Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

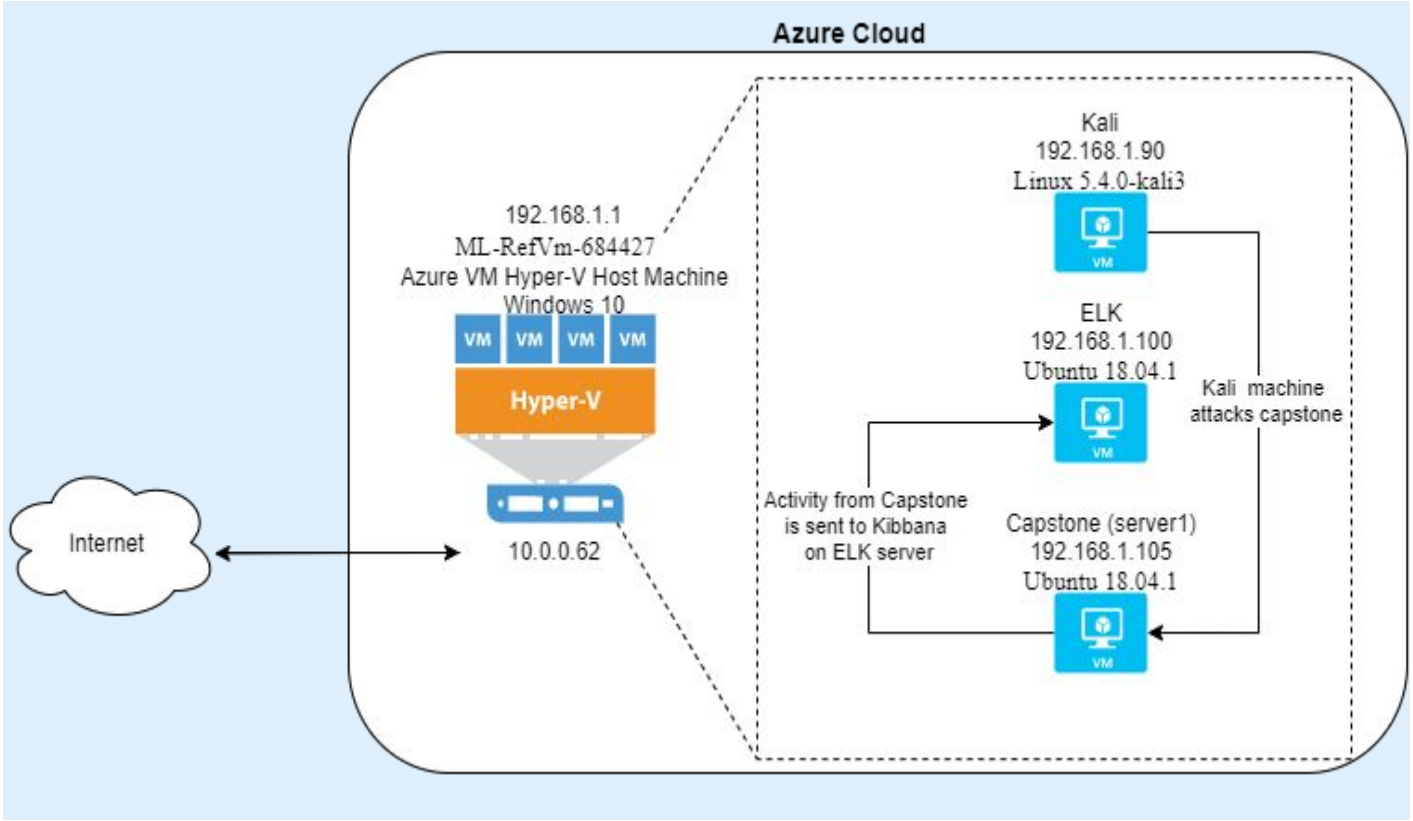
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.62

Machines
IPv4: 192.168.1.90
OS: Linux 5.4.0-kali3
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1
Hostname: Capstone (server1)

