**Recon Phase Notes**

During recon, discovered name of web application:

Badstore.net - Used this information to carry out OSINT online.

*My IP: 192.168.71.131*

*BadStore IP: 192.168.16.128*

**Commands & Screenshots**

$ sudo apt-get update && sudo apt-get install net-tools

NB: Had to place Kali on NET to get working

$ sudo arp-scan -l

A screenshot of a computer

Description automatically generated with medium confidence

Fig Shows three IP addresses on network

NB: First is unreachable, third is another modules VM, deduced it’s the second IP.

\*\* Use nmap here to double check \*\*

$ ping 192.168.16.128

A screenshot of a computer

Description automatically generated with medium confidence

Fig Shows 0% packet loss when pinging discovered IP

Now tried nmap scan but would only work with kali on the Nat network. I will try again at uni to see if this is an issue.

*$ sudo nmap -sV -p 80, 443 --script vulners 192.168.16.128*

**┌──(kali㉿kali)-[~]**

**└─$ sudo nmap -sV -p 80, 443 --script vulners 192.168.16.128**

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 13:35 EST

Nmap scan report for 192.168.16.128

Host is up (0.00082s latency).

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 1.3.28 ((Unix) mod\_ssl/2.8.15 OpenSSL/0.9.7c)

|\_http-server-header: Apache/1.3.28 (Unix) mod\_ssl/2.8.15 OpenSSL/0.9.7c

| vulners:

| cpe:/a:apache:http\_server:1.3.28:

| CVE-2004-0492 10.0 https://vulners.com/cve/CVE-2004-0492

| SSV:6610 7.6 https://vulners.com/seebug/SSV:6610 \*EXPLOIT\*

| SSV:63874 7.6 https://vulners.com/seebug/SSV:63874 \*EXPLOIT\*

| SSV:429 7.6 https://vulners.com/seebug/SSV:429 \*EXPLOIT\*

| SSV:16391 7.6 https://vulners.com/seebug/SSV:16391 \*EXPLOIT\*

| SAINT:B572402CE6E5C851D7572BF044507A14 7.6 https://vulners.com/saint/SAINT:B572402CE6E5C851D7572BF044507A14 \*EXPLOIT\*

| SAINT:386ECCECD3AA34FA1E84E6D3D2B71C7B 7.6 https://vulners.com/saint/SAINT:386ECCECD3AA34FA1E84E6D3D2B71C7B \*EXPLOIT\*

| SAINT:35A5AA91DCF68555669689272BFFD3E7 7.6 https://vulners.com/saint/SAINT:35A5AA91DCF68555669689272BFFD3E7 \*EXPLOIT\*

| SAINT:14705540EFEE2160EBFBAF5BDA3E828C 7.6 https://vulners.com/saint/SAINT:14705540EFEE2160EBFBAF5BDA3E828C \*EXPLOIT\*

| PACKETSTORM:83108 7.6 https://vulners.com/packetstorm/PACKETSTORM:83108 \*EXPLOIT\*

| PACKETSTORM:62377 7.6 https://vulners.com/packetstorm/PACKETSTORM:62377 \*EXPLOIT\*

| PACKETSTORM:56989 7.6 https://vulners.com/packetstorm/PACKETSTORM:56989 \*EXPLOIT\*

| PACKETSTORM:55727 7.6 https://vulners.com/packetstorm/PACKETSTORM:55727 \*EXPLOIT\*

| PACKETSTORM:49400 7.6 https://vulners.com/packetstorm/PACKETSTORM:49400 \*EXPLOIT\*

| EXPLOITPACK:8FEEBCD1B617ED74B8D2179061252A44 7.6 https://vulners.com/exploitpack/EXPLOITPACK:8FEEBCD1B617ED74B8D2179061252A44 \*EXPLOIT\*

| EXPLOITPACK:6E3090CD46CEEE08D52992589E824D90 7.6 https://vulners.com/exploitpack/EXPLOITPACK:6E3090CD46CEEE08D52992589E824D90 \*EXPLOIT\*

| EDB-ID:3680 7.6 https://vulners.com/exploitdb/EDB-ID:3680 \*EXPLOIT\*

| EDB-ID:2237 7.6 https://vulners.com/exploitdb/EDB-ID:2237 \*EXPLOIT\*

| CVE-2006-3747 7.6 https://vulners.com/cve/CVE-2006-3747

| CVE-2004-1082 7.5 https://vulners.com/cve/CVE-2004-1082

| CVE-2003-0993 7.5 https://vulners.com/cve/CVE-2003-0993

| CVE-2003-0987 7.5 https://vulners.com/cve/CVE-2003-0987

| CVE-2003-0542 7.2 https://vulners.com/cve/CVE-2003-0542

| CVE-2004-0940 6.9 https://vulners.com/cve/CVE-2004-0940

| SSV:19019 6.8 https://vulners.com/seebug/SSV:19019 \*EXPLOIT\*

| CVE-2010-0010 6.8 https://vulners.com/cve/CVE-2010-0010

| SSV:66957 5.0 https://vulners.com/seebug/SSV:66957 \*EXPLOIT\*

| SSV:20993 5.0 https://vulners.com/seebug/SSV:20993 \*EXPLOIT\*

| SSV:20979 5.0 https://vulners.com/seebug/SSV:20979 \*EXPLOIT\*

| SSV:20969 5.0 https://vulners.com/seebug/SSV:20969 \*EXPLOIT\*

| SSV:17994 5.0 https://vulners.com/seebug/SSV:17994 \*EXPLOIT\*

| SSV:14432 5.0 https://vulners.com/seebug/SSV:14432 \*EXPLOIT\*

| PACKETSTORM:85018 5.0 https://vulners.com/packetstorm/PACKETSTORM:85018 \*EXPLOIT\*

