Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System.

Sam O.

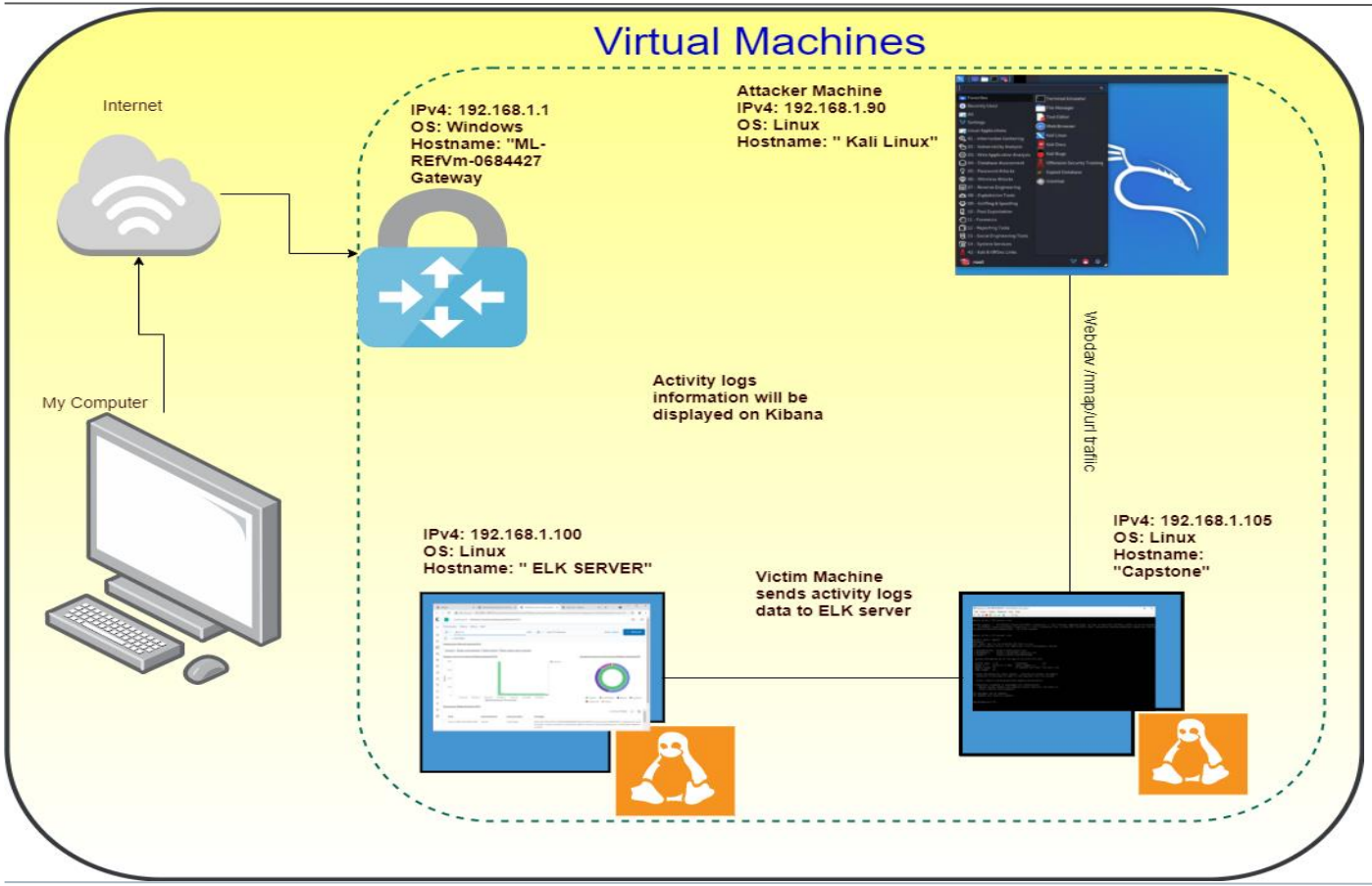
Suggested Time:

