RAHUL KUMAR
rahulwell1997@gmail.com

Project: **Penetration Testing on Web Server**

Website: ____Certfied Hacker___**(cerifiedhacker.com)**___________

Footprinting and Reconnaissance

Supportive ScreenShorts On **Footprinting and Reconnaissance** **Google Drive Link**

Click link ScreenShorts

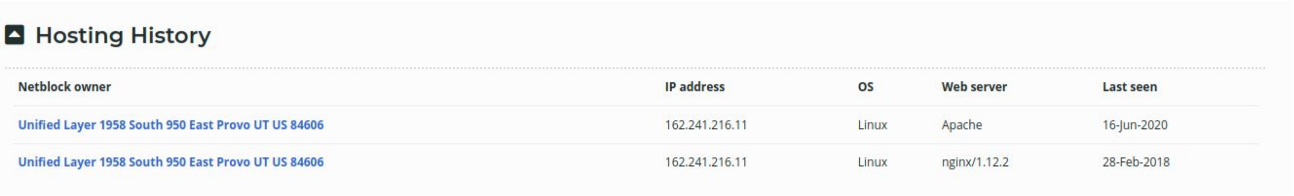
1. About company

Testing Website for Attack And finding vulnerability

2. IP address of Website

162.241.216.11

3. Location of server



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	16-Jun-2020
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Feb-2018

United States

4. Operating System of server

Linux

5. Web server technology and version

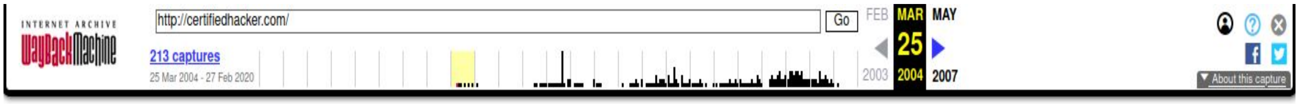
Apache

6. Built in technology

- Google Font API
- jQuery
- jQuery Migrate
- MySQL
- PHP
- Twitter
- WordPress
- Yoast SEO

7. When website first seen

25/03/2004
checking on web.archive.org



8. Previous technology used by website
//Support from netcraft.com

Netblock owner	IP address	OS	Web server	Last seen
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	Apache	6-Jul-2020
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.14.1	29-May-2019
Unified Layer 1958 South 950 East Provo UT US 84606	162.241.216.11	Linux	nginx/1.12.2	28-Nov-2018

Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	-	nginx/1.12.1	5-Nov-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	Apache	17-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.1	6-Oct-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.12.0	28-May-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.2	15-Apr-2017
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.1	19-Oct-2016
Unified Layer 1958 South 950 East Provo UT US 84606	69.89.31.193	Linux	nginx/1.10.0	31-May-2016

9. Which ISP IP range server is using

```
NetRange:       162.240.0.0 - 162.241.255.255
CIDR:           162.240.0.0/15
```

10. Do any other domains are on same server, if yes domain names

Complete List Present on this Link(bgp.he.net)

11. Ports open on Webserver

- 21
- 22
- 26
- 53
- 80
- 110
- 443
- 995

//support from dmitry -p certifiedhacker.com

12. Registrar information of domain

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2019-08-22T08:13:02Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2021-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
```

//getting info by complete list Url

13. Email ID of some employees of company

abuse@web.com

14. Social Networking Profiles of employees

```
Usufy -n certifiedhacker.com -p youtube twitter facebook
Searchfy -q certifiedhacker.com
```

15. LinkedIn Search for profiles with company name

Osrframework using

