Capstone Engagement

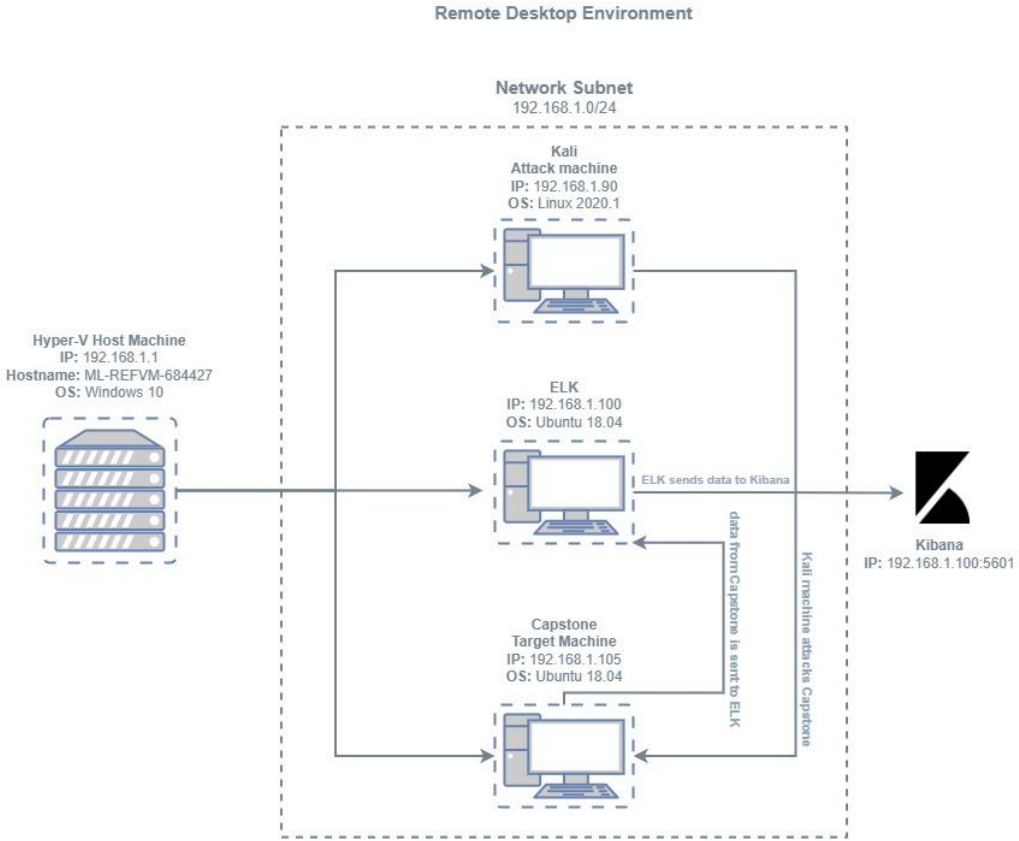
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows 10
Hostname: ML-REFVM-684427

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-REFVM-684427	192.168.1.1	Host machine
Kali	192.168.1.90	Network Attack machine
ELK	192.168.1.100	Data Monitoring machine
Capstone	192.168.1.105	Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration	This vulnerability does not have lockout thresholds and can leave access ports open.	The attacker can easily brute force passwords with no limitations or being locked out.
Brute Force Vulnerability	This vulnerability allows the user to access credentials using tools that combine numbers and letters to guess a password.	A threat attacker can brute force a simple password in a matter of minutes, gaining access to sensitive data.
Port 80 Vulnerability	This vulnerability allows user to easily access company files and secret folder on an organization's website.	Using this vulnerability, an attacker can access secret company files step-by-step and finding a hash to breach the network.
Webdav Vulnerability	This vulnerability allows for any user to upload files into a webdav folder with no restrictions.	An attacker can upload a malicious file or php script into the webdav folder with simple "drag and drop" method. The attacker can later gain access with a meterpreter session.

Exploitation: Security Misconfiguration

01

Tools & Processes

An nmap service scan was used to determine which ports were open. According to the scan, port 22 (which allows a user to SSH into a system) was open. Port 80 was open as well.

02

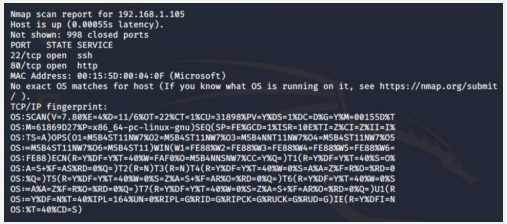
Achievements

This exploit allowed us to SSH into the system and access sensitive data on the network with the cracked employee password.

