Capstone Engagement

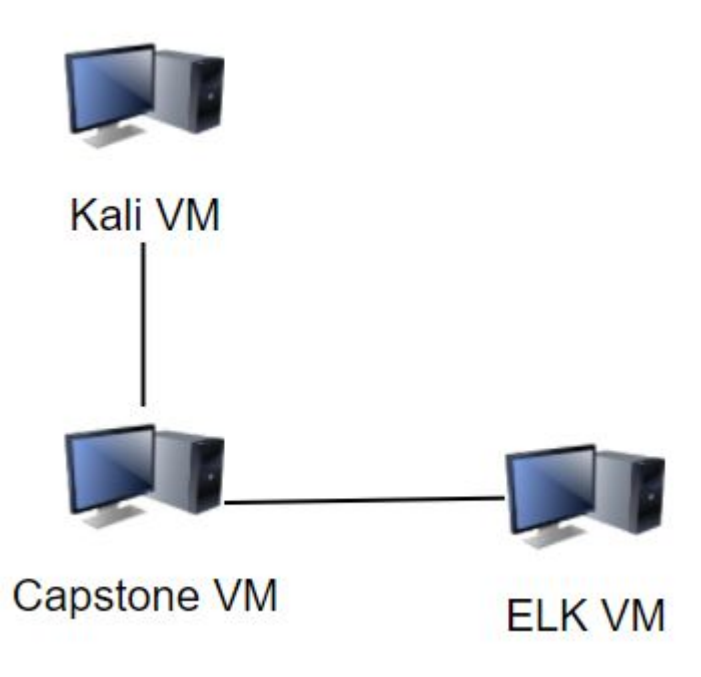
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
IP Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali
Purpose: Attack Machine

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK
Purpose: Logging Machine

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
<N/A>	192.168.1.1	Gateway
Kali	192.168.1.90	Used to analyze network and machines on network
ELK	192.168.1.100	Network and system data collector and analyzer
Capstone	192.168.1.105	Web Server

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.*
Sensitive Data Exposure (#3 in OWASP Top 10 for 2017)	Data can be accessed without any authentication measures	In the case of the Capstone server, the data compromised the credentials of the WebDAV folder
Unauthorized File Upload	Users can upload arbitrary files	The server is exposed to any manner of malicious file
Remote Code Execution (#1 in OWASP Top 10 for 2017)	Attackers can execute shells and other arbitrary code remotely	The PHP uploaded and executed can do any manner of harm to the server as well as allow unrestricted data access

Exploitation: Sensitive Data Exposure

01

Tools & Processes

Used “nmap” to find the server and determine that port 80 was open. Used “dirb” to map the URLs. Used a browser to explore the server directories.

02

Achievements

The exploit found the “secret_folder” server folder. Navigating to “company_folders/secret_folder” opened up a authentication pop-up that indicated the user was “ashton”. Used this to brute-force the password.

03

After using “hydra” to brute force the password, gained the following password: “leopoldo”.

Exploitation: Unauthorized File Upload

01

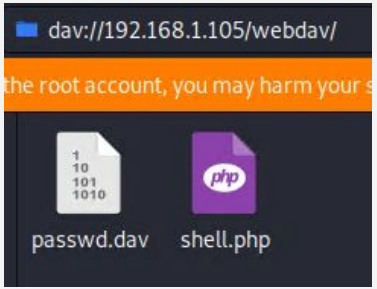
Tools & Processes
Found the “connect_to_corp_server” file which gave use the “WebDAV” folder plus the user and password hash for user “ryan”. Used “john the ripper” to crack the password hash.

02

Achievements
Since we had the username and password, we uploaded our PHP shell code to the server using WebDAV.

03

Here’s a screenshot of the shell uploaded to the server:



Exploitation: Remote Code Execution

01

Tools & Processes

Generated a remote shell file using “msfvenom”. Uploaded the shell file using the WebDAV. Set up a listener in “Metasploit”. From the browser, executed the shell on the web server which connected to the listener.

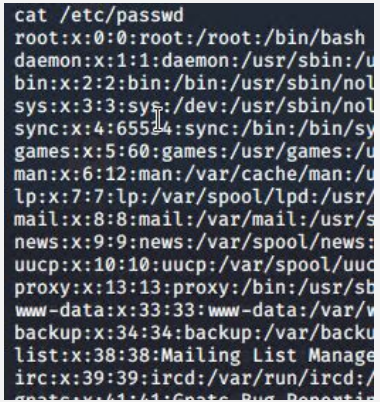
02

Achievements

The shell allowed us to execute arbitrary commands on the web server.