```
Usufy -n certifiedhacker.com -p youtube twitter facebook
Searchfy -q certifiedhacker.com
```

16. Address of company

PERFECT PRIVACY, LLC
5335 Gate Parkway care of Network Solutions PO Box 459,
Jacksonville, FL, 32256, us
r69rg8833re@networksolutionsprivateregistration.com
(p) 15707088780

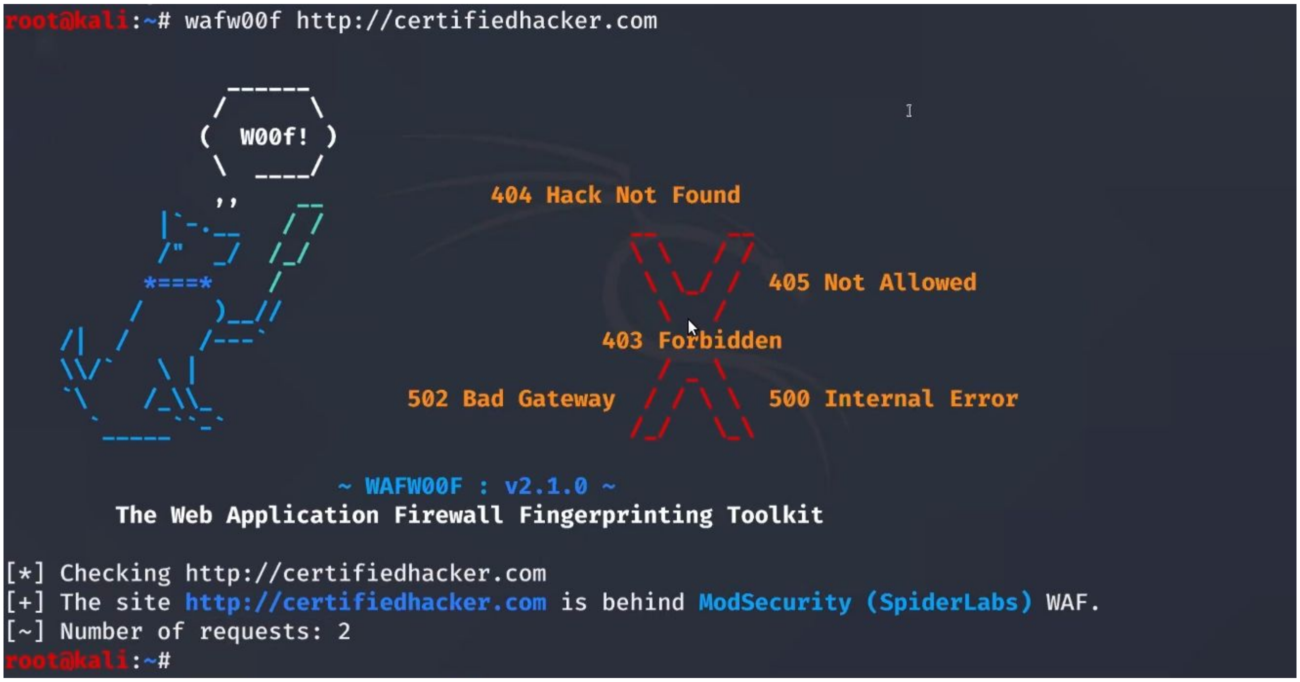
17. Director/CEO of company

NA

18. Check firewall and load balancer presence

Certifiedhacker.com doesn't use any load Balancing.
lbd certifiedhacker.com

Command as--
wafwoof http://certiidhacker.com