| PACKETSTORM:82197 5.0 https://vulners.com/packetstorm/PACKETSTORM:82197 \*EXPLOIT\*

| PACKETSTORM:105672 5.0 https://vulners.com/packetstorm/PACKETSTORM:105672 \*EXPLOIT\*

| PACKETSTORM:105591 5.0 https://vulners.com/packetstorm/PACKETSTORM:105591 \*EXPLOIT\*

| EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B 5.0 https://vulners.com/exploitpack/EXPLOITPACK:460143F0ACAE117DD79BD75EDFDA154B \*EXPLOIT\*

| EXPLOITPACK:44DAC602FB30402C58970DFAB1C4AF87 5.0 https://vulners.com/exploitpack/EXPLOITPACK:44DAC602FB30402C58970DFAB1C4AF87 \*EXPLOIT\*

| EDB-ID:9887 5.0 https://vulners.com/exploitdb/EDB-ID:9887 \*EXPLOIT\*

| EDB-ID:17969 5.0 https://vulners.com/exploitdb/EDB-ID:17969 \*EXPLOIT\*

| CVE-2011-3368 5.0 https://vulners.com/cve/CVE-2011-3368

| CVE-2007-6750 5.0 https://vulners.com/cve/CVE-2007-6750

| CVE-2004-0263 5.0 https://vulners.com/cve/CVE-2004-0263

| CVE-2003-0020 5.0 https://vulners.com/cve/CVE-2003-0020

| CVE-2001-1556 5.0 https://vulners.com/cve/CVE-2001-1556

| SSV:2174 4.7 https://vulners.com/seebug/SSV:2174 \*EXPLOIT\*

| CVE-2007-3304 4.7 https://vulners.com/cve/CVE-2007-3304

| SSV:71772 4.3 https://vulners.com/seebug/SSV:71772 \*EXPLOIT\*

| SSV:2818 4.3 https://vulners.com/seebug/SSV:2818 \*EXPLOIT\*

| SSV:2801 4.3 https://vulners.com/seebug/SSV:2801 \*EXPLOIT\*

| SSV:24250 4.3 https://vulners.com/seebug/SSV:24250 \*EXPLOIT\*

| PACKETSTORM:61420 4.3 https://vulners.com/packetstorm/PACKETSTORM:61420 \*EXPLOIT\*

| PACKETSTORM:102234 4.3 https://vulners.com/packetstorm/PACKETSTORM:102234 \*EXPLOIT\*

| EXPLOITPACK:683C3B1D02827D6B32706DB1D146B2D8 4.3 https://vulners.com/exploitpack/EXPLOITPACK:683C3B1D02827D6B32706DB1D146B2D8 \*EXPLOIT\*

| EDB-ID:17393 4.3 https://vulners.com/exploitdb/EDB-ID:17393 \*EXPLOIT\*

| CVE-2011-4317 4.3 https://vulners.com/cve/CVE-2011-4317

| CVE-2007-6388 4.3 https://vulners.com/cve/CVE-2007-6388

| CVE-2007-5000 4.3 https://vulners.com/cve/CVE-2007-5000

| CVE-2006-5752 4.3 https://vulners.com/cve/CVE-2006-5752

| CVE-2006-3918 4.3 https://vulners.com/cve/CVE-2006-3918

|\_ CVE-2005-3352 4.3 https://vulners.com/cve/CVE-2005-3352

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 2 IP addresses (1 host up) scanned in 7.95 seconds

*$ nikto -h 192.168.16.128*

**──(kali㉿kali)-[~]**

**└─$ nikto -h 192.168.16.128**

- Nikto v2.5.0

---------------------------------------------------------------------------

+ Target IP: 192.168.16.128

+ Target Hostname: 192.168.16.128

+ Target Port: 80

+ Start Time: 2023-03-08 13:43:58 (GMT-5)

---------------------------------------------------------------------------

+ Server: Apache/1.3.28 (Unix) mod\_ssl/2.8.15 OpenSSL/0.9.7c

+ /: Server may leak inodes via ETags, header found with file /, inode: 331, size: 3583, mtime: Sun May 14 17:16:23 2006. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ /supplier/: Directory indexing found.

+ /robots.txt: Entry '/supplier/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600\_robots-txt-file

+ /backup/: Directory indexing found.

+ /robots.txt: Entry '/backup/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600\_robots-txt-file

+ /robots.txt: contains 6 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt

+ mod\_ssl/2.8.15 appears to be outdated (current is at least 2.9.6) (may depend on server version).

+ Apache/1.3.28 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

+ OpenSSL/0.9.7c appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.

+ /index: Uncommon header 'tcn' found, with contents: list.

+ /index: Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275

+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918

+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .

+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross\_Site\_Tracing

+ Apache/1.3.28 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod\_rewrite and mod\_cgi.

+ /backup/: This might be interesting.

+ /cgi-bin/test.cgi: This might be interesting.

+ /icons/: Directory indexing found.

+ /images/: Directory indexing found.

+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

+ 8913 requests: 0 error(s) and 22 item(s) reported on remote host

+ End Time: 2023-03-08 13:44:27 (GMT-5) (29 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

Next I download Nessus and carry out a scan. 22 Vulnerabilities were found.

18% of which are critical

14% are High

23% are medium

5% is low

40% are informational

Try: sql injection

*Admin’ or ‘x’ = x’*

*Also, go through each lab on BadStore.net to see if you can do the lab exercises on it\*\**