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	Security Monitor
Capstone (server1)	192.168.1.105	Apache Server (Target Machine)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Security Misconfiguration	This vulnerability gives users unprecedented access to the system by not allowing for a lockout threshold and leaving access ports open	The attack is able to brute force users passwords in order to gain access to confidential information due to no lockout threshold, as well as access to a system by an open port 22
Webdav Vulnerability (CVE-2020-24389)	This vulnerability gives users the ability to “drag and drop” files into the webdav folder with no restrictions	Using this vulnerability, the attacker is able to upload a malicious php script to act as a listener to give access to the system via a meterpreter session
Port 80 Vulnerability	This vulnerability gives any remote user the ability to access the web containing company files and “secret” folders	Using this vulnerability we were able to access company files containing information that lead us to connect to a secret folder giving us a hash to breach the network

Exploitation: Security Misconfiguration

01

Tools & Processes

Using an nmap service scan, we were able to find that port 22 was open, which allows for SSH into the system. We also discovered through company files the correct user to get access to confidential folders, then were able to brute-force his password via hydra and a rockyou.txt file

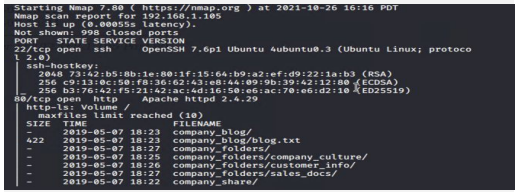
02

Achievements

This exploit gave us user access into the system via SSH, after cracking his password, as well as access to confidential folders within their network

03

Hydra command- hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/



Exploitation: Webdav Vulnerability

01

Tools & Processes

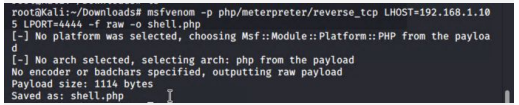
Using msfvenom & metasploit we were able to to create a payload into a php file to then drag and drop our malicious file into the webdav folder

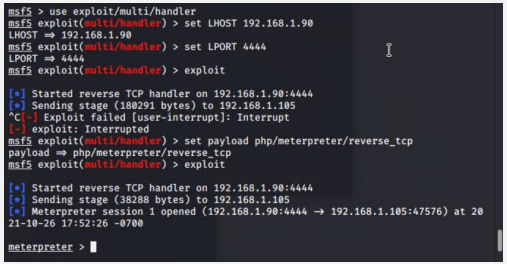
02

Achievements

Using our created payload, we were able to create a listener uploaded to the webdav folder, once the file is clicked on giving us access to the system via a meterpreter session

03





Exploitation: Port 80

01

Tools & Processes

To exploit this vulnerability, we used nmap to determine that port 80 was open, without restriction to any IP address, allowing any remote user to access web archives

02

Achievements

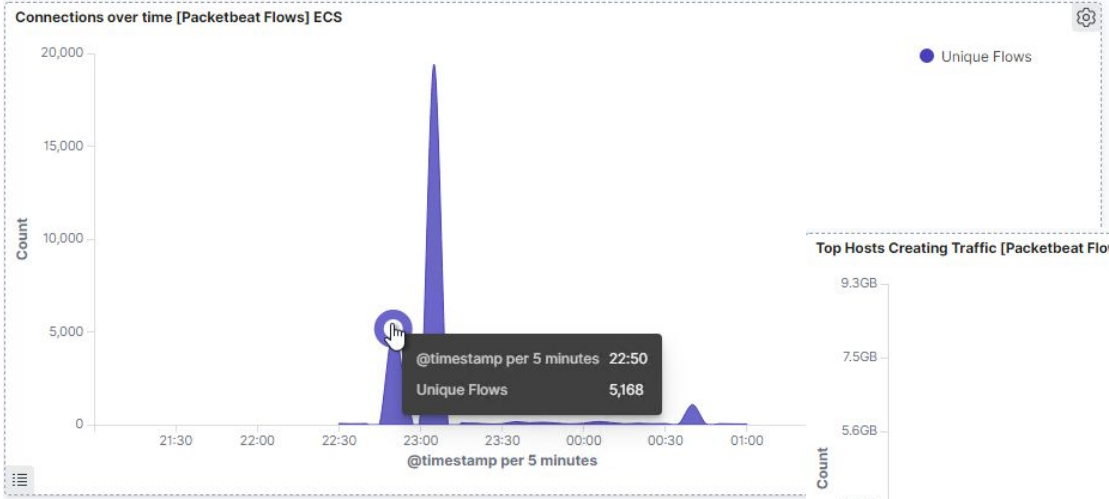
Using this information, we were able to breach confidential files, giving us access to “secret” folders which contained Ryan’s password hash that allowed us to gain access to the system