```
root@kali:~# wafw00f http://certifiedhacker.com
```

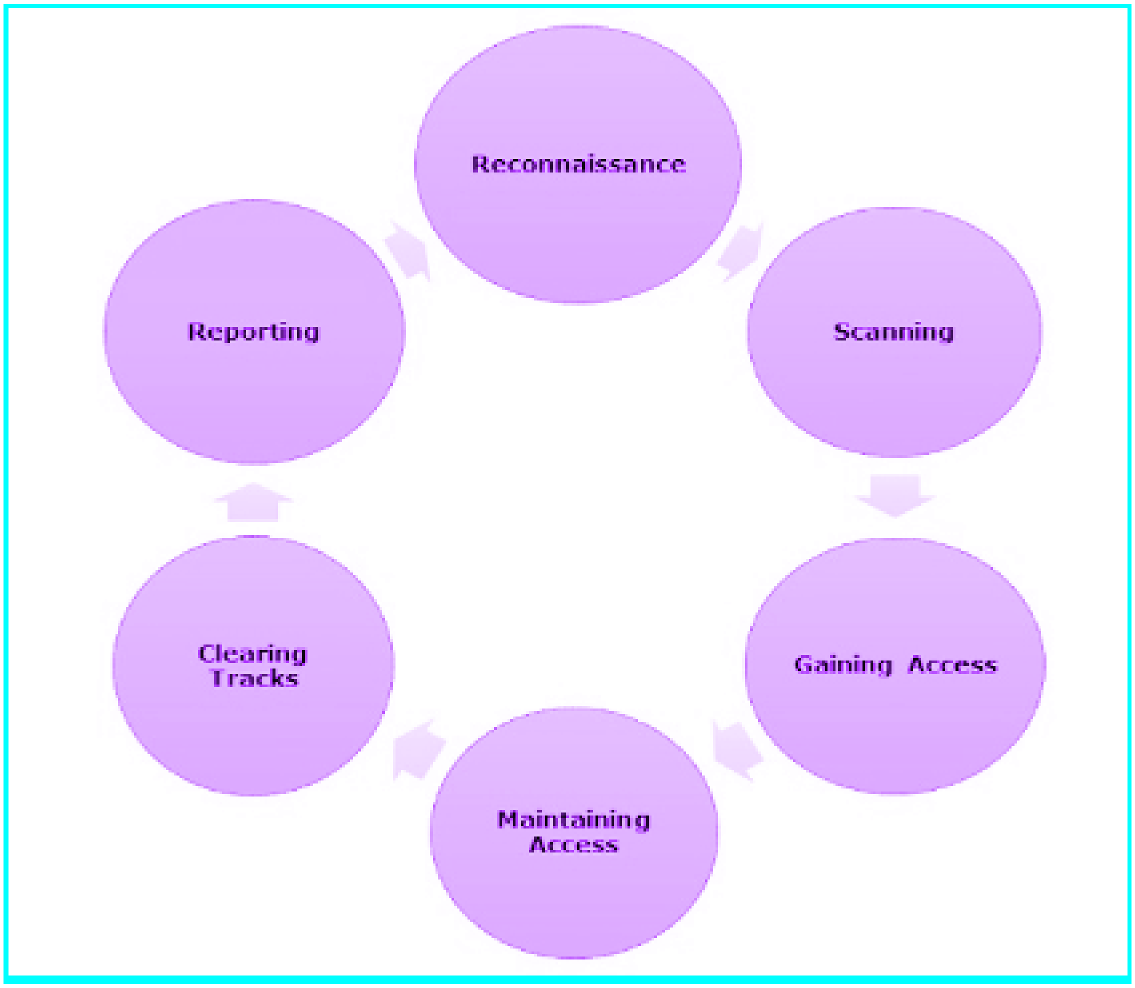
```
                    ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://certifiedhacker.com
[+] The site http://certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.
[~] Number of requests: 2
root@kali:~#
```

19. Check directory listing, if enabled write the directory structure

NA

20. Check for files such as robots.txt and sites.xml

NA



Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus,and NMAP.

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks

