Mitigation: Blocking the Port Scan

Alarm

An alarm can be sent when nmap is located in the user.agent_original field to notify the system administrator when a port scan is occurring on the local network.

A threshold of 1 verified nmap user agent is sufficient from a non-whitelisted IP address.

An alarm can also be set when more than 500 connections are made within a 5 minute period.

System Hardening

Configure the network firewall to detect and respond to any port scan attempt in real time.

Conduct regular in-house port scans to ensure vulnerable ports are not open to malicious actors.

Set server firewall to drop packet traffic when connection thresholds are exceeded.

Regularly patch firewalls and software to avoid zero-day attacks.

Mitigation: Finding the Request for the Hidden Directory

Alarm

To detect unauthorized access requests for hidden folders, I would block all incoming HTTP traffic when the source IP originates outside whitelisted company IP addresses.

A threshold should be set to a maximum of 10 attempts per hour before a triggered alert is sent to the system administrator.

System Hardening

Sensitive files should not be open to the public facing file systems. An alternative to the Web Distributed Authoring and Versioning (WebDAV) service should be explored.

In the meantime, sensitive information/data should be encrypted and the folders should only be accessed by whitelisted IP addresses.

VPN tunneling could also be a solution that will provide infrastructure towards continuing security improvements.

Mitigation: Preventing Brute Force Attacks

Alarm

Send an email alert and lock the account when more than 20 bad login attempts are made.

Create a dashboard item that tracks HTTP 401 Unauthorized client error statuses and the associated IP address.

Send an alert when the user agent indicates usage of Hydra or any other credential stuffing software.

System Hardening

Implementation of more complex passwords that are 8-12 characters in length with at least one number and one symbol included.

Account lockout policy that triggers a 30 minute waiting period after 20 bad login attempts.

A running blacklist and whitelist of IP addresses that trigger the lockout alert. If a lockout effects an employee, a password locker/education may be necessary.

Mitigation: Detecting the WebDAV Connection

Alarm

Block all HTTP traffic originating outside of a whitelisted company IP address to the WebDAV folder.

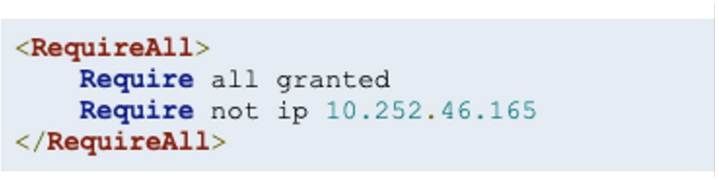
Email the system administrator when more than 5 HTTP GET requests are made to the folder from a single IP source outside the company whitelist.

Email the system administrator of any HTTP PUT request made to the folder from outside the company whitelist.

System Hardening

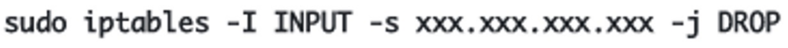
Restrict access to sensitive portions of the linux server and website with:

mod_authz_host



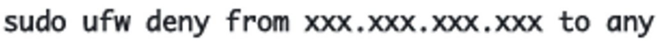
```
<RequireAll>
    Require all granted
    Require not ip 10.252.46.165
</RequireAll>
```

Uncomplicated Firewall (UFW)



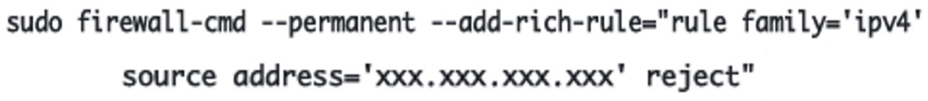
```
sudo iptables -I INPUT -s xxx.xxx.xxx.xxx -j DROP
```

iptables



```
sudo ufw deny from xxx.xxx.xxx.xxx to any
```

Firewalld



```
sudo firewall-cmd --permanent --add-rich-rule="rule family='ipv4'
        source address='xxx.xxx.xxx.xxx' reject"
```

https://docs.rackspace.com/support/how-to/block-an-ip-address-on-a-Linux-server/

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alert the system administrator when any http PUT request is recorded to sensitive folders from an IP address outside of the company whitelist.

Alert the system administrator when an attempt is made to access port 80, 4444, and 1337 from all network traffic.

The previous alert can be paused if/when remote access is needed by the I.T. dept. for scheduled maintenance purposes.

System Hardening

Block all http PUT requests from IP addresses outside of the company whitelist.

Set access to the WebDAV folder to read only to prevent any unwanted executable files from being uploaded.

Close/Block any ports that are not necessary to continue with business operations.

The End