Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

TEAM 2 SECURITY SERVICES

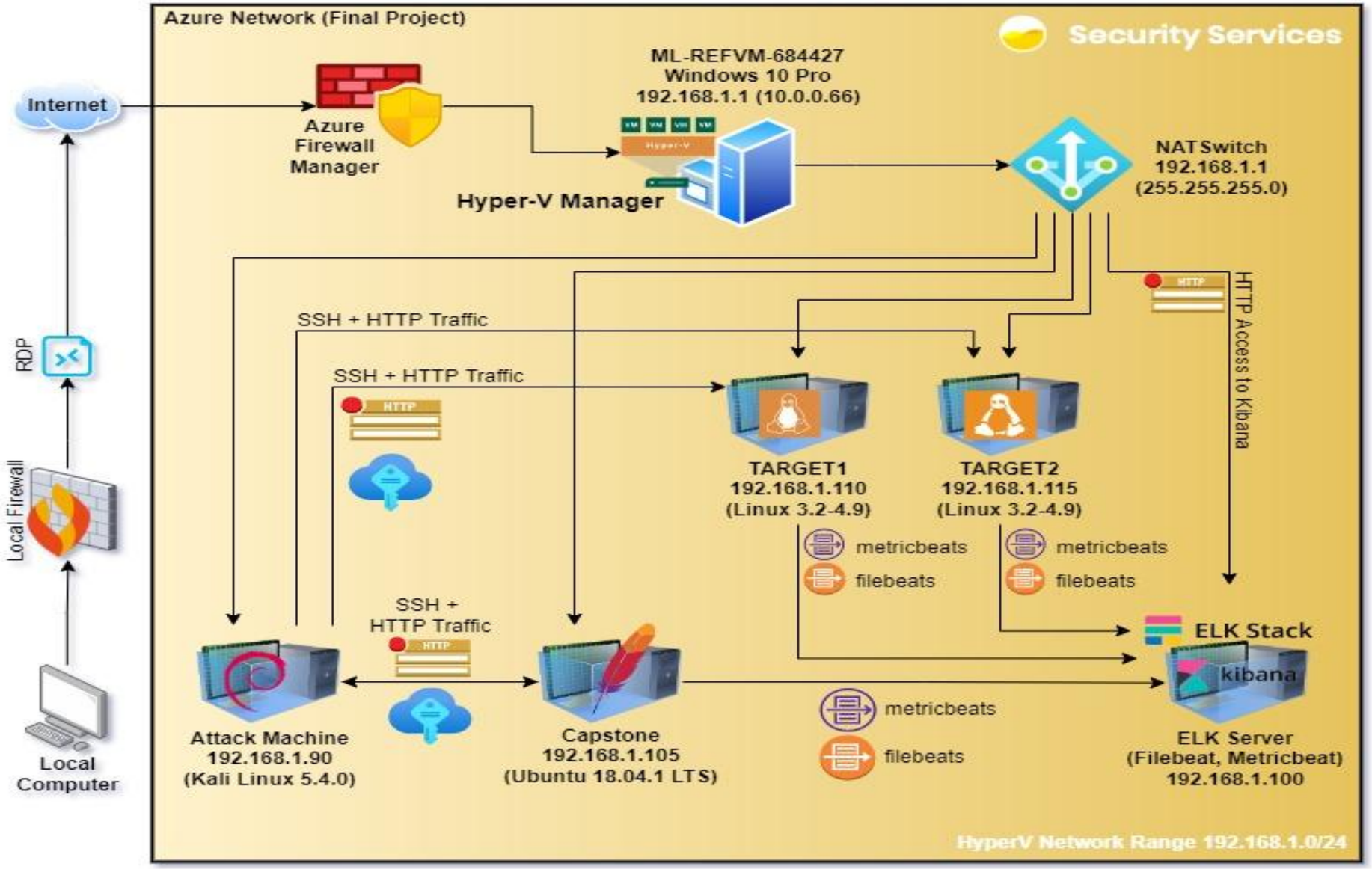
Prepared by:
Frank Lin, David Guereca, Nathan Turner, Kamalpreet Kaur, & Ruben Ochoa-Banuelos

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology for Raven Security Services



Network
Address Range: 192.168.1.1/24
Netmask: 255.255.255.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.14.4 LTS
Hostname: ELK

