Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

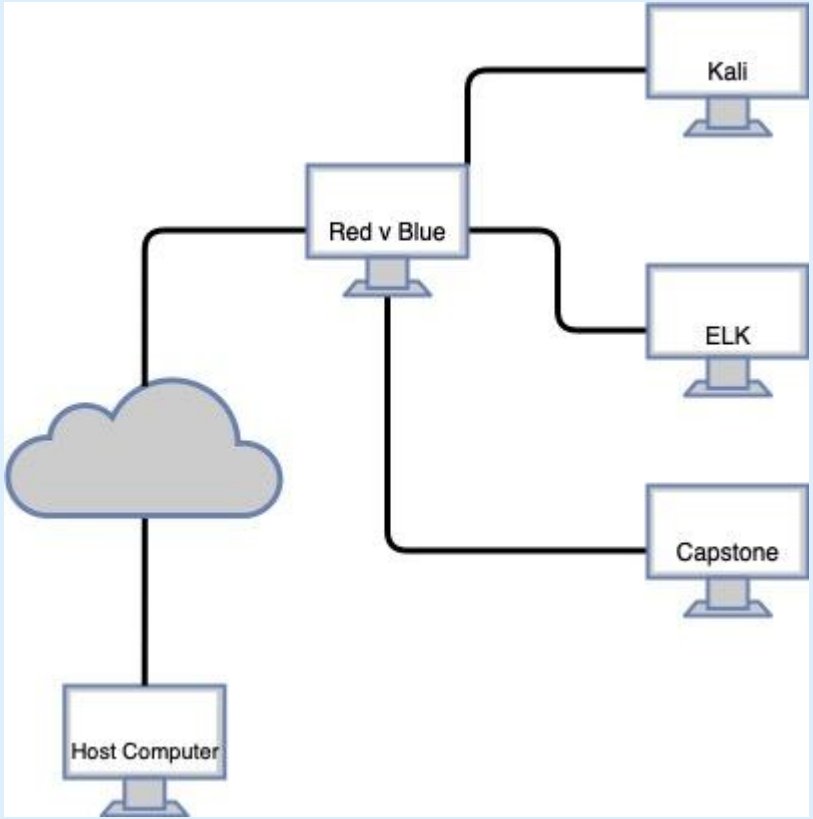
By Briana Norman

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: 192.168.1.1
OS: Windows
Hostname: Red V. Blue

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red v Blue	192.168.1.1	Gateway/Jumpbox
ELK	192.168.1.100	ELK server
Kali	192.168.1.90	Attacker machine
Capstone	192.168.1.105	Webserver/Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Password Policy (CWE-521) & Improper restriction of excessive authentication attempts (CWE-307)	CWE-521, This system does not require that users have strong passwords therefore making it easier for attackers to compromise user accounts. CWE-307, The software doesn't implement sufficient measures to prevent multiple failed authentication attempts within a short time frame.	The combination of the two vulnerabilities makes it sufficiently easier for the hacker to brute force and gain access to user accounts.
Improper limitation of a Pathname to a Restricted Directory (CWE-22)	The software uses an external input to construct a pathname that is intended to identify a file or directory located beneath a restricted parent directory. The software doesn't properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory	This vulnerability allows the hacker to directly locate the secret file by searching for it via the URL.
Local File Inclusion (CWE-98)	The PHP application receives input from an upstream component but it doesn't restrict the input before its usage.	Allows the upload of a reverse shell php which once uploaded and accessed, allows the hacker unrestricted access.

Exploitation: Weak Password Policy and Improper restriction of excessive authentication attempts

01

Tools & Processes

This vulnerability was exploited with the use of Hydra.

02

Achievements

The exploit was able to determine the correct user credentials to gain access to the secret folder directory within the company server.

03

Command used :
Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -fvV 192.168.1.105 http-get /company_folders/secret_folder