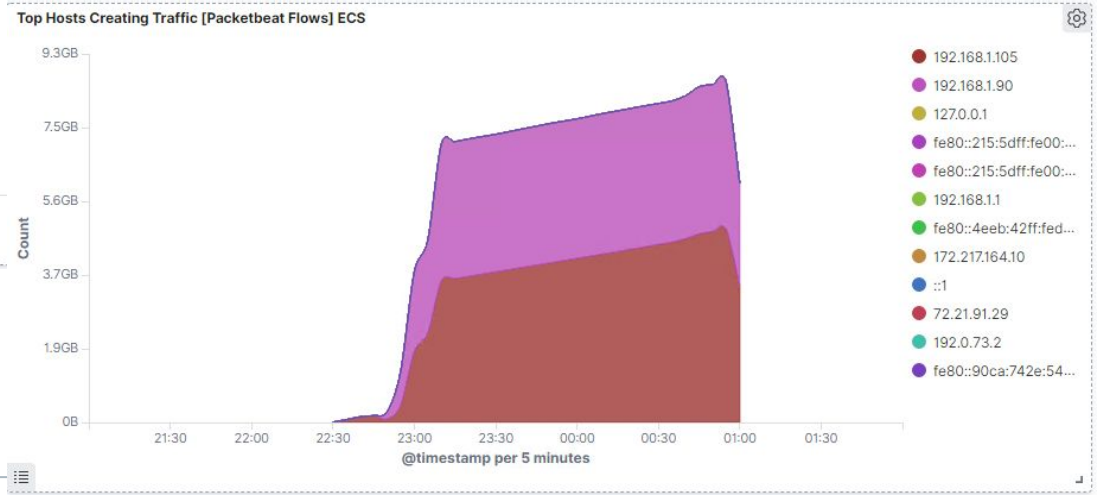
03

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

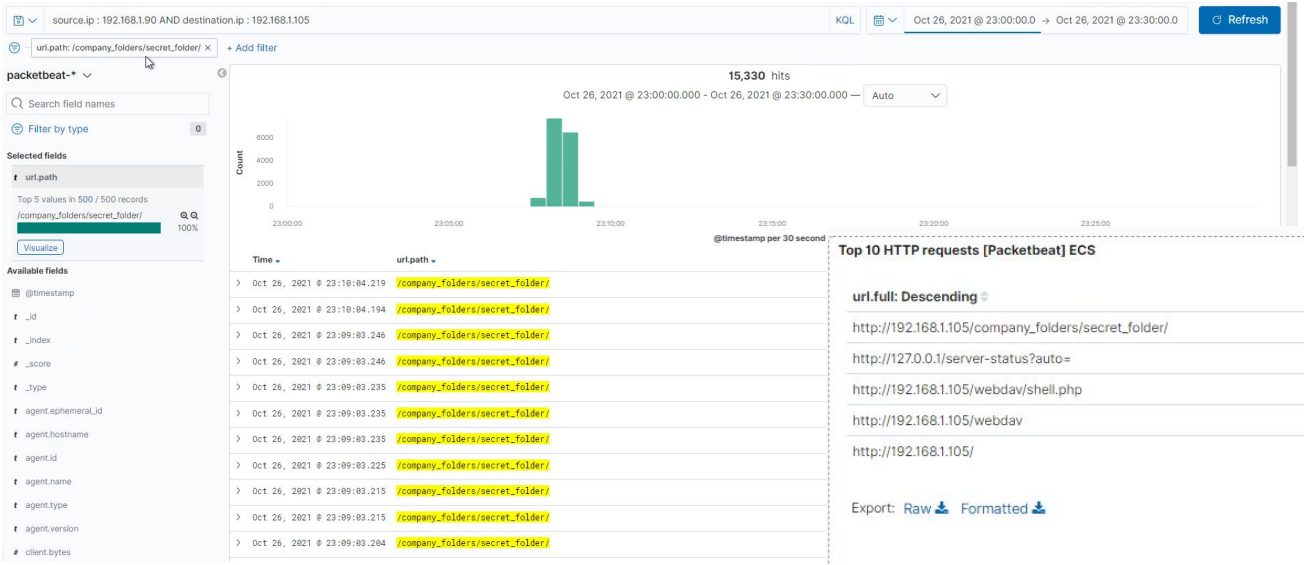
- The port scan began around 22:50 on Oct 26, 2021.
- The peak number of packets sent 19,409 and as shown the majority of the traffic was coming from 192.168.1.90 - the attacking machine.
- The fact that there was a sudden dramatic inflow of traffic can be an indication of a port scan.