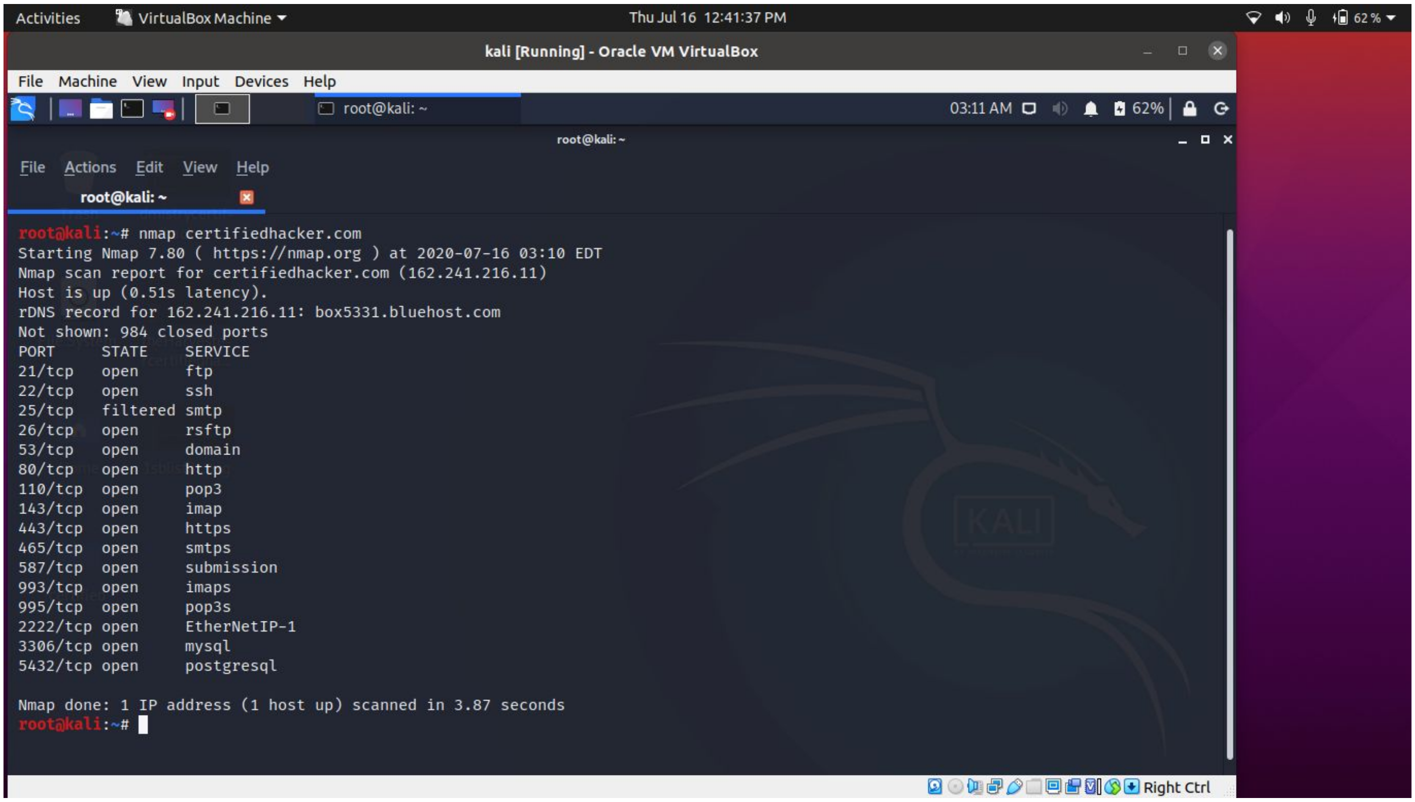
This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

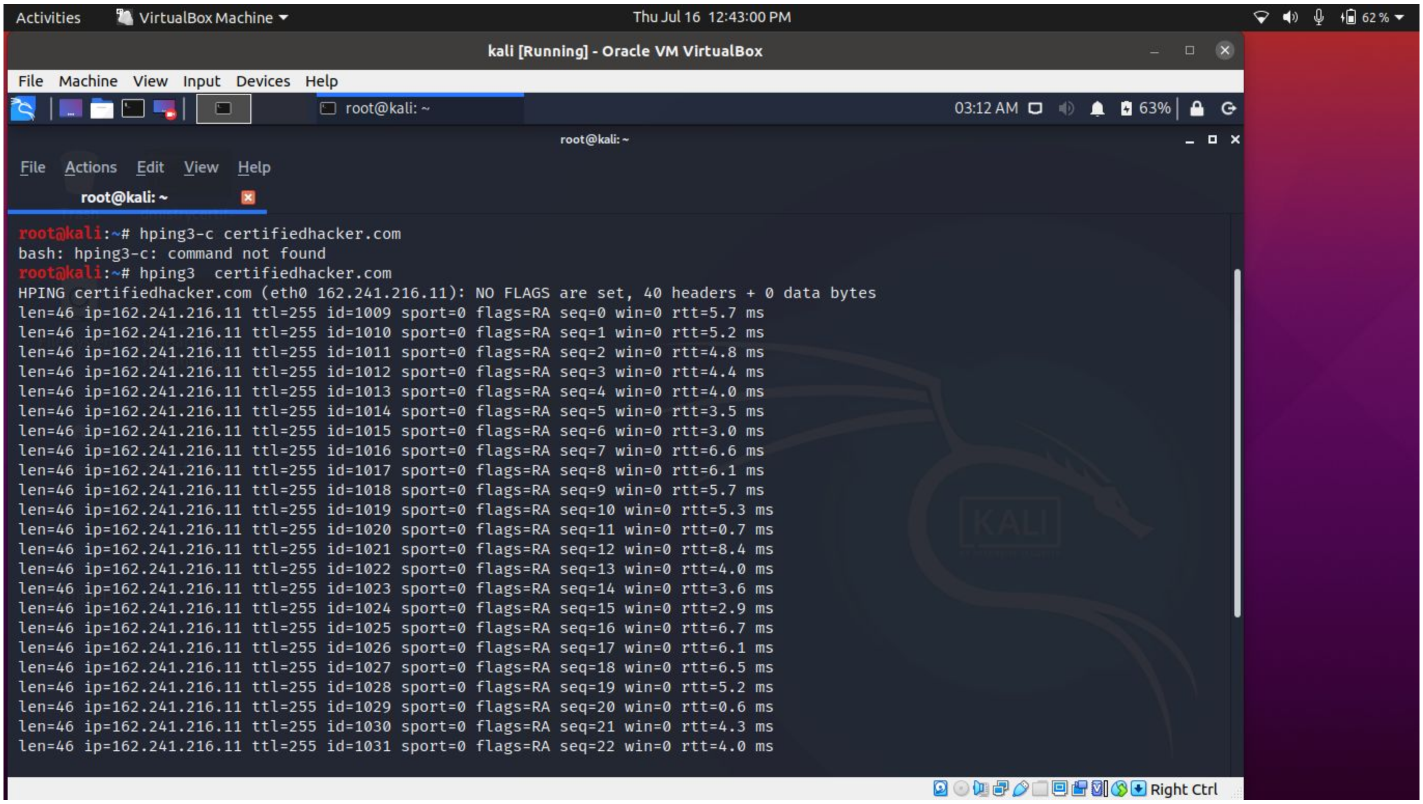
Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

2. Based on the Information from above source, scan the website of company for vulnerabilities

through different scanners, make a report on vulnerability which you find there.


Activities
VirtualBox Machine
Thu Jul 16 12:41:37 PM
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
03:11 AM
62%
File Actions Edit View Help
Right Ctrl