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



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

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: ML-REfVm-0684427

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	Captures log activity from Capstone Machine.
Capstone	192.169.1.105	Vulnerable Machine.
Red vs Blue ML-REfVm-0684427	192.168.1.1	Virtual Host Machine displaying Log activity on Kibana.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Port 80.	Attackers are able to access sensitive private information through open ports.	The red team was able to access company folders with secret files which had the hashed password.
Sensitive Data Exposure	Web applications and APIs do not protect sensitive data since the secret_folder is publicly accessible but contains sensitive data intended only for authorized personnel.	The exposure compromises credentials that attackers can use to break into the webserver. This vulnerability allowed the Red team to brute force and accessed unencrypted secret file information.
Unauthorized File Upload	Users are allowed to upload arbitrary files to the webserver.	This vulnerability allows attackers to upload PHP scripts to the server.
Remote Code Execution via Command Injection	Attackers can use PHP scripts to execute arbitrary shell commands.	The vulnerability allows attackers to open a reverse shell to the servers.

Exploitation: Open Port 80

01

Tools & Processes

- **We used nmap** to scan the network for open ports and other services.

Achievements

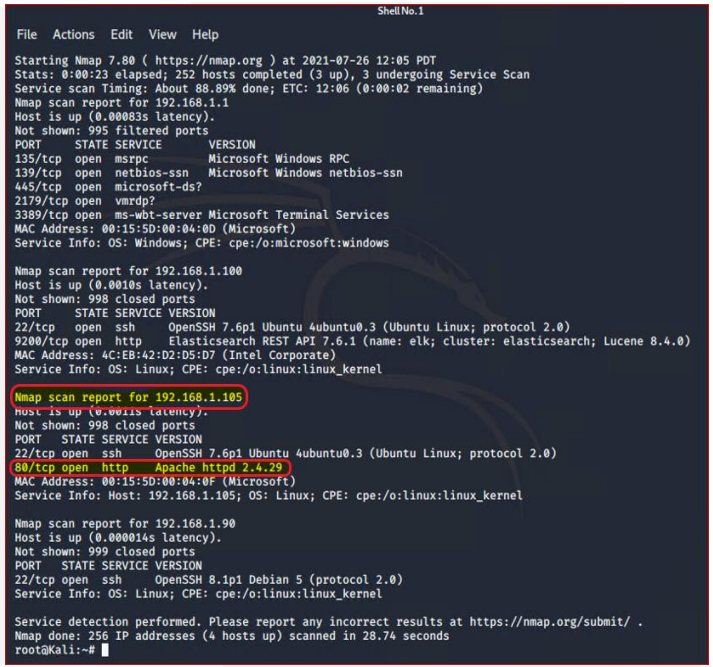
- The IP address 192.168.1.105 had an open port 80.
- The exploit revealed a **secret_folder** directory with important company files.

02

Exploitation

- This information is used to explorer the files and find out the user_name and the path of the secret folder.

03



Exploitation: Sensitive Data Exposure

01

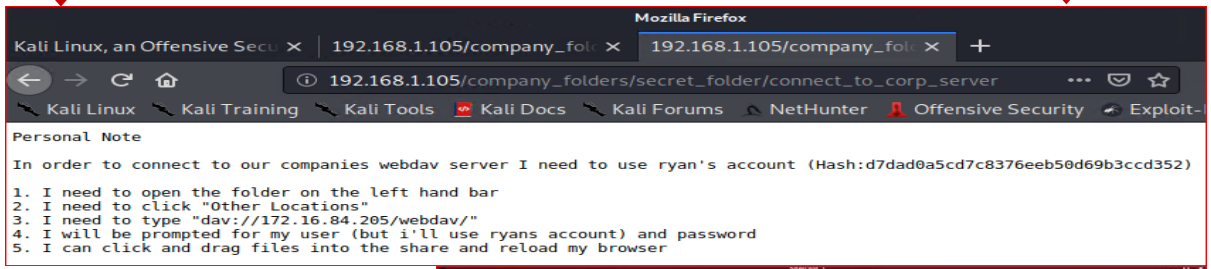
Tools & Processes

- **dirb** to map URLs
- Browser to explore
- Hydra to brute force and reveal user and password.