IPv4: 192.168.1.90
OS: Kali Linux 5.4.0
Hostname: Kali

IPv4: 192.168.1.110
OS: Linux 3.2 - 4.9
Hostname: Target1

IPv4: 192.168.1.115
OS: Linux 3.2 - 4.9
Hostname: Target2

Critical Vulnerabilities: Target 1 (192.168.1.110)

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

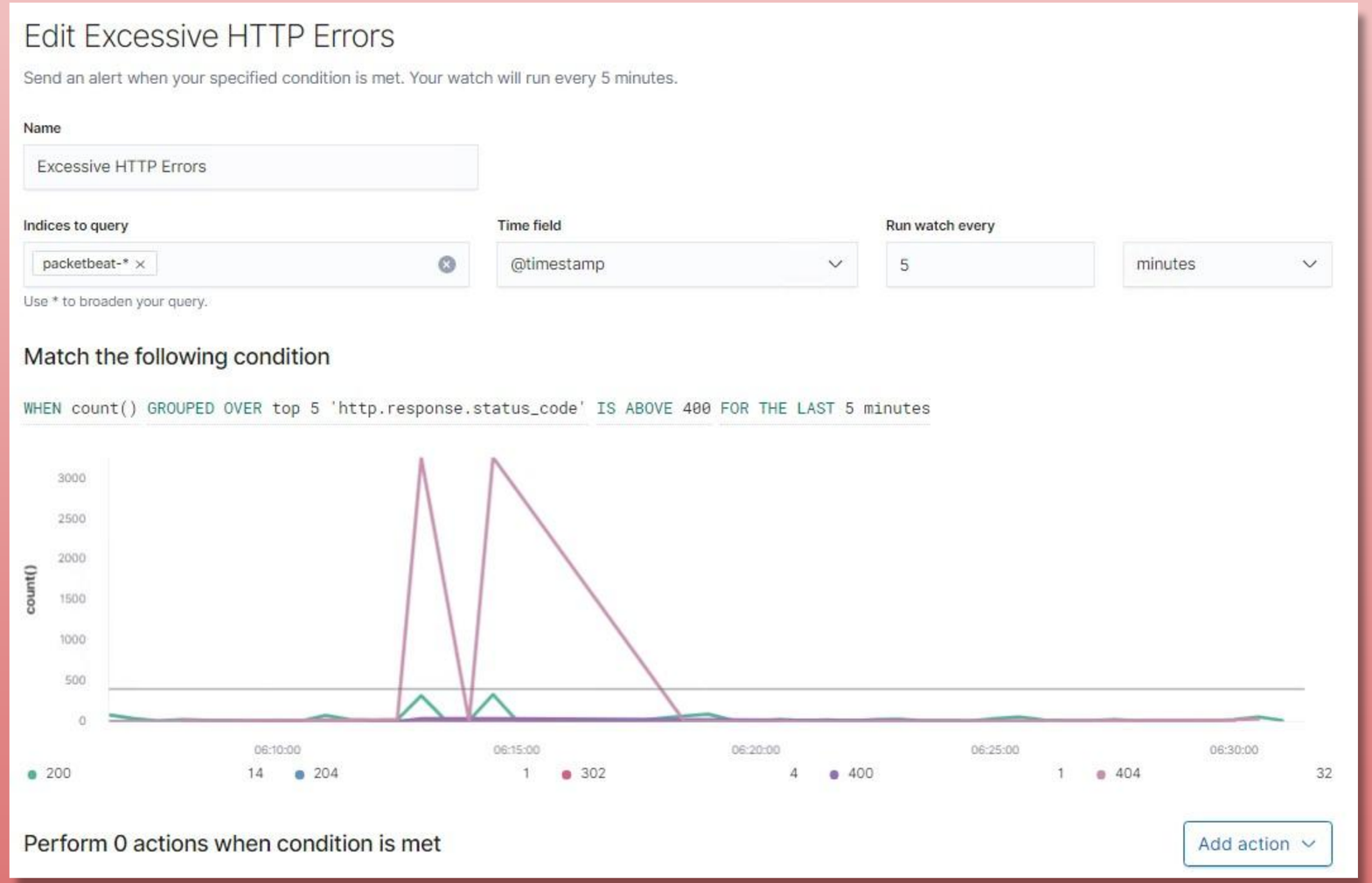
Vulnerability	Description	Impact
Network Mapping Scan (NMap)	Port scanning tool to find open ports and software versioning	Allows users to find open ports and possible known vulnerabilities with outdated system software
WPScan WordPress User Enumeration	Brute Force detection of possible Users/Authors of WordPress site	Permits attackers to utilize login credentials to brute force or password crack for unauthorized access into systems
Unsalted Password Hash(es)/ Weak Password Encryption/ Exposed mySQL Database Password	Weak passwords & hashes, weak password hash encryption, and exposed plaintext passwords	Enables bad actors to easily and quickly access databases to decrypt other simple passwords to gain unauthorized access to the system(s)
Plain Text Storage of Secret Information	Critical or confidential information easily viewable and searchable	Lets unauthorized parties inside compromised systems to steal confidential information (flags)
(Root) Privilege Escalation Access	Sudo privileges available to lower level users allow exploits to be run	Grants escalated super user privileges to an attacker to take control over a system with unfeathered access