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (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 2022-05-02 19:48:38
root@Kali:~#
```

- End of the hydra output

Exploitation: Improper Limitation of a Pathname to a Restricted Directory

01

Tools & Processes

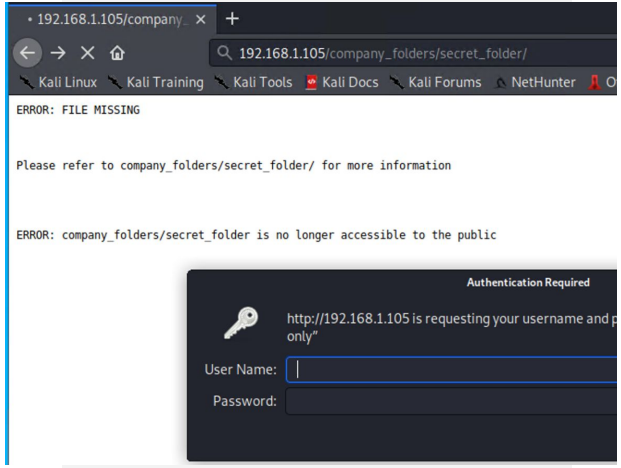
To exploit this vulnerability, attacker simply needs to enter the name of the specified files within the url of the application

02

Achievements

Grants access to the secret folder directory within the company folders

03



By Briana Norman

Exploitation: Local File Inclusion

01

Tools & Processes

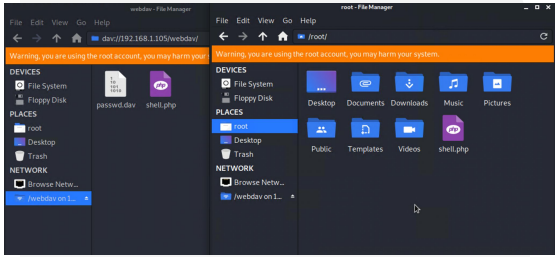
The exploit for this file was completed by simply dragging and dropping the shell payload onto the webDAV server

02

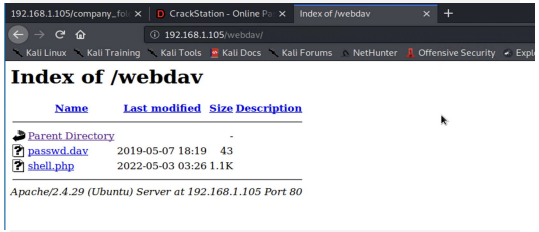
Achievements

The exploit successfully allowed a way to remotely connect to the server by uploading an executable file with the desired payload Local File Inclusion

03



- Click and drag

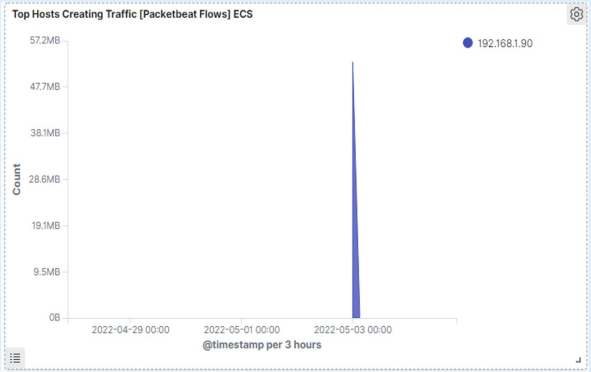


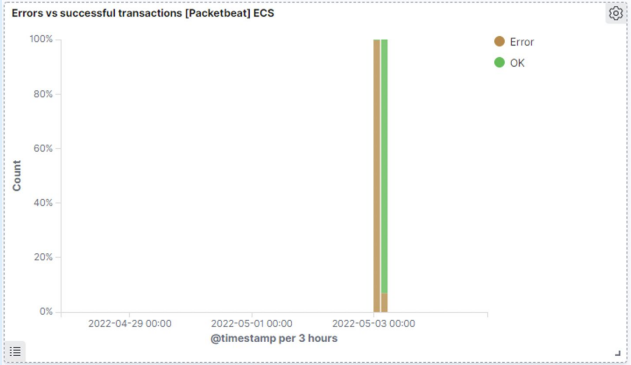
- Successful upload

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,518
http://192.168.1.105/webdav	160
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/company_folders/secret_folder/	7

- The port scan occurred 05/03/22, time 12:00 am
- Packets sent from machine IP 192.168.1.90, total packets sent 16,767 bytes from Kali linux
- Multiple packets sent to the webserver at the same time are indicative of a port scan

Analysis: Finding the Request for the Hidden Directory

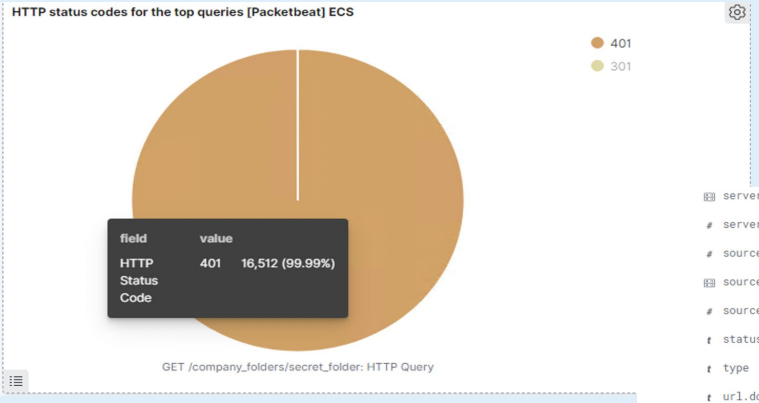
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,518
http://192.168.1.105/webdav	160
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/company_folders/secret_folder/	7

Export: Raw Formatted

- There were a total of 16,518 requests made for the hidden directory
- A file within the secret folder was accessed, information contained was pertaining to gaining access to the corporate server
    - File located within directory - connect_to_corp_server

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	16,518
http://192.168.1.105/webdav	160
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/company_folders/secret_folder/	7

Export: Raw Formatted

- 16,512 unsuccessful attempts before determining the password
- 16,518 attempts total

Analysis: Finding the WebDAV Connection

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,518
http://192.168.1.105/webdav	160
http://192.168.1.105/webdav/passwd.dav	42
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/company_folders/secret_folder/	7

- Total requests for the webdav directory - 160
- Files requested were shell.php (40) and passwd.dav (42)

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alarm can be can be set to count the number of requested ports for each source IP, when a threshold is reached, it would then trigger an alert for a potential port scan and notify a SOC analyst to further investigate

Search Criteria:
Destination.ip 192.168.1.105 and source.ip: (not 102.168.1.105) and destination.port: (not 443 or 80)

Report criteria:
Number of ports accessed per source IP per second

Alert Criteria/Threshold:
Alert email and log when > 4

System Hardening

- Host can install a firewall to prevent future port scans from occurring
