Capstone Engagement

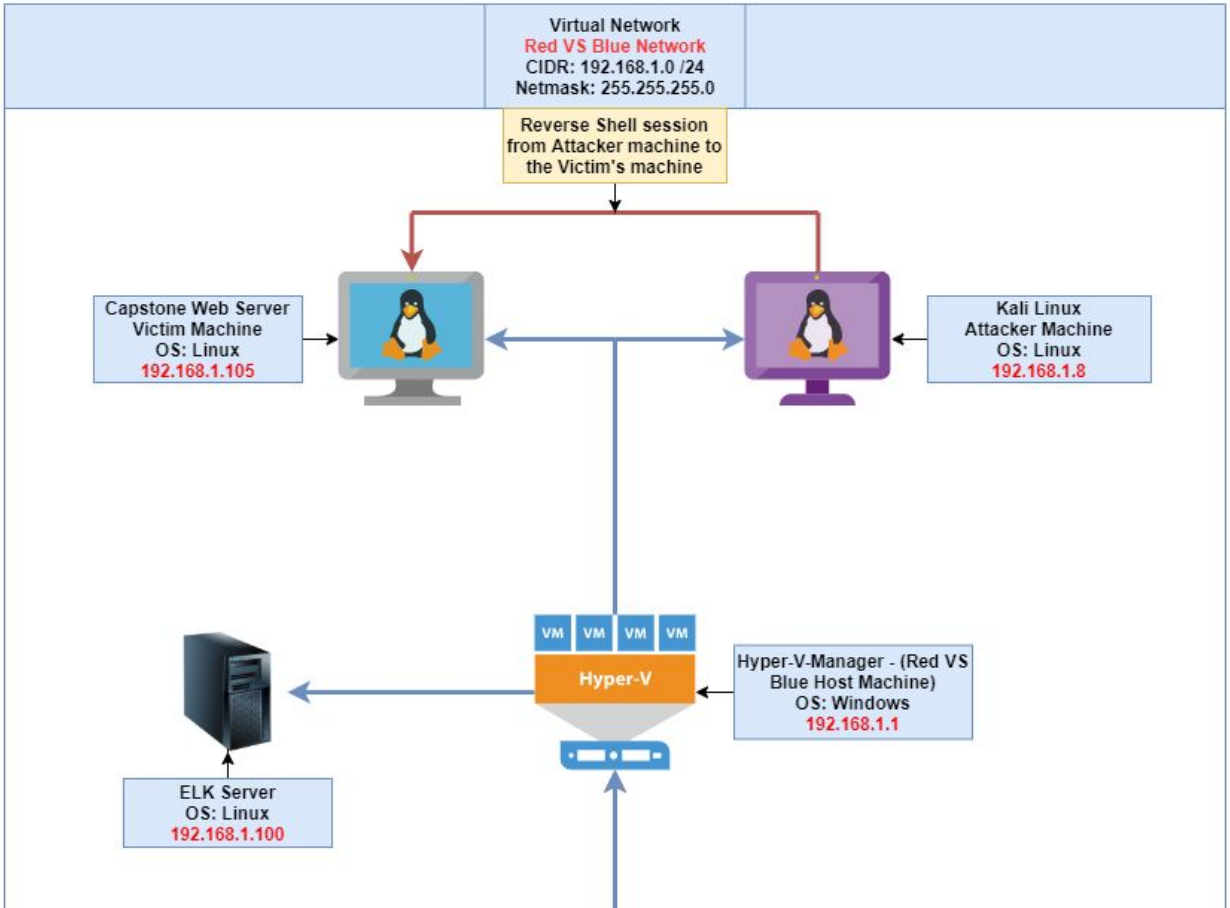
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.1 - 192.168.1.254
CIDR: 192.168.1.0 /24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Red Vs Blue

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

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	This is the VM that is running Hyper-V-Manager, allowing us to access the Capstone and Kali machines.
ELK Stack Machine	192.168.1.100	This machine is the ELK Stack (Elastic search, Logstash and Kibana) that collects the logs, sorts them and displays them in Kibana.
Kali	192.168.1.8	This is the attacker machine that I used to run all exploits against the Capstone machine.
Capstone	192.168.1.105	This is the vulnerable machine I ran all exploits against and had some fun while doing it.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Exploitation: Terrible Website Security (CWE-23: Relative Path Traversal)	This exploit did not require any tools. The “web devs” left an easter egg in file1.txt that there is a hidden directory called /secret_folder/….terrible web security!	If the web dev team did not leave this easter egg, then I could have just used a tool like dirb to find the hidden directory, but by having this hidden directory they are setting themselves up to be attacked.
Exploitation: Hydra Brute Force Attack (CVE-2021-XXXX)	This exploit I used the hydra command to launch a Brute Force Attack on the site for the credentials to login into the /secret_folder/ directory.	This allowed me to obtain the credentials to login into the /secret_folder/, which ultimately allowed me to launching an attack on the site via a reverse shell.
Exploitation: Reverse Shell (CVE-2019-13386)	This exploit allows a user to execute a reverse shell with user privileges.	This is a catastrophic vulnerability for an organization or website, every piece of data is at risk, all user credentials are at risk and even the website is at risk because an attack can encrypt all files and shut the website down.