```
root@kali:~# nmap certifiedhacker.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 03:10 EDT
Nmap scan report for certifiedhacker.com (162.241.216.11)
Host is up (0.51s latency).
rDNS record for 162.241.216.11: box5331.bluehost.com
Not shown: 984 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
25/tcp   filtered smtp
26/tcp   open     rsftp
53/tcp   open     domain
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap
443/tcp  open     https
465/tcp  open     smtps
587/tcp  open     submission
993/tcp  open     imaps
995/tcp  open     pop3s
2222/tcp open     EtherNetIP-1
3306/tcp open     mysql
5432/tcp open     postgresql

Nmap done: 1 IP address (1 host up) scanned in 3.87 seconds
root@kali:~# 
```

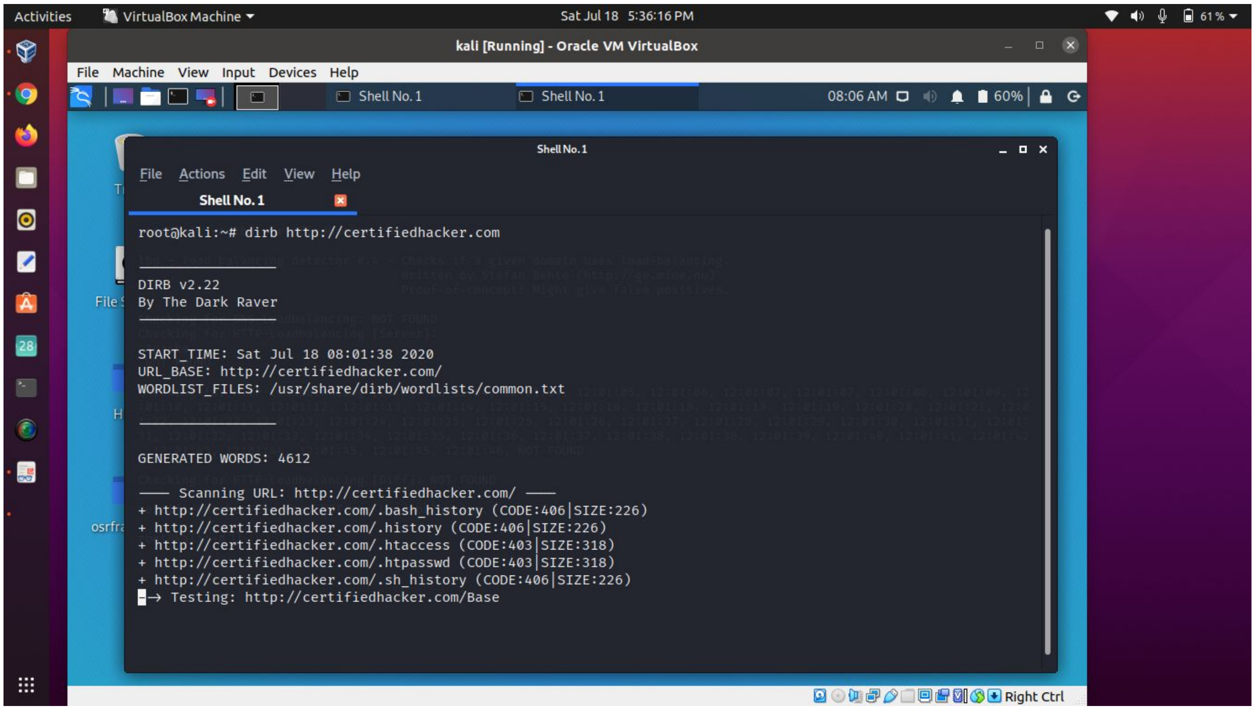

Activities
VirtualBox Machine
Thu Jul 16 12:43:00 PM
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
03:12 AM
63%
File Actions Edit View Help
Right Ctrl