Alerts Implemented

Excessive HTTP Errors

- This packetbeat alert metric monitors the http response status codes above 400 (client errors) for the last 5 minutes

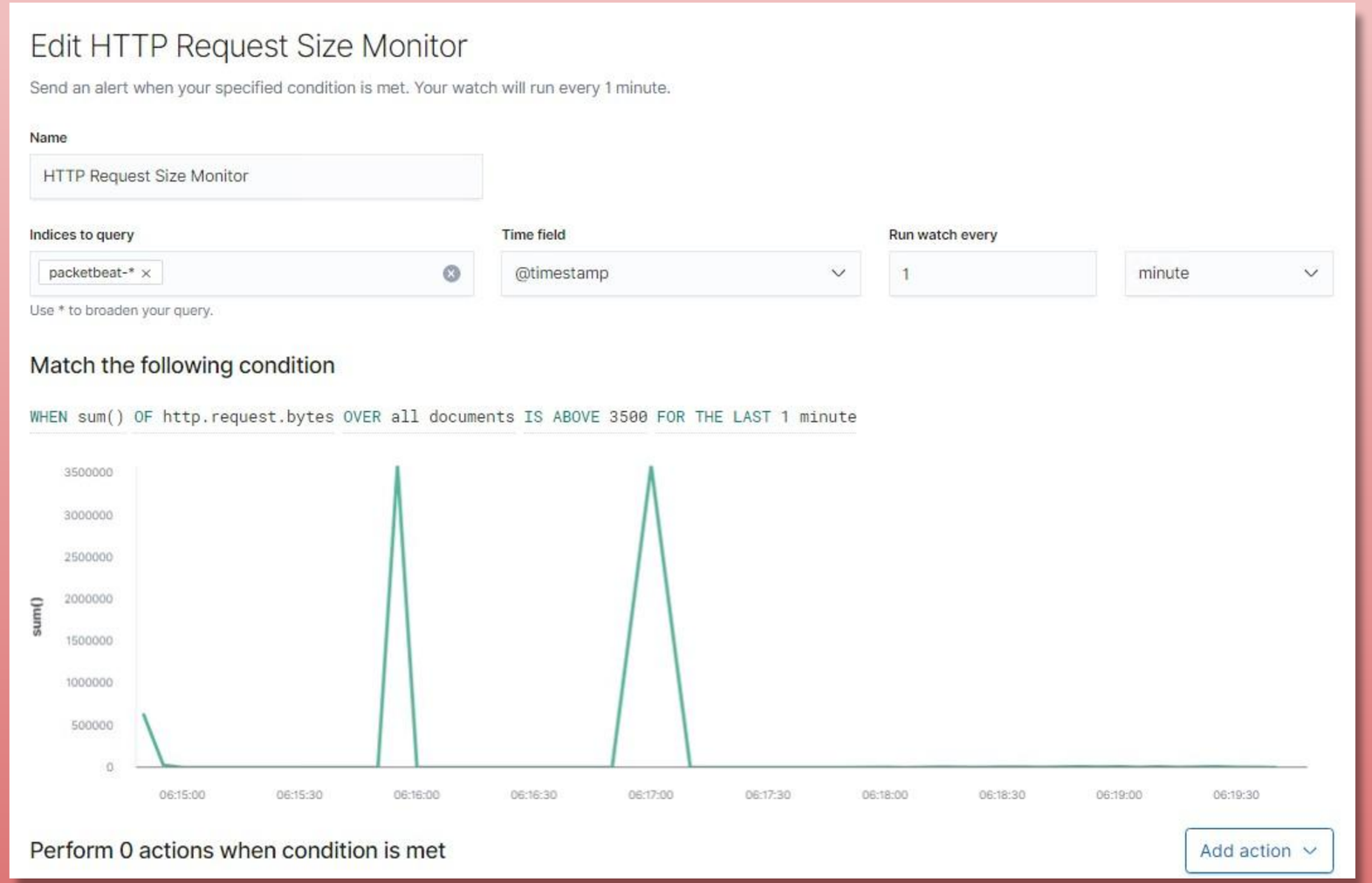
- The alert fires when the top 5 error codes are above 400