Achievements

- The exploit granted the Red team user shell access into the victim machine and revealed a **secret_folder** directory with secret files.

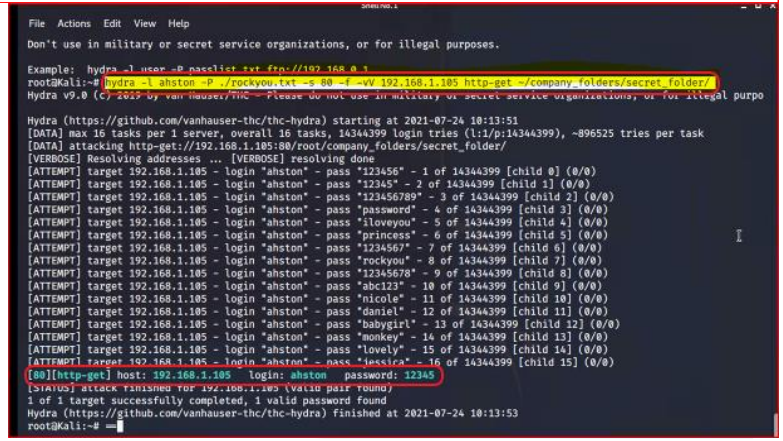
02



Exploitation

The login prompt reveals that the user is `ashton`.

03



Exploitation: Unauthorized File Upload

01

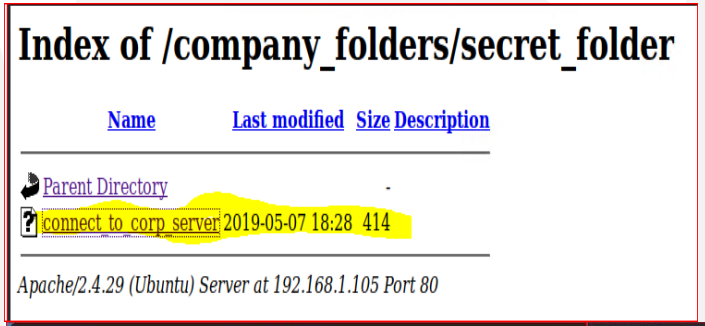
Tools & Processes

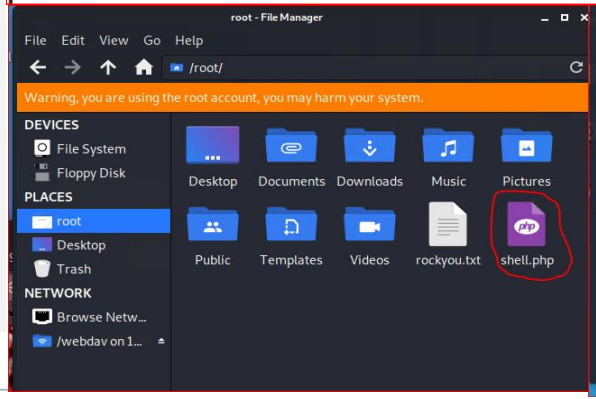
- Crack hash to connect via WebDAV
- Generate custom web shell with msfconsole
- Upload shell via WebDAV

Achievements

- Uploading a web shell allows us to execute **arbitrary shell commands** on the target