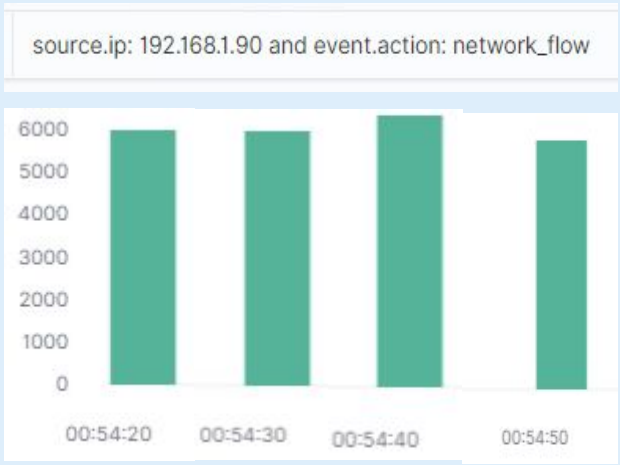
03

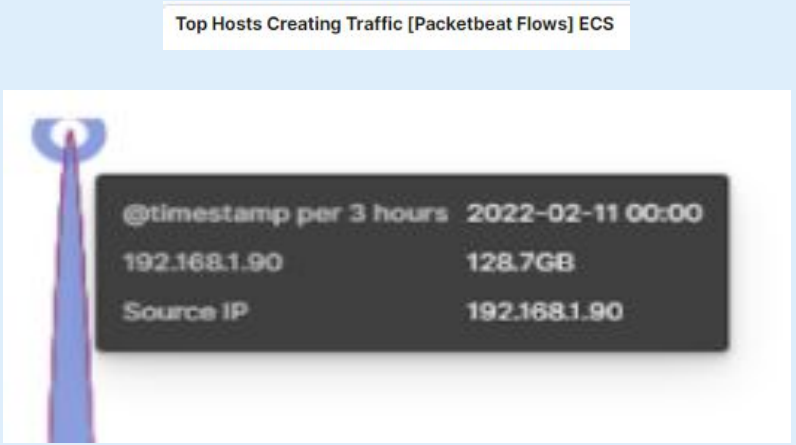
Here’s a screenshot of the shell executing “cat /etc/passwd”:



