



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

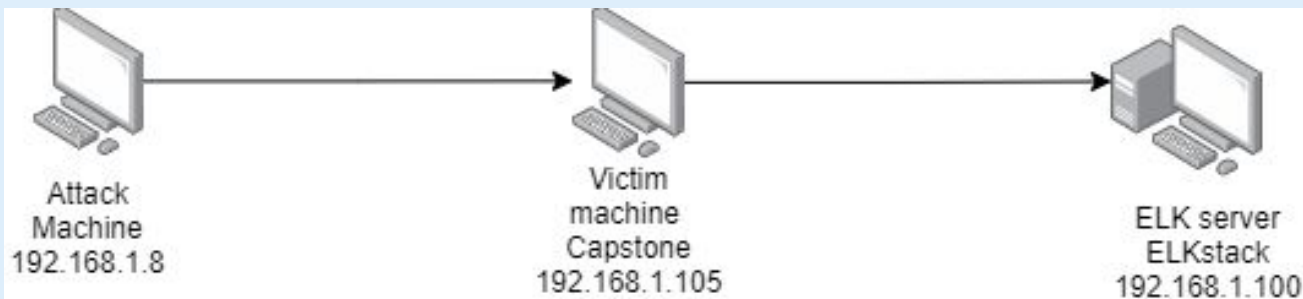
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address

Range: 192.168.1.1/225

Netmask: 255.255.240.0

Gateway: 10.0.0.1

Machines

IPv4: 192.168.1.100

OS: Windows

Hostname: ELK

IPv4: 192.168.1.8

OS: Linux

Hostname: Kali

IPv4: 192.168.1.105

OS: Linux

Hostname: Capstone

IPv4: 192.168.1.1

OS: windows

Hostname: Red vs Blue

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue	192.168.1.1	View logs
Kali	192.168.1.8	Attack Machine
Capstone	192.168.1.105	Victim machine
ELK	192.168.1.100	Activity logging from Capstone

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 is open	Leaving port open can allow attackers to access the system	Attackers can gain access to your data and also make changes.
Brute force attack capability	Attackers can guess passwords without a limit.	Attackers can login in using someone else's credentials and gain access to data.
Saving password hash	Once a hash is generated for a password it should not be saved, if it is attackers can gain access to and try to crack the password.	Attackers can login in using someone else's credentials and gain access to data.

Exploitation: [Port 80 open]

01

Tools & Processes

Used nmap to scan for any open ports.

02

Achievements

Found that port 80 was open in IP address 192.168.1.105

03

Nmap 192.168.1.0/24

Exploitation: [Brute force password]

01

Tools & Processes

Used Hydra to brute force a user's password.

02

Achievements

Using the username and password we were able to log in to the victim's machine.

03

```
hydra -l ryan -P  
rockyou.txt.gz -s 4444 -f -vV  
192.168.1.105 http-get  
/company_folder/secret_fold  
er
```

Exploitation: [Saving hashed password]

01

Tools & Processes

Used online hash cracker tool.

02

Achievements

Since the hashed password was saved we were able to crack that and logged in the victim machine using that username and password

03

md5 cracker


Hashing > precalculated md5 hashes

d7dad0a5cd7c8376eeb50d69b3ccd352

Search

[↑ Top] [↓ Bottom]

Text	Hash
linux4u	d7dad0a5cd7c8376eeb50d69b3ccd352



Blue Team

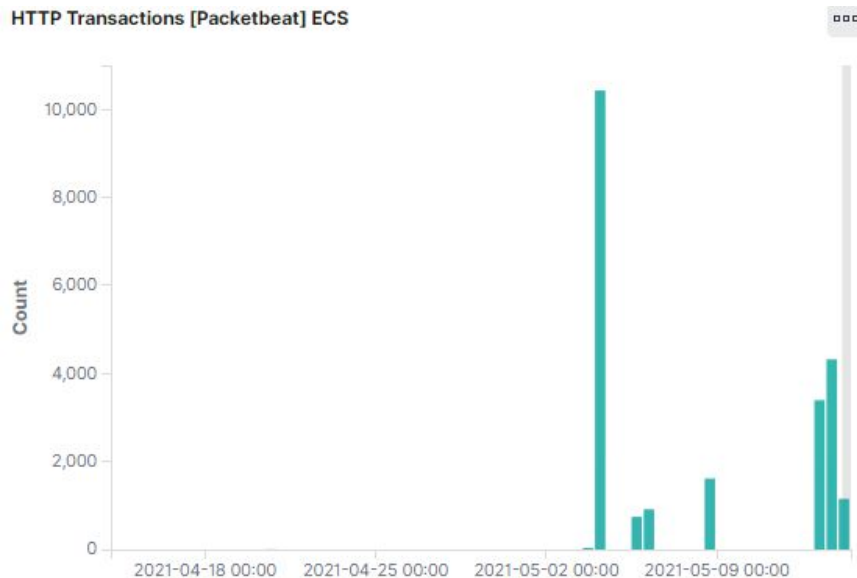
Log Analysis and Attack Characterization

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.



- Port scans began around midnight.
- 12,508 scans from 192.168.1.10
- nmap sends ping to the ports.

