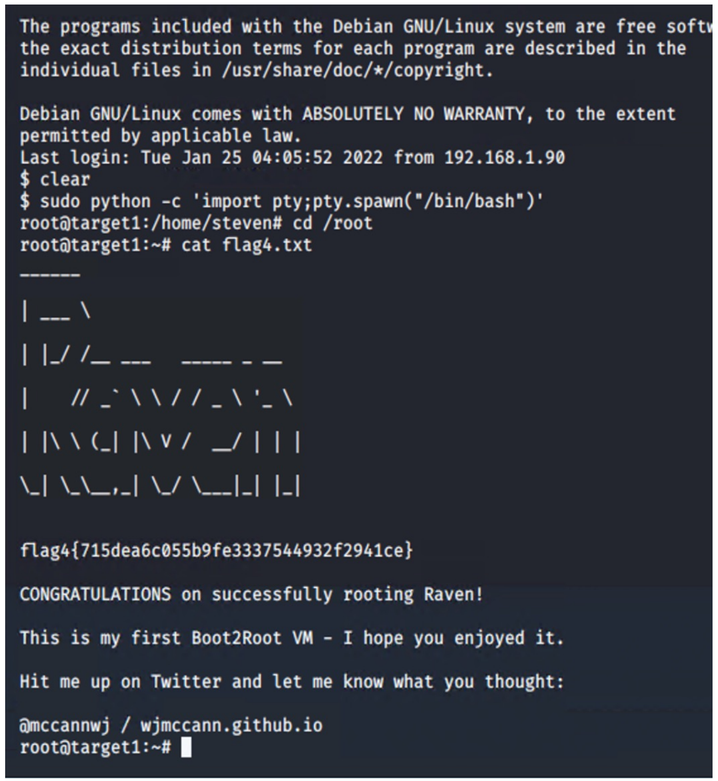
Used John the Ripper to crack Steven's hash



Exploitation: Python Privilege Escalation

Summarize the following:

- *SSH'd into steven @192.168.1.110 with password pink84*
- *After gaining access to Stevens shell I escalated my privileges to root by by the following command*
  - ***Sudo python –c 'import pty;pty.spawn)"/bin/bash')***
  - *Then went to* ***cd/root***

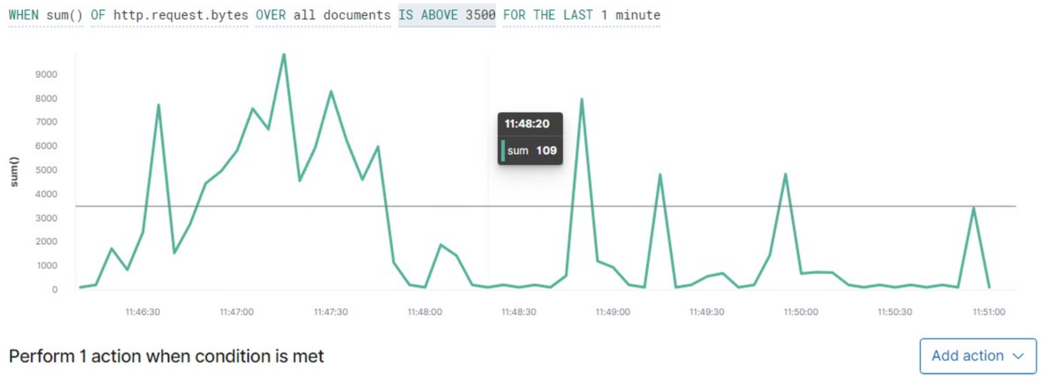


Avoiding Detection

Stealth Exploitation of Network Enumeration

Monitoring Overview

- *WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minue*
- *Request from the same IP to all ports*
- *If the request bytes are over 3500 hit a minute*