```
root@kali:~# hping3-c certifiedhacker.com
bash: hping3-c: command not found
root@kali:~# hping3  certifiedhacker.com
HPING certifiedhacker.com (eth0 162.241.216.11): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=162.241.216.11 ttl=255 id=1009 sport=0 flags=RA seq=0 win=0 rtt=5.7 ms
len=46 ip=162.241.216.11 ttl=255 id=1010 sport=0 flags=RA seq=1 win=0 rtt=5.2 ms
len=46 ip=162.241.216.11 ttl=255 id=1011 sport=0 flags=RA seq=2 win=0 rtt=4.8 ms
len=46 ip=162.241.216.11 ttl=255 id=1012 sport=0 flags=RA seq=3 win=0 rtt=4.4 ms
len=46 ip=162.241.216.11 ttl=255 id=1013 sport=0 flags=RA seq=4 win=0 rtt=4.0 ms
len=46 ip=162.241.216.11 ttl=255 id=1014 sport=0 flags=RA seq=5 win=0 rtt=3.5 ms
len=46 ip=162.241.216.11 ttl=255 id=1015 sport=0 flags=RA seq=6 win=0 rtt=3.0 ms
len=46 ip=162.241.216.11 ttl=255 id=1016 sport=0 flags=RA seq=7 win=0 rtt=6.6 ms
len=46 ip=162.241.216.11 ttl=255 id=1017 sport=0 flags=RA seq=8 win=0 rtt=6.1 ms
len=46 ip=162.241.216.11 ttl=255 id=1018 sport=0 flags=RA seq=9 win=0 rtt=5.7 ms
len=46 ip=162.241.216.11 ttl=255 id=1019 sport=0 flags=RA seq=10 win=0 rtt=5.3 ms
len=46 ip=162.241.216.11 ttl=255 id=1020 sport=0 flags=RA seq=11 win=0 rtt=0.7 ms
len=46 ip=162.241.216.11 ttl=255 id=1021 sport=0 flags=RA seq=12 win=0 rtt=8.4 ms
len=46 ip=162.241.216.11 ttl=255 id=1022 sport=0 flags=RA seq=13 win=0 rtt=4.0 ms
len=46 ip=162.241.216.11 ttl=255 id=1023 sport=0 flags=RA seq=14 win=0 rtt=3.6 ms
len=46 ip=162.241.216.11 ttl=255 id=1024 sport=0 flags=RA seq=15 win=0 rtt=2.9 ms
len=46 ip=162.241.216.11 ttl=255 id=1025 sport=0 flags=RA seq=16 win=0 rtt=6.7 ms
len=46 ip=162.241.216.11 ttl=255 id=1026 sport=0 flags=RA seq=17 win=0 rtt=6.1 ms
len=46 ip=162.241.216.11 ttl=255 id=1027 sport=0 flags=RA seq=18 win=0 rtt=6.5 ms
len=46 ip=162.241.216.11 ttl=255 id=1028 sport=0 flags=RA seq=19 win=0 rtt=5.2 ms
len=46 ip=162.241.216.11 ttl=255 id=1029 sport=0 flags=RA seq=20 win=0 rtt=0.6 ms
len=46 ip=162.241.216.11 ttl=255 id=1030 sport=0 flags=RA seq=21 win=0 rtt=4.3 ms
len=46 ip=162.241.216.11 ttl=255 id=1031 sport=0 flags=RA seq=22 win=0 rtt=4.0 ms
```

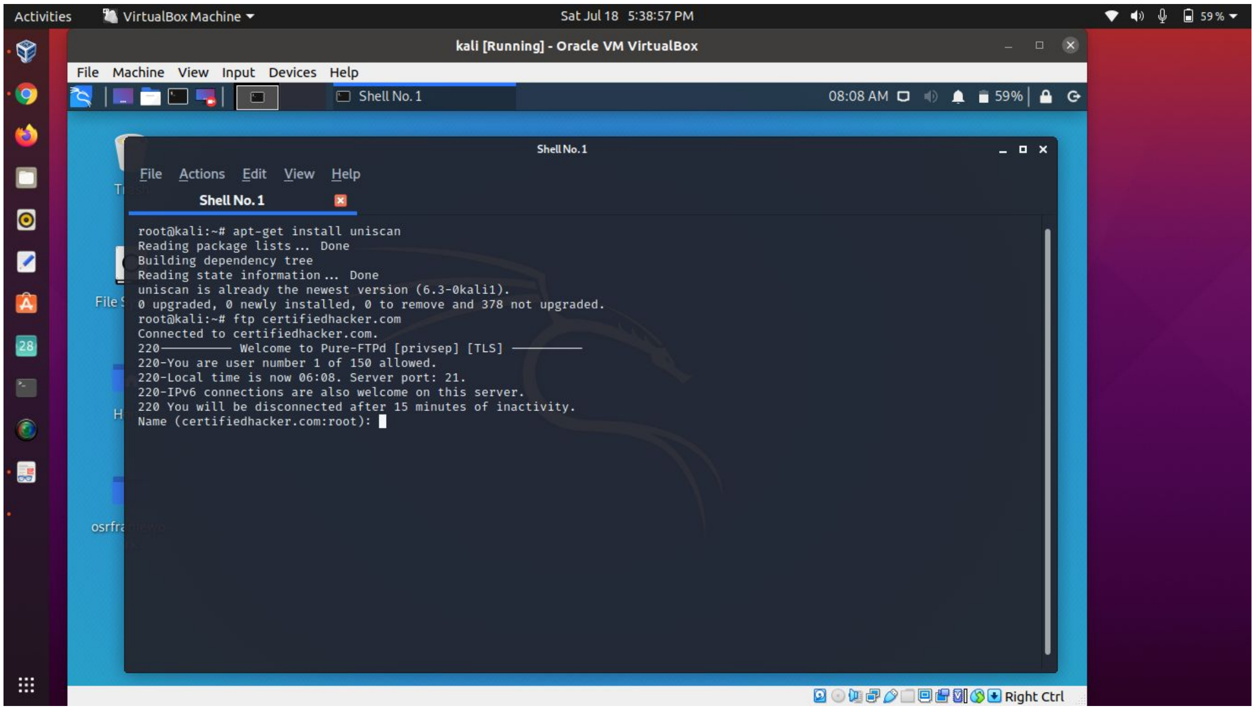
3. Try to hack that server for services which you found there like ftp, login passwords. In report

write the tools which you have used to hack on that server and its output.

4. Check for database and try to get into database..