Exploitation: Terrible Website Security (CWE-23: Relative Path Traversal)

01

Tools & Processes

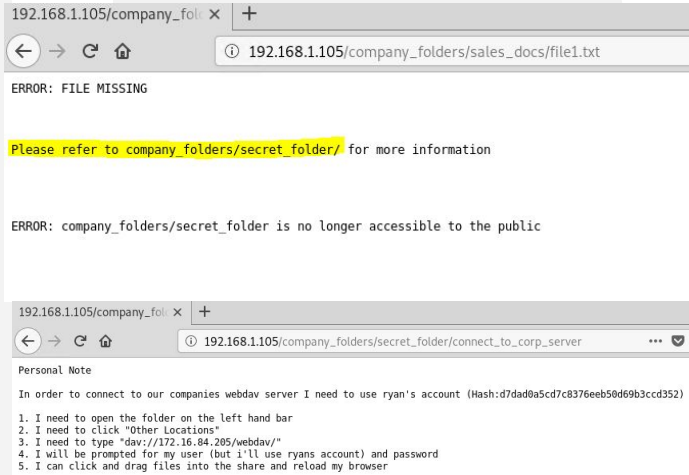
Answer: No tools were needed to find this exploit. While navigating around the site I clicked on file1.txt and the output referred to a /secret_folder/ for more information. This was deliberately referring to a directory that a normal user should not be able to access and how to navigate to the directory.

02

Achievements

Answer: This exploit led me to navigate to the /secret_folder/ which then led me to find the /webdav/ directory, where I could ultimately launch my attack.

03



Exploitation: Hydra Brute Force Attack (CVE-2021-XXXX)

01

Tools & Processes

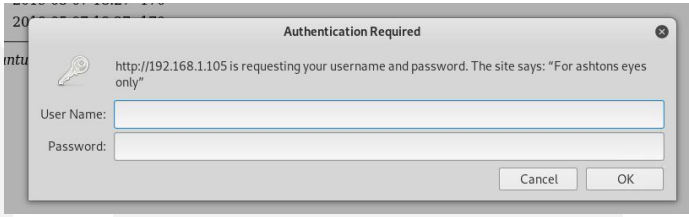
Answer: The tool that I used to achieve this vulnerability was Hydra. Hydra uses a wordlist, username, victim's IP address and a specified port to crack a password.

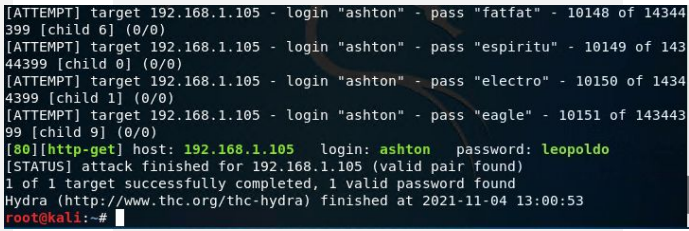
02

Achievements

Answer: With this exploit I was able to obtain the password for the user Ashton and from there I was able to login into the /secret_folder/ directory that was found on the site. Once I was in the /secret_folder/ directory I was shown a series of instructions to access the /webdav/ directory as well as a password hash to crack to gain access to the directory.

03





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

Exploitation: Reverse Shell (CVE-2019-13386)

01

Answer: The last exploit was establishing a meterpreter session on the site with a reverse shell. This way a 2 step process. First we accessed the /webdav/ directory that we cracked the password hash for in the previous step. Once we accessed the /webdav/ directory we uploaded a script file to activate the revershell once it has been opened. Second we set up our Kali machine to wait and listen on port 4444 for the file to be opened. Once the file was opened we achieved a reverse shell into the site.

02

Achievements

Answer: This exploit was the holy grail of the exercise. We gained full access to the site and user access to all of its files. This allowed us to find the Flag on the site in order to “Capture the Flag”.