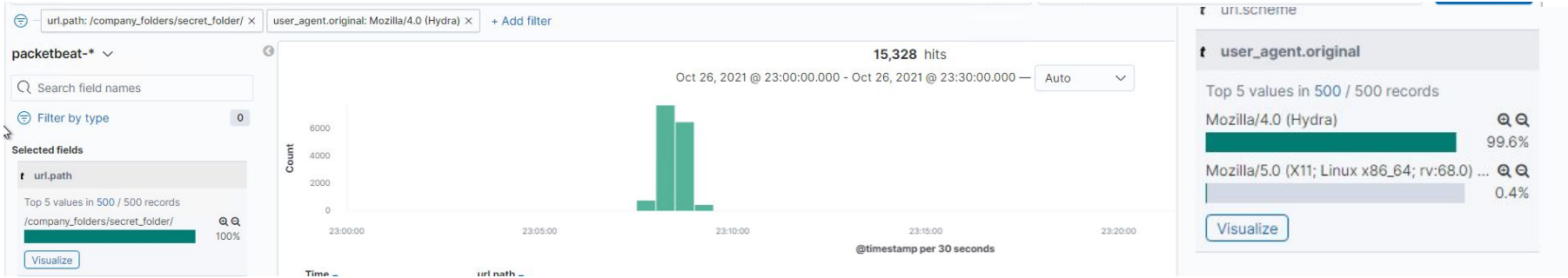
Analysis: Finding the Request for the Hidden Directory

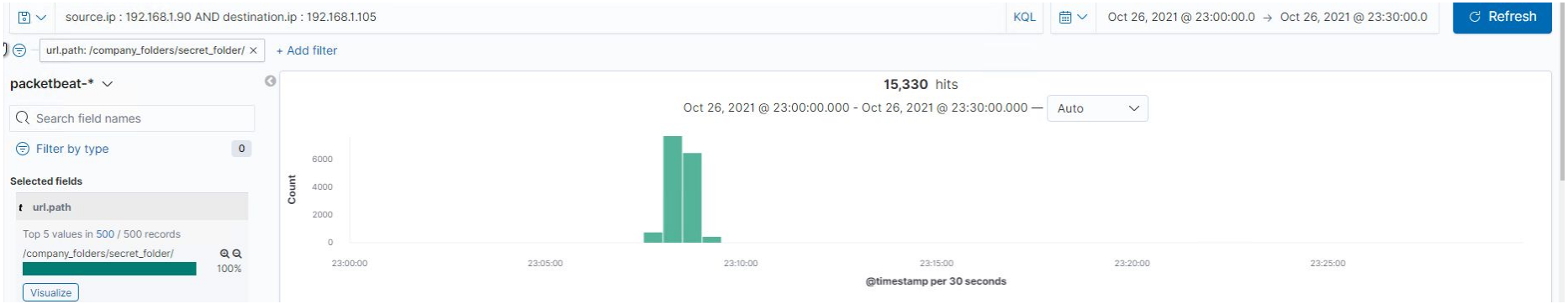
- The requests started around 23:05 on October 26th, 2021 and 15,330 requests were made.
- A doc file containing a password hash and instructions on how to access the company's WebDav server was stored in the secret_folder.