03

Nmap scan:

Command: `nmap -sS -O -PN 192.168.1.0/24`



Exploitation: Brute Force Vulnerability

01

Tools & Processes

Through company files, the user who has access to the secret files was discovered. Using hydra, the password was brute forced within a matter of minutes.

02

Achievements

Once the password was discovered, sensitive data could be accessed on the network.

03

Brute force:

Command: `hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder -t 40`

Exploitation: Port 80 Vulnerability

01

Tools & Processes

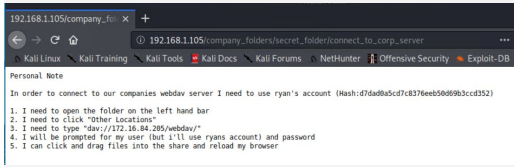
It was previously determined that port 80 was open using the nmap service. Any remote user can gain access to the company's web archives.

02

Achievements

Confidential files were explored, thus the "secret folder" was found. The password hash of an employee was inside the folder, along with step-by-step instructions on how to access the webdav network.

03



Exploitation: Webdav Vulnerability

01

Tools & Processes

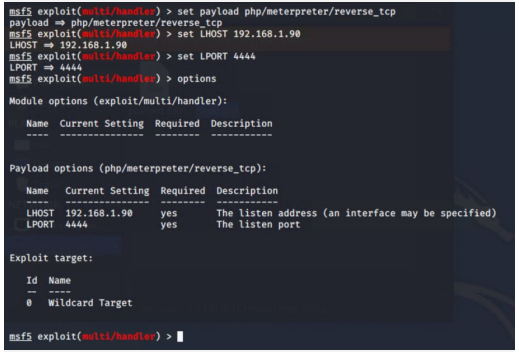
A malicious php payload was created using msfvenom and metasploit. Once the php file was made, it was dragged and dropped into the webdav network folder.

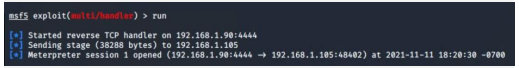
02

Achievements

This created a listener for the webdav network folder. Once the file was double clicked and a meterpreter session was started, access to the system was gain.

03





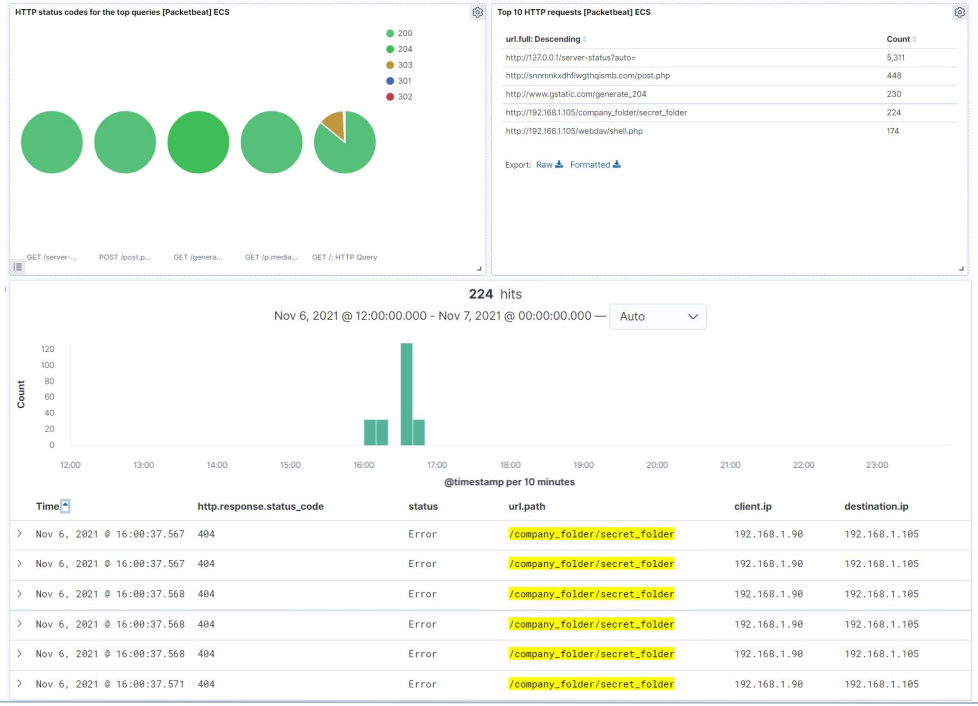
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan began on November 6th, 2021
- 11,238 packets were sent from 192.168.1.90 (the attack machine)
- The sudden spike in traffic indicates that this is a port scan