HTTP Request Size Monitor

- This packetbeat alert metric monitors when the total accumulated size of documents for the last 1 minute is larger than 3500 bytes

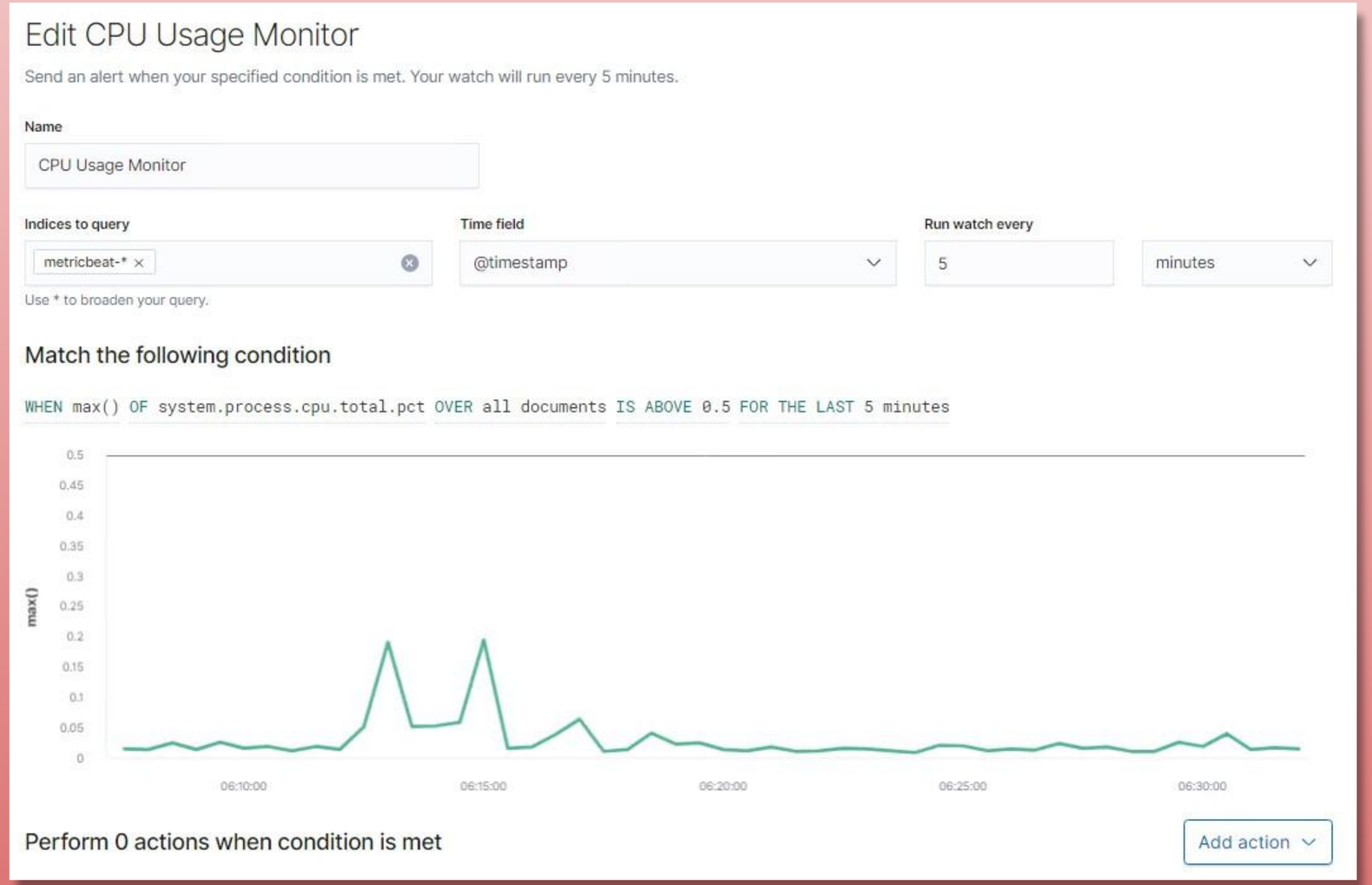
- This alert fires when that total is above 3500 bytes