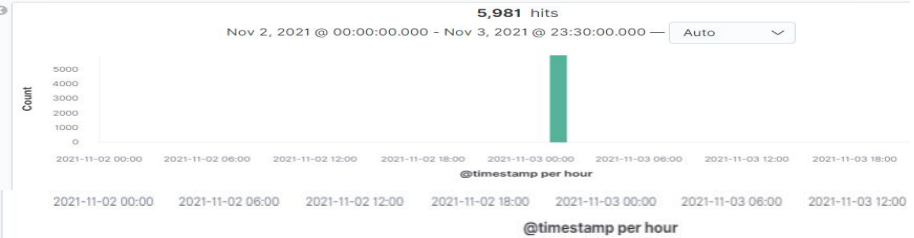
03

Blue Team
Log Analysis and Attack Characterization

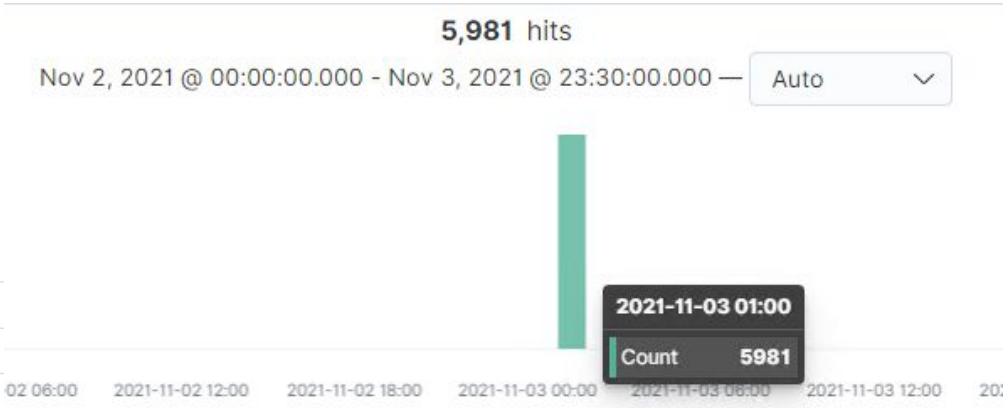
Analysis: Identifying the Port Scan

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?



Time	destination.port
Nov 3, 2021 @ 01:49:20.001	113
Nov 3, 2021 @ 01:49:20.001	445
Nov 3, 2021 @ 01:49:20.001	111
Nov 3, 2021 @ 01:49:20.001	3389
Nov 3, 2021 @ 01:49:20.001	135
Nov 3, 2021 @ 01:49:20.001	1720
Nov 3, 2021 @ 01:49:20.001	1025
Nov 3, 2021 @ 01:49:20.001	22
Nov 3, 2021 @ 01:49:20.001	139
Nov 3, 2021 @ 01:49:20.001	8888
Nov 3, 2021 @ 01:49:20.001	199



Analysis: Finding the Request for the Hidden Directory

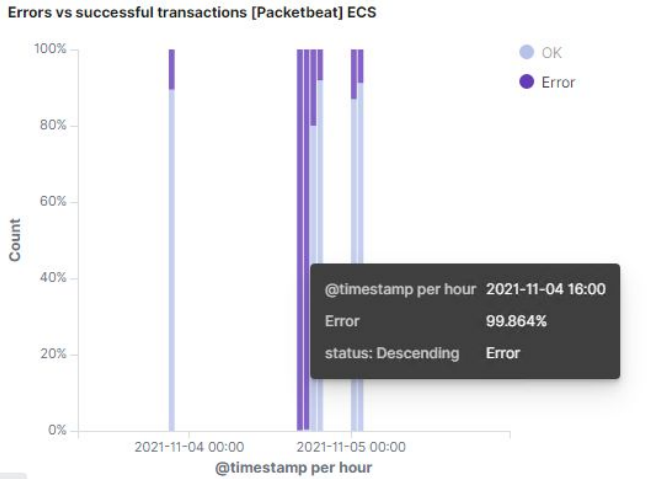
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

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

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	10,034
http://192.168.1.105/webdav/shell.php	197
http://192.168.1.105/webdav	86
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/webdav/shell1.php	10

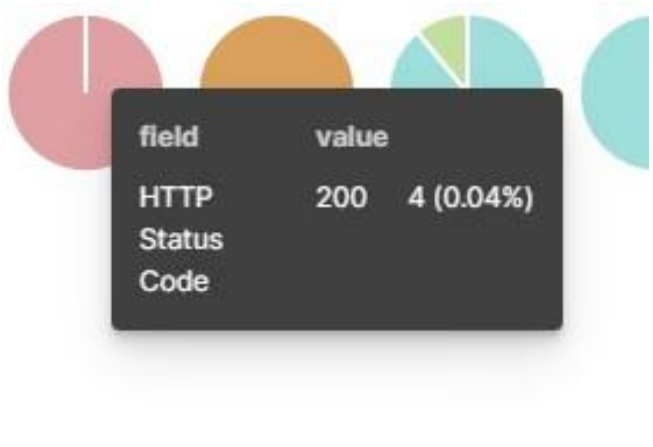
Export: Raw Formatted



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?