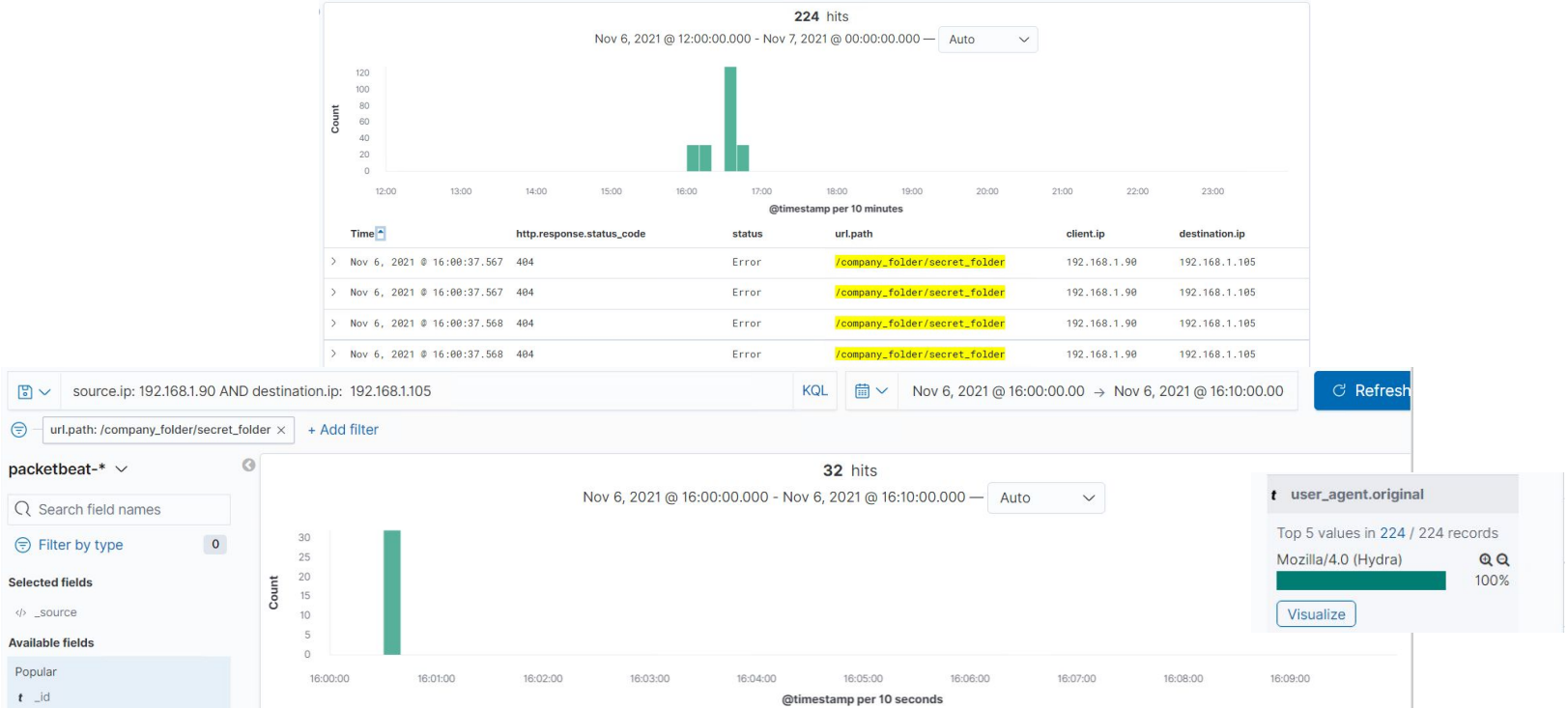
Analysis: Finding the Request for the Hidden Directory

- 224 requests were made to the hidden directory at 4pm
- The file that was requested was a _doc file. This file contained instructions on how to add and access the webdav network server.