Analysis: Uncovering the Brute Force Attack

- Overall 15,330 requests were made during the brute force attack.
- Of these 15,330 requests 15,328 came from Hydra which means it took 15,328 attempts before the attack was successful.



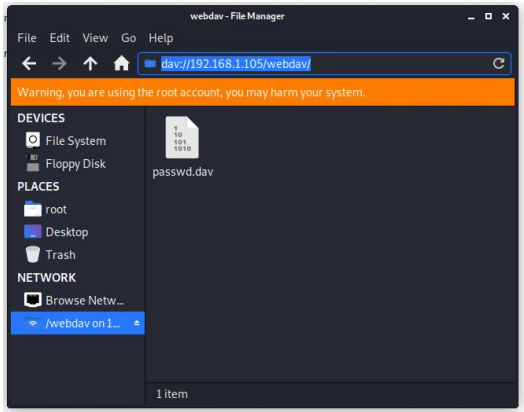


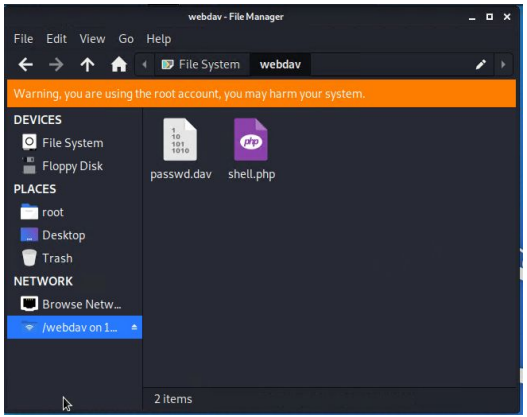
Analysis: Finding the WebDAV Connection

- Overall 63 requests were made to the webdav folder itself. 64 requests were made to the shell.php file that was put into the folder.
- There were 2 files in the webdav folder: the passwd.dav which had a password has for Ryan and the shell.php file that we put in that allowed us to gain access to the system through a meterpreter session.

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	64
http://192.168.1.105/webdav	63

Export: Raw Formatted





Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set up an alarm for when a firewall detects more than 10 port scans in a minute

Email and log when more than 10 port scans hit in a minute

System Hardening

Enable traffic based on need and block everything else. Ports 80 and 443 can be kept open to allow internet traffic

Deploy an IPS that allows for real time alerting.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Send an alert email

More than 5 attempts made to access the folder.

System Hardening

IP's can be whitelisted in /etc/httpd/conf/httpd.conf

Only allowing internal IP's would block outside attacks from accessing the network. Encrypting the data within the folders will help mitigate unauthorized access to sensitive data.

Mitigation: Preventing Brute Force Attacks

Alarm

Set a login alarm for logins

Alert is emailed when 10 or more attempts are made in a 1 minute period

System Hardening

After 10 attempts to login, the user account is locked out and has to be unlocked by an administrator

Display a message to user that they must contact an admin to unlock the account.

Mitigation: Detecting the WebDAV Connection

Alarm

Set an email alert when an unauthorized IP address attempts to connect.

When 1 attempt is made, since the machine would be an unauthorized machine

System Hardening

Connections should not be allowed from the web interface. Also, again creating a whitelist of allowed IP's

Only allow certain users to access the folder. This can be done with group policy. Adding stronger passwords would also help mitigate the possibility of brute force.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Any attempts at an outbound connections from the target machine should email an alert. Anytime someone uploads to the webdav folder, send an email alert. Lastly send an email alert when port 4444 is accessed.

If any attempt is made for these alarms, an alert is immediately sent. There is no need for any of these to be available.

System Hardening

Block all IP's except internal. You could also set access to the webdav folder to read only. This would prevent uploads to the folder.

You can modify the configuration.
nano /etc/httpd/conf/httpd.conf
Allow from 192.168.1.1
Allow from 192.168.1.105
Deny from all external IPs


The End