Shocker HTB

- 🏷️**Tags** : #01-2023 #report
- CTF link: https://app.hackthebox.com/machines/Shocker/

Service Enumeration

Port	Protocol	State	Service
80	tcp	open	http
2222	tcp	open	EtherNetIP-1

Web mapping

```
===================================================================
ID           Response   Lines    Word       Chars       Payload
===================================================================

000000001:   200        9 L      13 W       137 Ch      "http://10.10.10.56/"
000000013:   403        11 L     32 W       295 Ch      ".htpasswd"
000000012:   403        11 L     32 W       295 Ch      ".htaccess"
000000011:   403        11 L     32 W       290 Ch      ".hta"
000000820:   403        11 L     32 W       294 Ch      "cgi-bin/"
000002020:   200        9 L      13 W       137 Ch      "index.html"
000003588:   403        11 L     32 W       299 Ch      "server-status"
===================================================================
ID           Response   Lines    Word       Chars       Payload
===================================================================

000000031:   403        11 L     32 W       301 Ch      ".hta - sh"
000000039:   403        11 L     32 W       307 Ch      ".htpasswd - cgi"
000000034:   403        11 L     32 W       306 Ch      ".htaccess - sh"
000000036:   403        11 L     32 W       307 Ch      ".htaccess - cgi"
000000038:   403        11 L     32 W       307 Ch      ".htpasswd - php"
000000033:   403        11 L     32 W       302 Ch      ".hta - cgi"
000000035:   403        11 L     32 W       307 Ch      ".htaccess - php"
000000037:   403        11 L     32 W       306 Ch      ".htpasswd - sh"
000000032:   403        11 L     32 W       302 Ch      ".hta - php"
000012676:   200        7 L      17 W       118 Ch      "user - sh"
```

```
❯ curl -s -X GET http://10.10.10.56/cgi-bin/user.sh
Content-Type: text/plain

Just an uptime test script

 04:44:18 up 23:57,  0 users,  load average: 0.00, 0.01, 0.00
```

Penetration

Vulnerability Exploited

> *CVE-2014-6271 updated to CVE-2014-7169*

System Vulnerable

> *10.10.10.56*

Vulnerability Explanation

> *Shellshock is a vulnerability that allows systems containing a vulnerable version of Bash to be exploited to execute commands with higher privileges. This allows attackers to potentially take over that system. While Bash is not inherently Internet-facing, many internal and external services such as web servers do use environment variables to communicate with the server's operating system.*
>
> *PERL binary is allowed to run as SUDO without requiring a password what leads into an easy privilege escalation*

Vulnerability Fix

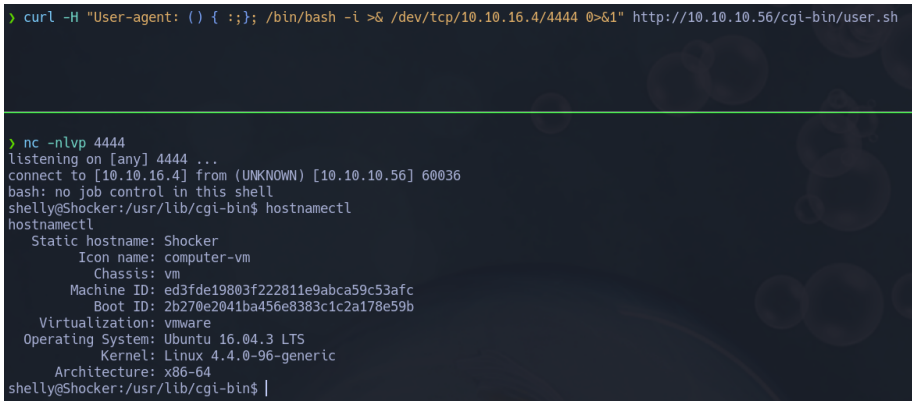
> *Update how bash interprets the `x=() {...}` environment variable as a function definition. Exporting functions with `export -f x` will now set a environment variable `BASH_FUNC_x%%=() {...}` instead of simply `x=() {...}`*
>
> *Remove SUDO (NoPasswd) from PERL binary*

Severity

> *According to CSSv3.1 vector calculator base score metrics there is an overall CVSS score of 9.8 [Critical]*

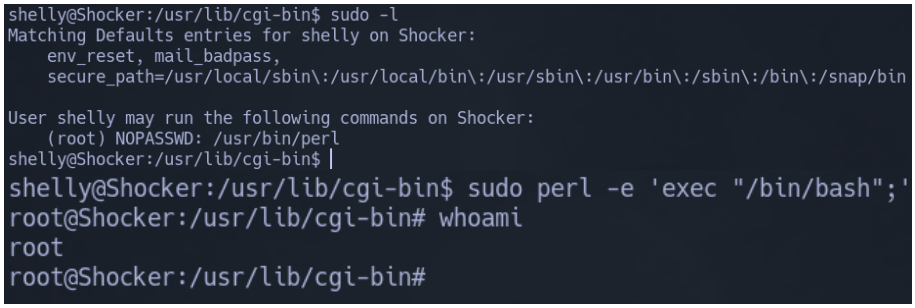
Proof of Concept

- *Initial Access*



User flag: 5ed6e9e418d60b4cdacbcc568e8f6ebe

- *Privilege Escalation*



Root flag: 27adf3538e39d2d2c3e18b5316cd12d9