02

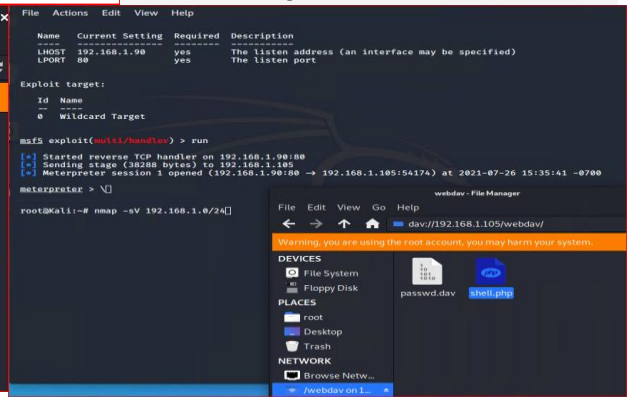




03

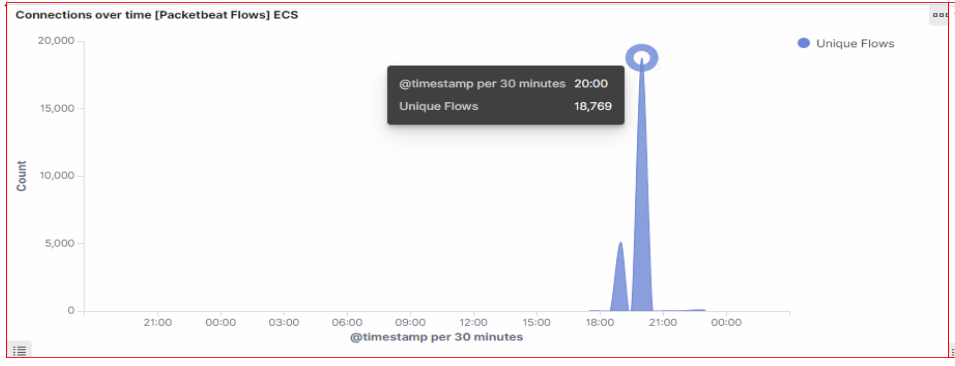
Aftermath

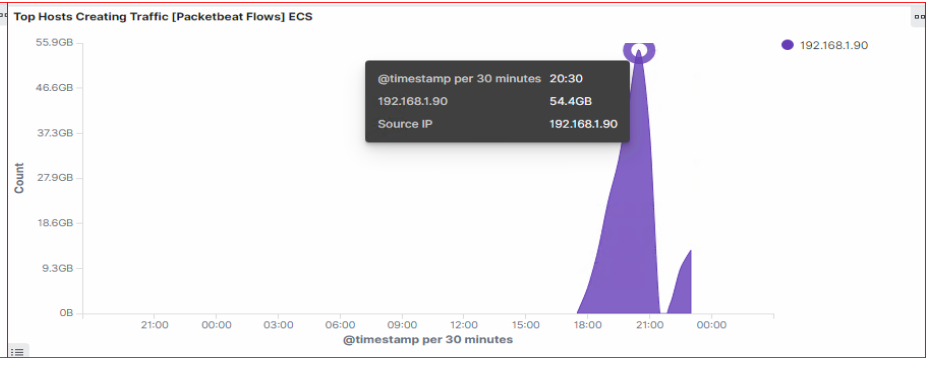
- Running arbitrary shell commands allows Meterpreter to open a full-fledged connection to the target



