

WordPress Website

Proof of Concept Technical Solutions for the Marconi Law Firm,
LLC.

Antonio Thomas
MetroIT Consultants

Network Topography

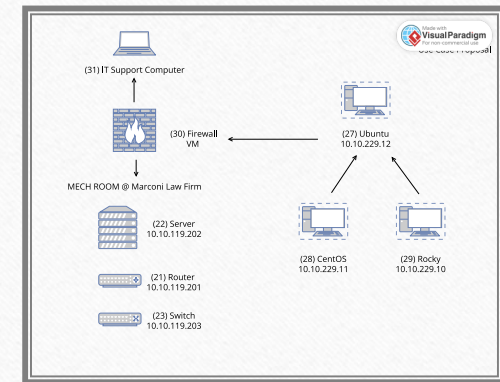
Request from the browser

Handling by Nginx

Processing by the ghost container

Respond handling by Nginx

Returning the response to the browser



Defense in Depth

The multi-layered approach to security includes:

Physical Controls

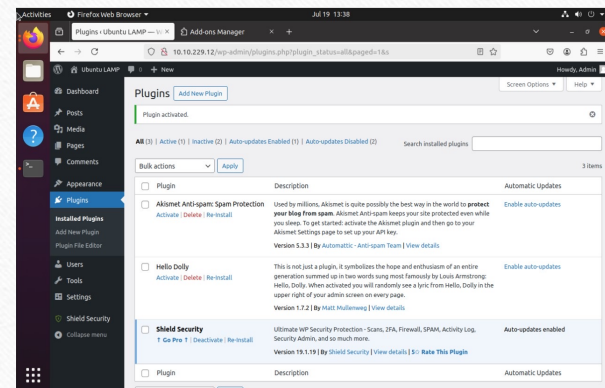
Network Security Controls

Administrative Controls

Antivirus

Behavioral and Analysis

Antivirus



Identifying Vulnerabilities

File Permission Vulnerability

```
user@UbuntuTHOMAS:~$ cd /var/www/html/
user@UbuntuTHOMAS:/var/www/html$ ls -la
total 252
drwxr-xr-x 6 www-data www-data 4096 Jul 12 19:21 .
drwxr-xr-x 3 root root 4096 Jul 12 14:03 ..
drwxr-xr-x 8 root root 4096 Jul 12 19:09 .git
-rw-r--r-- 1 www-data www-data 523 Jul 12 19:21 .htaccess
-rw-r--r-- 1 www-data www-data 405 Jul 12 18:58 index.php
-rw-r--r-- 1 www-data www-data 19915 Jul 12 18:58 license.txt
-rw-r--r-- 1 www-data www-data 7409 Jul 12 18:58 readme.html
-rw-r--r-- 1 www-data www-data 7387 Jul 12 18:58 wp-activate.php
drwxr-xr-x 9 www-data www-data 4096 Jul 12 18:58 wp-admin
-rw-r--r-- 1 www-data www-data 351 Jul 12 18:58 wp-blog-header.php
-rw-r--r-- 1 www-data www-data 2323 Jul 12 18:58 wp-comments-post.php
-rw-r--r-- 1 www-data www-data 3322 Jul 12 19:18 wp-config.php
-rw-r--r-- 1 www-data www-data 3033 Jul 12 18:58 wp-config-sample.php
drwxr-xr-x 5 www-data www-data 4096 Jul 12 19:34 wp-content
-rw-r--r-- 1 www-data www-data 5611 Jul 12 18:58 wp-cron.php
drwxr-xr-x 0 www-data www-data 12288 Jul 12 18:58 wp-includes
-rw-r--r-- 1 www-data www-data 2502 Jul 12 18:58 wp-links-opml.php
-rw-r--r-- 1 www-data www-data 3937 Jul 12 18:58 wp-load.php
-rw-r--r-- 1 www-data www-data 51198 Jul 12 18:58 wp-login.php
-rw-r--r-- 1 www-data www-data 8525 Jul 12 18:58 wp-mail.php
-rw-r--r-- 1 www-data www-data 28774 Jul 12 18:58 wp-settings.php
-rw-r--r-- 1 www-data www-data 34385 Jul 12 18:58 wp-signup.php
-rw-r--r-- 1 www-data www-data 4885 Jul 12 18:58 wp-trackback.php
-rw-r--r-- 1 www-data www-data 3246 Jul 12 18:58 xmlrpc.php
```

Understanding
infrastructure

Vulnerability Scanner

Performing Configurations

```
user@UbuntuTHOMAS:/var/www/html$ sudo find /var/www/html/* -type d -exec chmod 740 {} \;
```

Owner

- Access Level 7
- Read, Write and Exec

Group

- Access Level 4
- Read Only

User

- Access Level 0
- Permission denied

Testing

File Permission Validation

User

- Permission Denied

Owner
/ Group

- Permission Granted

```
user@UbuntuTHOMAS:/var/www/html$ cd wp-admin
bash: cd: wp-admin: Permission denied
```

```
user@UbuntuTHOMAS:/var/www/html$ cd wp-content
bash: cd: wp-content: Permission denied
```

```
user@UbuntuTHOMAS:/var/www/html$ cd wp-includes
bash: cd: wp-includes: Permission denied
```

```
root@UbuntuTHOMAS:/var/www/html/wp-includes
root@UbuntuTHOMAS:/var/www/html# cd wp-admin
root@UbuntuTHOMAS:/var/www/html/wp-admin# cd ..
root@UbuntuTHOMAS:/var/www/html# cd wp-content
root@UbuntuTHOMAS:/var/www/html/wp-content# cd ..
root@UbuntuTHOMAS:/var/www/html# cd wp-includes
root@UbuntuTHOMAS:/var/www/html/wp-includes#
```

In Conclusion:

- Data Security
- Defense in Depth
- File Permissions
- Logging and Auditing
- Continuous Monitoring
- Intrusion Detection
- Behavior Analytics