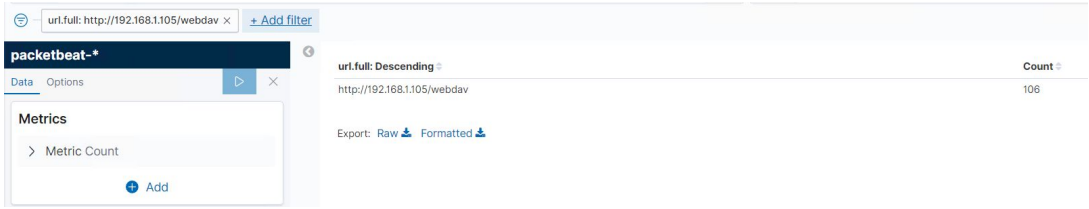
Analysis: Uncovering the Brute Force Attack

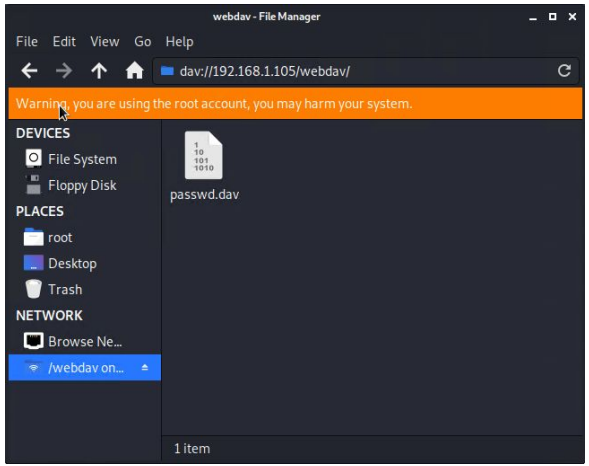
- 224 requests were made during the brute force attack.
- 34 requests were made before the attacker discovered the password

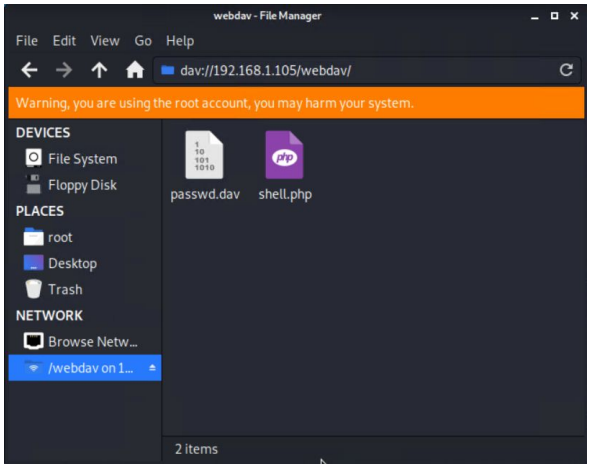


Analysis: Finding the WebDAV Connection

- 106 requests were made to the webdav directory
- A password.dav file and a shell.php file.







Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm that that alerts a high number of port scan through a firewall

An email should be sent to administrators when more then 10 port scans are done within a minute.

System Hardening

Only traffic from certain ports should be allowed; such as, port 80 and 443 to allow traffic from the internet.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Set an alarm that sends an email alert of higher than normal traffic and unauthorized IPs accessing the secret folder.

No more than 4 attempts to access the folder should be made.

System Hardening

Only allow authorized IPs to have access to the secret folder as a whitelist. Also, encrypt any sensitive data and folders.

`/etc/httpd/conf/httpd.conf` is where a whitelist can be made.

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm should be set to limit how many attempts can be made when entering a password before the user is locked out.

The threshold should be set very low to deter threat actors, for example, 5 attempts.

System Hardening

After 5 attempts, the user will be permanently locked out until and administrator can be contacted.

Two factor authentication, complex passwords (8 or more characters, special characters, numbers and case sensitive) and changing passwords once a month would be additional ways to mitigate attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm can be set to monitor traffic and connection attempts from unauthorized IPs to the webdav network.

The unauthorized user will only have 1 attempt.

System Hardening

Blocking traffic from unauthorized IPs with a whitelist or group policy

Also, more complex passwords (8 or more characters, special characters, numbers and case sensitive) should be implemented to avoid brute force attacks.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Create an alarm to alert when a file is being upload to the webdav folder, whether it is malicious or not. Another alarm should be made when port 4444 is being connected to.

Alerts should be immediate!

System Hardening

Access to the webdav folder should be set to “ready only”. Also, only authorized IPs should have access to the webdav folder.


The End