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?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	10,034
http://192.168.1.105/webdav/shell.php	197
http://192.168.1.105/webdav	86
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/webdav/shell1.php	10

Export: Raw Formatted

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?
Answer: An alarm that can detect future port scans with NMAP needs to be able to identify when SYN-SYN/ACK-RST packets are occurring regularly, because this is a tall tail sign of a port scan. Once, a system identifies that a client is running through different ports and dropping all packets after SYN/ACK in the three-way handshake, then the system can drop all packets from this client.

What threshold would you set to activate this alarm?
Answer: For a system to properly detect a NMAP port scan, a good threshold of 50-100 SYN-SYN/ACK-RST occurrences in 1 hour is a good threshold to start with.

System Hardening

What configurations can be set on the host to mitigate port scans?
Answer: Mitigating simple “loud” port scans that are dropping TCP packets after SYN/ACK are simple, create a firewall rule to drop clients that are continuously not completing the TCP three-way handshake on multiple ports in a short amount of time. As I said in the alarm threshold section 50-100 RST’s on different ports is a good start and work up or down from there based on the amount of alerts. *I continue below with more details to my explanation.*

Describe the solution. If possible, provide required command lines.
Answer: Simply add a firewall rule to drop clients that are continuously not finishing the three-way TCP handshake with the threshold of 50-100 RST’s occurring on different ports in a 1 hour time frame.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Answer: An alarm that can be set to detect this unauthorized access is a firewall rule that alerts the system admins anytime a non-authorized (Not whitelisted) IP address attempts to accesses the /secret_folder/.

What threshold would you set to activate this alarm?
Answer: As long as only the authorized IP addresses will have access to this directory the threshold would be 1 time. Since, no one other than the authorized IP addresses should have access to the directory. An alert should be sent if any other IP addresses accesses the folder.

System Hardening

What configuration can be set on the host to block unwanted access?
Answer: A configuration that can be set on the host to block unwanted traffic is to whitelist only internal IP addresses that should have access to the /secret_folder/ directory. Blocking all other unwanted access. With that being said, the best solution would be to delete the /secret_folder/ all together.

Describe the solution. If possible, provide required command lines.
Answer: To add a whitelist for IP addresses a firewall must be in place in order to program the firewall. Then you can program the firewall to only allow specific IP addresses into the directory and block all other IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Answer: An alarm to detect a Brute Force attack could be an alert that watches for more than 10 packets for a single user that have a 400 response code in 1 hour. This would mean someone has messed up their own password 10 times in a row in 1 hour or someone is trying to access a user's account maliciously.

What threshold would you set to activate this alarm?
Answer: The threshold is the toughest part, since it's different for every organization. For this scenario, starting with a threshold of 10, then working down or up depending on the number of alerts being received by the system admins is the safest way to play this threshold.

System Hardening

What configuration can be set on the host to block brute force attacks?
Answer: With our alarm watching for 400 response codes with a threshold of 10 times per hour. After a user or attacker uses up the 10 attempts in 1 hour a system admin will be notified to contact the user. The users account will also be locked until the system admin makes contact with the employee and determines if it is an attack or forgotten password.

Describe the solution. If possible, provide the required command line(s).
Answer: The solution would be to lock the users account until the system admin determines if it was an attack or a case of forgotten password and unlocks the account to be logged into.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Answer: An alarm can be set to alert the system admins if a client tried to access the /webdav/ directory from NOT an internal IP address that is authorized (Whitelisted) to access the directory.

What threshold would you set to activate this alarm?
Answer: The threshold similar to accessing the /secret_folder/ would be 1 time. If anyone from an unauthorized IP address is attempting or already has access the /webdav/ directory, there is a problem.

System Hardening

What configuration can be set on the host to control access?
Answer :The best way to mitigate a client/attacker from accessing the /webdav/ directory is to not allow remote access to the directory over the web. This way only internal systems can access and make changes to the directory.

Describe the solution. If possible, provide the required command line(s).
Answer: To implement this solution the System admin team would have to block all connection over the internet via a firewall. Then create a white list of internal IP addresses that can access the server for the system admins to maintain the server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Answer: An alarm to detect a client trying to upload a reverse shell script can be set to alert all system admins if any file is being uploaded to the site and specifically the /webdav/ directory. This way any file being uploaded to the site will be looked at immediately.

What threshold would you set to activate this alarm?
Answer: The threshold I would use would be 1. If 1 file is uploaded to the /webdav/ file or anywhere on the website from a client the system admins will be notified.

System Hardening

What configuration can be set on the host to block file uploads?
Answer: The best way to mitigate this type of attack is block all clients and users other than the internal system admins from uploading any files to the site. And/Or you can change the /webdav/ directory to not allow script execution in order to still allow file upload, but stop malicious executables from running. But this can be tricky and abused by an attacker.

Describe the solution. If possible, provide the required command line.
Answer: To implement the blocking all files from being uploaded, simply add this security feature into the website and all clients will not be able to upload any files into the site.


The End