CPU Usage Monitor

- This metricbeat alert metric measures the percentage of CPU usage from system processes for the last 5 minutes

- This alert fires when the total CPU usage is above 50% for all requests processed



Hardening

Hardening Against Network Mapping Scan (NMap) on Target 1

How to patch

- Enable Windows Defender Firewall with Advanced Security Design
- Disable ICMP Echo Requests

How the patch works

- Filter inbound and outbound ports and connecting a well configured firewall will effectively slow and drop reconnaissance packets
- Effectively stops responding to ping requests

How to install it

- Firewall is default enabled on windows 8 or later
  - For basic firewall policy design please refer to [Basic Firewall Policy Design (Windows) - Security]
- To disable ICMP echo (ping) requests:
  - Press `*windows key+R*`→ Open `*firewall.cpl*` →Click on `*Advanced settings*` on the left-hand side options →Select `*Inbound Rules*` → Locate `*File and Printer Sharing*` → Right-click and select `*Disable Rule*`

Hardening Against WordPress User Enumeration on Target 1

How to patch

- Implement regular updates to WordPress, Plugins, and the PHP version(s)
  - Specified Plugins ‘WP-Hardening’ & ‘WPS Hide Login’

How the patch works

- Ensures patches for vulnerabilities are regularly maintained and installed
- WP-Hardening - stops user enumeration
- WPS Hide Login - Disable WordPress Logins from being publicly accessible specifically /wp-admin - changes the login url

How to install it

Implement `WP-Hardening` plugin via GUI

- Install and activate the plugin
  - locate `*Plugins > Add New*` in the admin dashboard → search for `*WP-Hardening*` → install → activate from the Plugins page **appears on the bottom left of the admin dashboard**
- Locate `*Security Fixers*` tab → Toggle the key next to `Stop User enumeration`

WPS Hide Login User Specifics

Hardening Against Plain Text Storage of Secret Info on Target 1

How to patch:

- Creating hashes for sensitive information.

Why the patch works:

- It creates a unique fingerprint using an algorithm that can be used to make it more difficult for attackers to see the sensitive information.
- It can also be used to verify the integrity of the files and password verification.

How to install it:

- Example of password hashing using md5 with Linux commands (below)
- Sha256 tool can be installed using *'sudo apt install hashalot'*

```
S3cr3tP4ss0rd
```

```
nano test.txt
md5sum test.txt >> pass_hash.txt
cat pass_hash.txt
```

```
21ac73e249f3c31a81f0d2b1ae70c713  test.txt
```

Hardening Against Unsalted Password Hashes on Target 1

How to patch:

- Utilizing password management tools, securing all user passwords with salted hashes.

Why the patch works:

- '*Salting*' passwords involve adding random stings either in front or at the end of the password string value before the hash is created.

How to install it:

- *SecureRandom* is suggested by the Open Web Application Security Project (OWASP).
    - Commonly used in JAVA and Ruby with instructions for JAVA below:
    - SecureRandom (Java Platform SE 8) (oracle.com)
- Alternatively, an in-house created algorithm can generate the random values with desired length.

Hardening Against Privilege Escalation Access on Target 1

How to patch:

- Incorporating good access management strategies such as Principle of Least Privilege, User and Entity Behavior Analytics (UEBA) and education to employees just to name a few.

Why the patch works:

- Principle of Least Privilege says every user of the system should operate using the least set of privileges necessary to complete the job.
- UEBAs continuously monitor user activity over time to create an appropriate behavior baseline to identify unusual activity using machine learning algorithms.

How to install it:

- Splunk has a UEBA tool that can downloaded and installed:
- UEBA - Splunk Security Content

Implementing Patches

Implementing Patches

- **Automate updates delivered through utilizing playbooks and cron jobs**
  - Can rapidly execute critical system maintenance across network
- **Change permissions of the “wp-config.php” file for owner access only**
  - Mitigates unauthorized viewing of MySQL login info
- **Install plugin that enforces stronger passwords**
  - Ex. length, complexity, lockouts for failed attempts
- **Replace SSH passwords with required public key login(s)**
  - Ensures user is trusted when accessed remotely

The End