  - Specified firewalls can be determined on base of need and function
- ignore/block the ICMP echo requests that are sent to the host server
  - Effectively ensures that the server is not responding to ping requests
- Block all incoming/outgoing connections to ports except 80 (HTTP) and 443 (HTTPS)
  - Can block, forward to honeypot or delay port scan

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alarm can be set to alert if any machine that is not on the authorized list tries to access the hidden directory

Search Criteria:
Source.ip: (not 192.168.1.105 or 192.168.1.1) and
url.path: *secret_folder*

Report Criteria:
Number of times “secret_folder” accessed from external IP

Alarm criteria/threshold:
Alert email and log when > 0 access is detected for “secret_folder” from IPs other than 192.168.1.1 and/or 192.168.1.105

System Hardening

- Host can remove the directory from the server and install a database that is a bit harder to exploit as long as the configurations are appropriately set
- MORE
- MORE
- MORE

Mitigation: Preventing Brute Force Attacks

Alarm

- Recommended to set an alarm for any time the user_agent.original is noted to be hydra within the Kibana logs
- As well as seven 401 HTTP responses have been returned from the server

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

Report Criteria:
Number of times error (401) response is detected in a 10 second interval

Alarm Criteria/threshold:
Alert email and log when, on protected files and folders, > 7 401 (Error) responses occur at any time OR any 200 (OK) responses occur from non-trusted IPs

System Hardening

- The system can be configured to block off any IP that triggers the alert by setting off the server to send more than seven 401 HTTP responses
- The rule can reset every day, therefore the block would only remain for 24 hours unless otherwise noted

Mitigation: Detecting the WebDAV Connection

Alarm

- An alarm can be set to to alert any time the directory is accessed from any machine that is not the authorized machine

Search Criteria:
Http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.1 or 192.168.1.105)

Report Criteria:
Number of times the directory is requested from non-trusted IPs

Alarm Criteria/threshold:
Alert email and log when requests are received for protected files and folders from non-trusted IPs

System Hardening

- Switch the server to a SQL database and would not need to protect a file from being accessed
- Block unwanted access to the “webdav” from any IP other than the ones specified by modifying the configuration file

Mitigation: Identifying Reverse Shell Uploads

Alarm

- design an alarm for any time a file is uploaded to the server from non-trusted IPs

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

****Reverse shell signature for detection of reverse shell detection****
Source.ip: 192.168.1.105 and destination.ip: (not 192.168.1.1 or 192.168.1.105) and destination.port > 0 and network.protocol: (not *) and http.response.body.bytes: (not *) and source.port: (not 80 or 22)

Report criteria
Count of “put” method from non-trusted IPs

Alarm criteria/threshold
Alert email and log when “put” request methods are made for protected folders sent from non-trusted IPs

System Hardening

- System configurations can be set to disable the uploading of files over the web interface from any IP other than the ones specified

the End