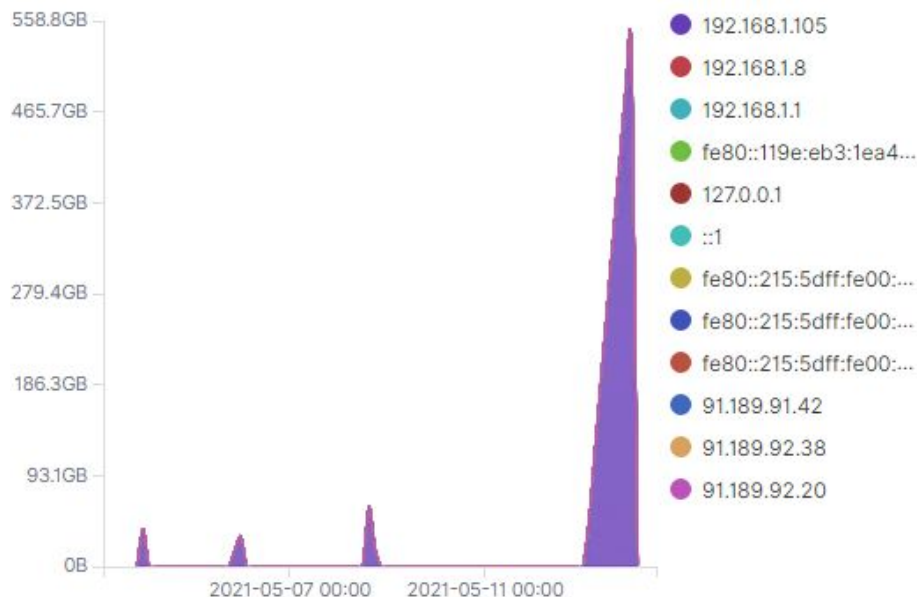


Analysis: Finding the Request for the Hidden Directory

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



- Request occurred around 3 am and the count was 9,978
- Files in secret_folder were requested which contained password hashes.

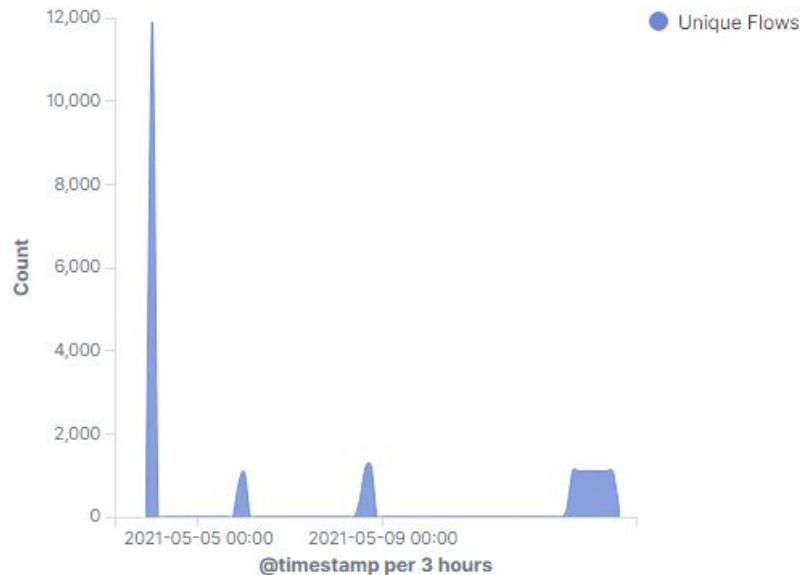


Analysis: Uncovering the Brute Force Attack

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



- 11,906 requests were made before the attacker found 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.



- 27 requests were made to this directory
- shell.php file was requested.

url.full: Descending ▾	Count ▾
http://127.0.0.1/server-status?auto=	12,508
http://192.168.1.105/company_folders/secret_folder	9,978
http://192.168.1.105/webdav/shell.php	27
http://192.168.1.105/	14
http://192.168.1.105/company_folders/	13



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We can set a firewall alarm that alerts us if ports are scanned.

We would set an alarm if the firewall detects more than 10 port scans per minute.

System Hardening

Whitelist IP addresses.

Only allow authorized IP addresses to access the system and block the rest.

Mitigation: Finding the Request for the Hidden Directory

Alarm

We can set an alarm that watches for machines that access the specified directory/file.

We can set the alarm so that it alerts us when the directory/file is accessed by an unauthorized machine.

System Hardening

We can remove the file from the server.

We can move it to a safer location or an offline location.

Mitigation: Preventing Brute Force Attacks

Alarm

We can set an alarm that watches for unsuccessful login attempts

We should limit unsuccessful login attempts to 10.

System Hardening

After the threshold is reached we can block the offending IP.

Mitigation: Detecting the WebDAV Connection

Alarm

We can create an alarm that watches when this directory is accessed by unauthorized user.

We can have this alarm alert us when more than 1 attempt is made to access this directory

System Hardening

We can restrict access to this folder by machine.

We can have 2 factor authorization to access this directory and one of which can be using the authorized machine.

Mitigation: Identifying Reverse Shell Uploads

Alarm

We can set an alarm to alert us when a .php file is uploaded to the server.

Threshold should be for any attempt to download/upload .php file to the server.

System Hardening

We can make this directory read only.

We can restrict access for anyone to upload files to this directory over the web interface.

*The
End*