

Red Team: Summary of Operations

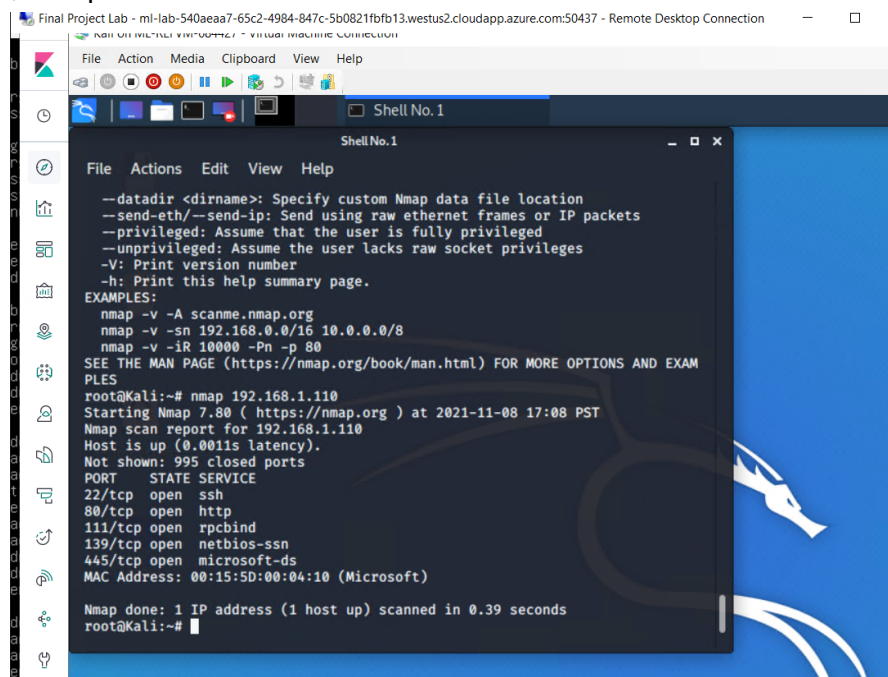
Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

\$ nmap 192.168.1.0.24



```
Final Project Lab - ml-lab-540a7-65c2-4984-847c-5b0821fbfb13.westus2.cloudapp.azure.com:50437 - Remote Desktop Connection
File Action Media Clipboard View Help
Shell No. 1
Shell No. 1
File Actions Edit View Help
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-08 17:08 PST
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@Kali:~#
```

This scan identifies the services below as potential points of entry:

- Target 1
 - Port 22 with SSH
 - Port 80 with HTTP
 - Port 111 with rpcbind
 - Port 139 with Netbios-ssn
 - Port 445 with Microsoft-ds

The following vulnerabilities were identified on each target:

- Target 1
 - SSH can allow unauthorized users to remote into a target machine and gain access to files or confidential information. It has a high severity. (<https://www.cvedetails.com/cve/CVE-1999-0013/>)
 - HTTP won't provide a secure session. Additionally, it can allow an attacker to send heavy traffic to deny access (a service) to the webpage. It has a high severity. [CVE-1999-0926](#)
 - rpcbind is used for listing active services, and telling the requesting client where to send the RPC request. If a host listens on port 111, one can use rpcinfo to get program numbers and ports and services running; ([CVE-2017-8779](#), [CVE-2015-7236](#), [CVE-2010-2064](#), [CVE-2010-2061](#))
 - Netbios on port 139 has known vulnerabilities on metasploit (<https://searchsecurity.techtarget.com/answer/The-dangers-of-open-port-139>) CVE-2008-4250
 - Known vulnerabilities on metasploit for microsoft-ds on port 445. <https://machn1k.wordpress.com/2012/10/29/smb-exploitation-port-445/> CVE-2008-4250

```

--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAM
PLES
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-08 17:08 PST
Nmap scan report for 192.168.1.110
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp    open  rpcbind
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@Kali:~#

```

TODO: Include vulnerability scan results to prove the identified vulnerabilities.

Exploitation

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

- Target 1
 - flag1.txt: b9bbcb33e11b80be759c4e844862482d

■ Exploit Used

- Able to SSH into the machine and cd into the directory /var/www/html/ to find the flag. Used grep to find it.
- grep -ER flag

```

vendor/examples/scripts/XRegExp.js: // Accepts a pattern and flags; returns an extended RegExp object. If the pattern and flag
vendor/examples/scripts/XRegExp.js: var key = pattern + "/" + (flags || "");
vendor/examples/scripts/XRegExp.js: return XRegExp.cache[key] || (XRegExp.cache[key] = XRegExp(pattern, flags));
vendor/examples/scripts/XRegExp.js: // Accepts a 'RegExp' instance; returns a copy with the 'g' flag set. The copy has a fresh
vendor/examples/scripts/XRegExp.js: // syntax and flag changes. Should be run after XRegExp and any plugins are loaded
vendor/examples/scripts/XRegExp.js: // third ('flags') parameter
vendor/examples/scripts/XRegExp.js: // capture. Also allows adding new flags in the process of copying the regex
vendor/examples/scripts/XRegExp.js: // Augment XRegExp's regular expression syntax and flags. Note that when adding tokens, the
vendor/examples/scripts/XRegExp.js: // Mode modifier at the start of the pattern only, with any combination of flags imsx: (?imsx)
vendor/composer.lock: "stability-flags": [],
service.html:     <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$

```

- flag2.txt: fc3fd58dcdada9ab23faca6e9a36e581c

■ Exploit Used

- SSH into the target and cd to the directory /var/www/ and ran a ls to find the flag2.txt
- cd /var/www/ and ls

```

Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help

Raven Security - Mozilla ... michael@target1:/var

michael@target1:/var
File Actions Edit View Help

/** Absolute path to the WordPress directory. */
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');

/** Sets up WordPress vars and included files. */
require_once(ABSPATH . 'wp-settings.php');
michael@target1:/var/www/html/wordpress$ ls
index.php      wp-blog-header.php  wp-cron.php      wp-mail.php
license.txt    wp-comments-post.php wp-includes       wp-settings.php
readme.html   wp-config.php       wp-links-opml.php wp-signup.php
wp-activate.php wp-config-sample.php wp-load.php       wp-trackback.php
wp-admin.php  wp-content          wp-login.php     xmlrpc.php
michael@target1:/var/www/html/wordpress$ cd ../
michael@target1:/var/www/html$ ls
about.html  css      img      scss      team.html
contact.php elements.html index.html Security - Doc wordpress
contact.zip fonts  js       service.html
michael@target1:/var/www/html$ cd ../
michael@target1:/var/www$ ls
flag2.txt
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdada9ab23faca6e9a36e581c}
michael@target1:/var/www$ cd ../
michael@target1:/var$ ls
backups cache lib local lock log mail opt run spool tmp
michael@target1:/var$

```

```

mysql> SELECT * FROM wp_users;
+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | michael | $P$BjRvZQ.VQcGZLDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | | 2018-08-12 22:49:12 | |
| 2 | steven | $P$Bk3VD9jsxx/loJogNsURGHiaB23j7W/ | steven | steven@raven.org | | 2018-08-12 23:31:16 | |
+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

```