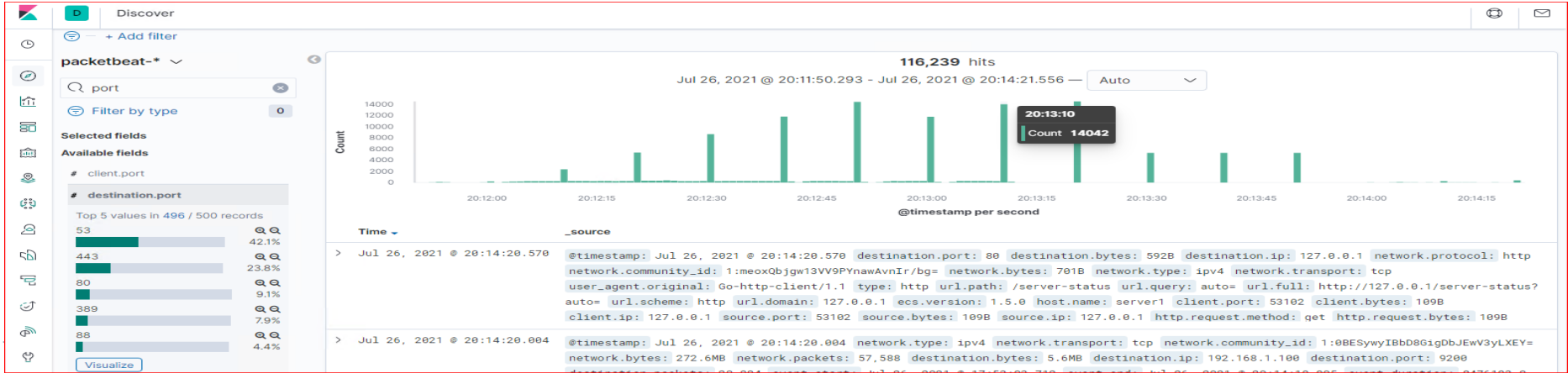
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





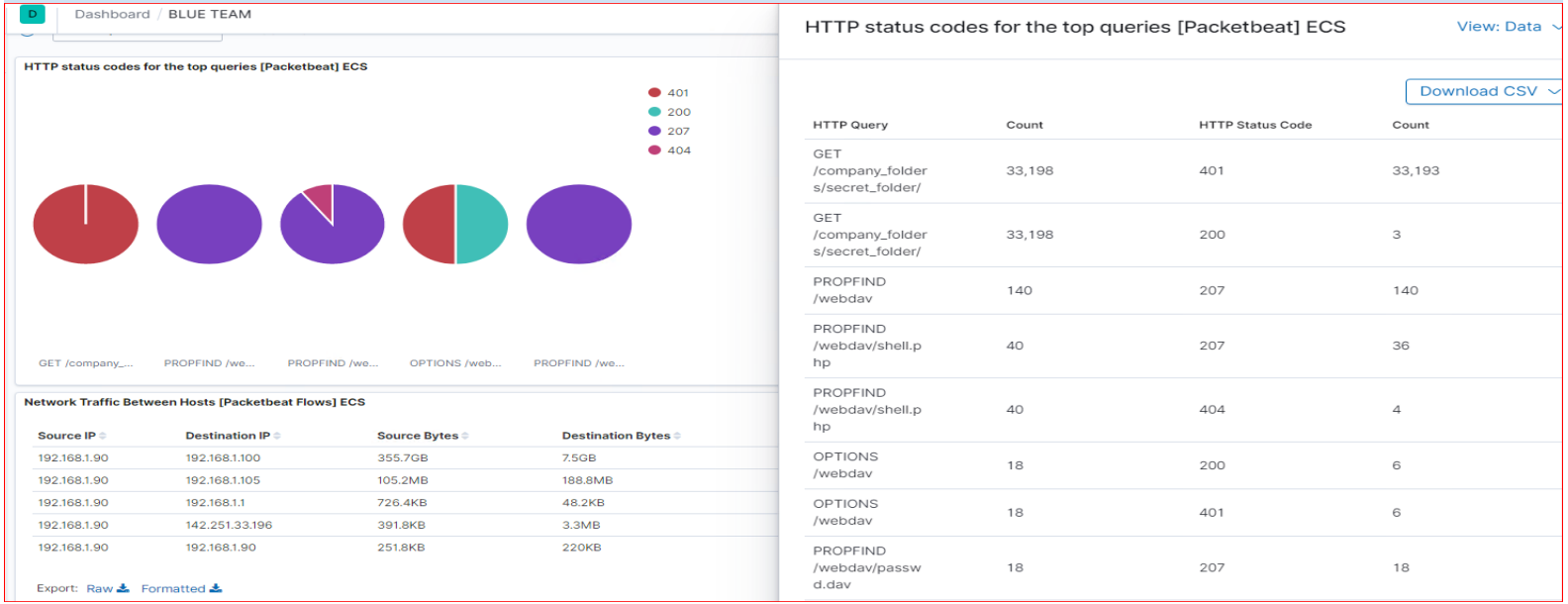
- Port scan began at 20:00 hours.
- 18,769 hits from the source IP 192.168.1.90. as indicated on the second chart.
- We have 496 port scaned in one minute and 30 seconds which is a port scan.