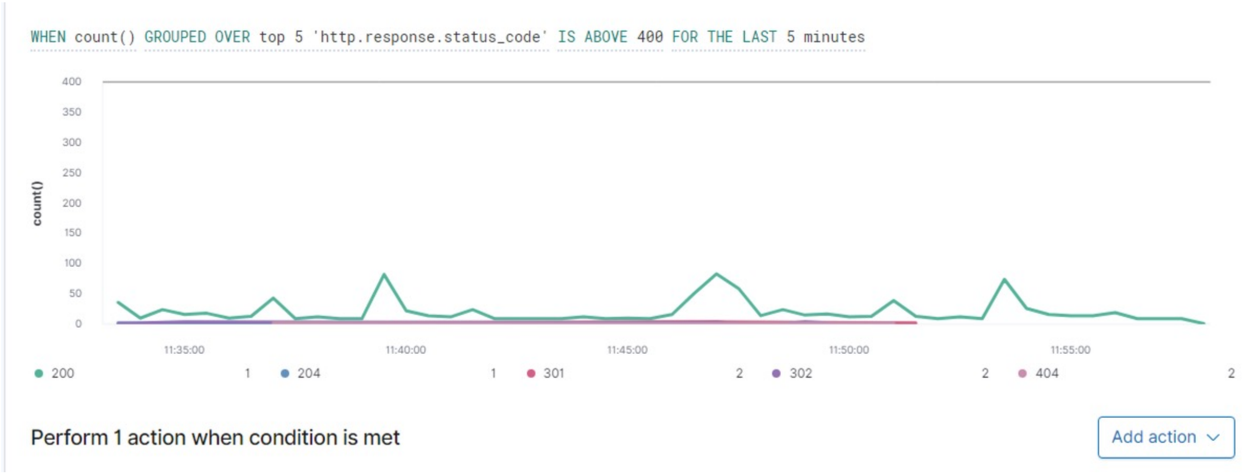
Mitigating Detection

- *Only scan ports that are know to be vulnerable to attacks*
- *Randomize the HTTP request you send within the minute*

Stealth Exploitation of Wordpress Vulnerability

Monitoring Overview

- *WHEN count () GROUPED OVER top 5 'http.response.status.code' IS ABOVE 400 FOR THE LAST 5 minutes*
- *HTPP errors and 401 request*
- *When there is over 400 HTTP responses in 5 minutes*



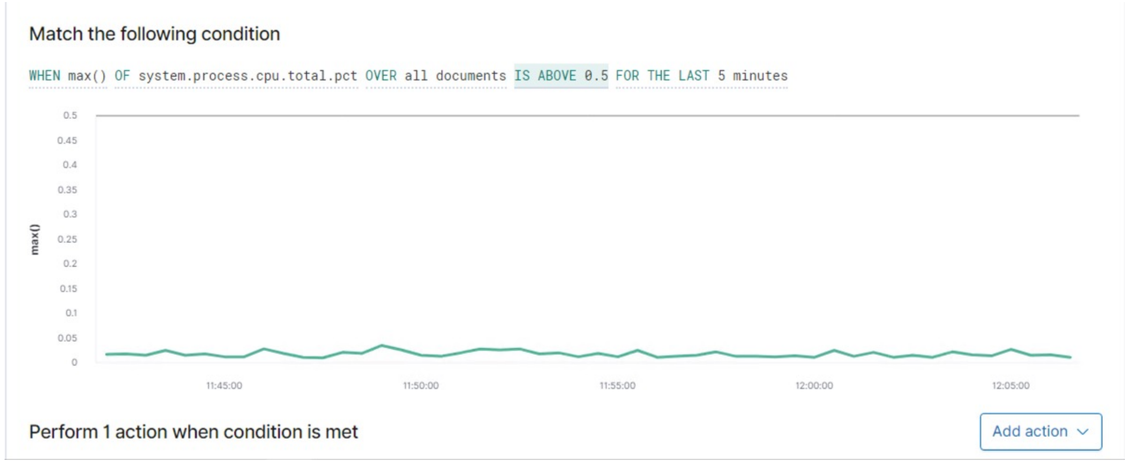
Mitigating Detection

- *You can put a pause after a certain amount of HTTP requests*
- *By using command line sniffing*

Stealth Exploitation of Brute Force

Monitoring Overview

- *WHEN max () OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 MINUTES*
- *System CPU Usage*
- *.5 for 5 minutes*



Mitigating Detection

- *Moving the wp_hashes.txt file to local machine so when John the Ripper is ran there won't be a spike in CPU Usage. I actually did this when I moved it to salts.txt and then ran John the Ripper on my local machine*
- *Using Hashcat instead of John the Ripper*