Blue Team
Log Analysis and Attack Characterization

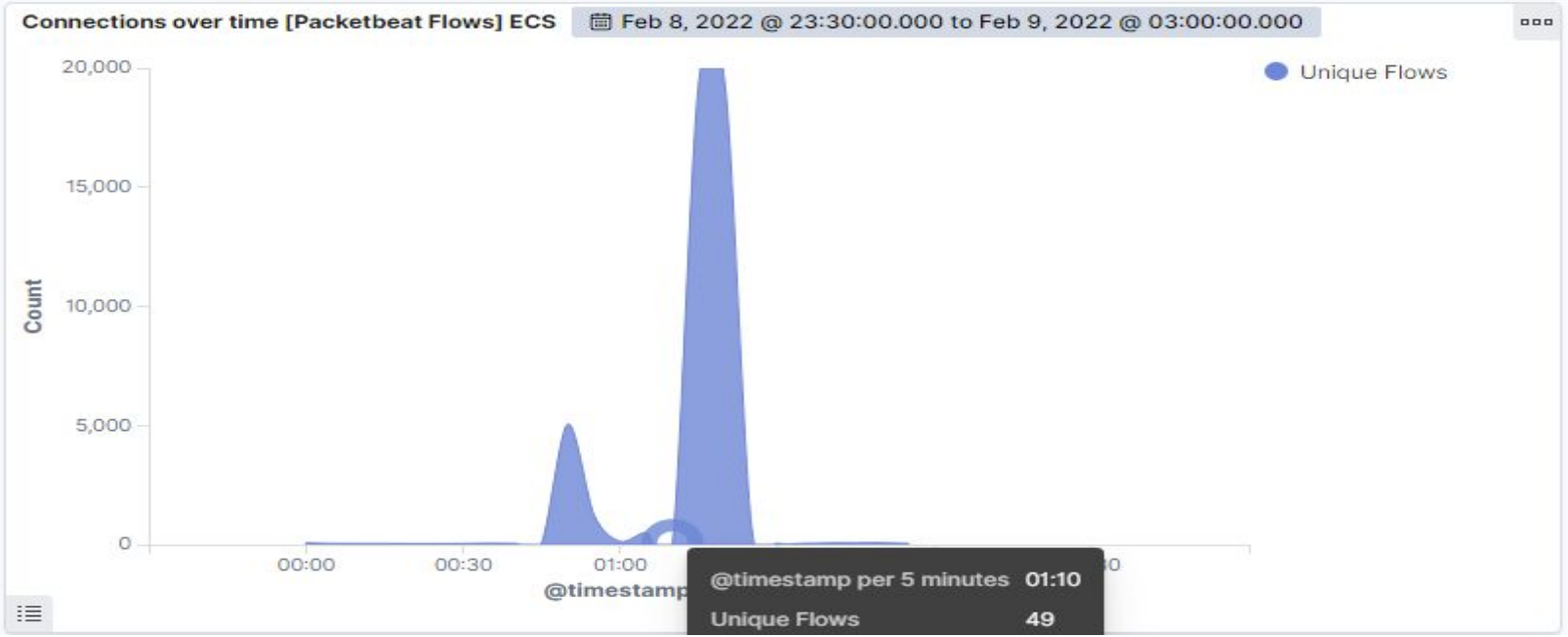
Analysis: Identifying the Port Scan





- The port scan occurred at roughly 12:54 AM on 2/9/22
- Roughly 25,000 packets were sent from 192.168.1.90.
- Indicators this was a port scan
    - See the first screenshot above. The Packetbeat search shows the “network_flow” packets captured at the time mentioned.
    - See the above screenshot that tracks the top hosts creating network traffic.

Analysis: Finding the Request for the Hidden Directory



- The request for the “secret_folder” started at around 1:10 AM on 2/9/22. There were a trivial amount of requests as the user was likely simply manually clicking and searching for sensitive data.
- Which files were requested? What did they contain?

Analysis: Uncovering the Brute Force Attack

- From the above screenshot, you can tell that 30K+ requests were made in the brute force attack. The 401 status code indicates that the attacker is trying numerous password attempts that are failing.

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	31,198
http://127.0.0.1/server-status?auto=	695
http://192.168.1.105/webdav	97
http://192.168.1.105/webdav/shell.php	66
http://ocsp.pki.goog/gts1c3	20

- From the above screenshot, we can see that the attacker used the WebDAV directory to not only get data – the password hash for the user “ryan” – but they used it to upload the PHP reverse shell.

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?

- We could set an alarm that monitors the number of requests per second. This could be done in the SIEM section of ELK.

What threshold would you set to activate this alarm?

- You could alert after a host receives greater than 25 requests in a second for more than 5 seconds.

System Hardening

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

- You could configure only certain IPs that are allowed to communicate with the host.
- You could throttle incoming connections. However, “nmap” can usually account for this.
- You could allow only certain IPs to use ICMP – ICMP filtering.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Set authorized IPs to the directory.
- Set an alarm to trigger when an unauthorized IP attempts to connect to the directory.

What threshold would you set to activate this alarm?

- The alarm will trigger on the first occurrence.

System Hardening

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

- Encrypt the sensitive data inside the directory.
- Use Linux's user system to restrict access to only specific users. However, this doesn't protect against the user getting compromised.
- Remove the directory from any public-facing web application. Only allow access to data from the local host.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Like the port scan alarm, we could set an alarm that monitors the number of requests per second.

What threshold would you set to activate this alarm?

- The same port scan criteria alert after a host receives greater than 25 requests in a second for more than 5 seconds – would catch this as well.

System Hardening

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

- Implement “fail2ban” which scans logs and bans IPs that show signs of malicious requests.
- Implement a solution that prevents IPs from attempting authentication – for WebDAV – for a given period of time after a small number of failed attempts.
- Configure WebDAV to only authentication from certain IPs

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Any access to WebDAV directories.

What threshold would you set to activate this alarm?

- This would simply trigger when the WebDAV directories were accessed.

System Hardening

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

- Limit only certain IPs access to WebDAV directories.
- Disable WebDAV on the web server.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Since the shell was uploaded using WebDAV, that alarm would cover this vulnerability.
- Trigger an alarm if any non-web packets are spotted leaving the web server. The reverse shell typically communicates with an outside machine.

System Hardening

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

- Significantly restricting write permissions on the web server could help mitigate this risk.
- Restrict all outgoing network traffic on the web server except normal web traffic – ports 80 and 443.


The End