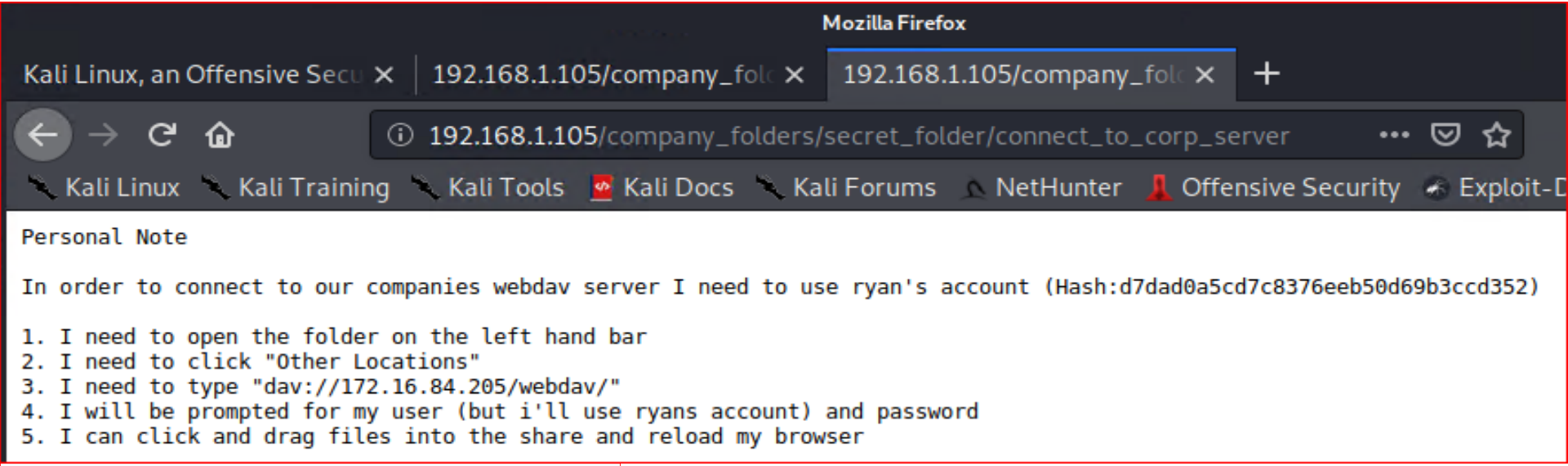
Analysis: Identifying the Port Scan (cont.)

What responses did the victim respond back with?

As indicated on the chart, the victim responded back with 401 (Unauthorized), 207 (Multi-Status), 200 (OK), and 404 (Not found) responses.



Analysis: Finding the Request for the Hidden Directory



- The attack started at 20:30 with 16,403 requests on the hidden directory.
- The files in the secret folder hidden in the company folder were of the interest .
  - http://192.168.1.105/company_folder/secret_folder
  - http://192.168.1.105/webdav/passwd.dav
  - http://192.168.1.105/webdav/shell.php
- The secret folder had a file with hashed password and contained Instructions on how to access WebDAV server by using Ryan's password.

.

Analysis: Uncovering the Brute Force Attack

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	33,198
http://192.168.1.105/webdav	18
http://192.168.1.105/	12
http://192.168.1.105/webdav/shell.php	10
http://192.168.1.105/company_folders/secret_folder	8

Export: Raw Formatted

server.ip	192.168.1.105
server.port	80
source.bytes	164B
source.ip	192.168.1.90
source.port	44000
status	Error
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)

- 33,198 requests were made for the sensitive data indicating a brute force attack.
- The password-protected secret_folder was requested 33,198 times, but the file inside that directory was only requested 8 times. Out of 33,198 requests, only 8 were successful.

Analysis: Finding the WebDAV Connection

In the chart we observe that 18 requests were made to WebDav directory.

The shell.php file was requested 10 times by the attacker

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	33,198
http://192.168.1.105/webdav	18
http://192.168.1.105/	12
http://192.168.1.105/webdav/shell.php	10
http://192.168.1.105/company_folders/secret_folder	8

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?

- Set an alarm to fire when a firewall detects over 5 ports scans in 30 seconds from the same IP source.

What threshold would you set to activate this alarm?

- Alarms should fire if a given IP address sends more than 10 requests per second for more than 5 seconds
- Set an alarm to fire and drop large packets if the size of any inbound ICMP packet is larger than the threshold 1024 bytes.

System Hardening

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

- Install a Firewall to close all unnecessary ports. A firewall can also help prevent unauthorized access to your network.
- Filter ICMP ping traffic on the system.
- Enable TCP wrappers to allow IP address list and close the open, vulnerable ports.

> iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443 -j DROP

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Allow authorized IP addresses.
- Trigger alarm if an IP not on the allow list attempts to connect.

What threshold would you set to activate this alarm?

If the incoming IP is *not* allowed, it fires on a threshold of a single attempt.

System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.
- On the terminal run
- Delete the current hidden directory and create a new one offline.
- `rm -r ../company_files/secret_folder` from the server

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 error' is returned from any server that detects failed login attempts
- Also create an alert to detect the "hydra" string value by the user_agent.

What threshold would you set to activate this alarm?

- Set the account to lock after more than 3 failed login attempts for one hour.

System Hardening

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

- Configure `fail2ban<apt-get install fail2ban>` or a similar utility would mitigate brute force attacks.

[WebDAV] enabled = true filter = webdav action = iptables-multiport[name=webdav, port="http, https"] logpath=dav://192.168.1.105/webdav maxretry = 3 findtime = 600 bantime = 600

- Lockout accounts for 1 hour after 3 incorrect password attempts until manually unlocked by an administrator.
- Lockout an IP address with multiple failed logins.
- Prompt user to answer secret questions after 3 failed login attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Monitor access to WebDAV with Filebeat
- Fire an alarm on any read performed on files within WebDAV.

What threshold would you set to activate this alarm?

- Simply trigger the alarm whenever someone accesses the WebDAV directory.
- Preferably, allow only valid IP addresses.

System Hardening

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

- Administrators must install and configure Filebeat on the host.

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

limit WebDAV access to a limited number of users.

> nano /etc/httpd/conf/httpd.conf Locate directory section (/var/www/) and set it as follows:<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>

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarms should fire upon receipt of any POST request containing the form or file data of a disallowed file type, e.g., .php.

What threshold would you set to activate this alarm?

- The alarm should fire whenever users upload a forbidden file.

System Hardening

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

- Files upload to require authentication and write permissions can be restricted on the host.
- Uploads can be isolated into a dedicated storage partition not accessible from the web.
- Filebeat should be enabled and configured.
- - <Limit PUT POST DELETE PROPFIND PROPPATCH MKCOL COPY MOVE LOCK UNLOCK>

Conclusion

In this project, we have learned more about the current threats and how sophisticated modern techniques compromise credentials, apps, and data. To defend your organization against these new threats, the cybersecurity team must focus on protecting the company data and include continuous monitoring, pen-testing, detecting, and response. For that reason, the use of the Red and Blue Team becomes very important.


The End