```
root@kali:~# dirb http://certifiedhacker.com

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

START_TIME: Sat Jul 18 08:01:38 2020
URL_BASE: http://certifiedhacker.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://certifiedhacker.com/ ----
+ http://certifiedhacker.com/.bash_history (CODE:406|SIZE:226)
+ http://certifiedhacker.com/.history (CODE:406|SIZE:226)
+ http://certifiedhacker.com/.htaccess (CODE:403|SIZE:318)
+ http://certifiedhacker.com/.htpasswd (CODE:403|SIZE:318)
+ http://certifiedhacker.com/.sh_history (CODE:406|SIZE:226)
--> Testing: http://certifiedhacker.com/Base
```



```
root@kali:~# apt-get install uniscan
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
uniscan is already the newest version (6.3-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 378 not upgraded.
root@kali:~# ftp certifiedhacker.com
Connected to certifiedhacker.com.
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 150 allowed.
220-Local time is now 06:08. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (certifiedhacker.com:root): 
```

**5. Write the final conclusion that you got from above process, if you found any vulnerabilities
then how those vulnerabilities can be cover and if not, then also how much secured server is.**

Conclusion

certifiedhacker.com One suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on **certifiedhacker.com** One operations if a malicious party had exploited them. Current policies concerning password reuse and deployed access controls are not adequate to mitigate the impact of the discovered vulnerabilities.

Recommendations

Due to the impact to the overall organization as uncovered by this penetration test, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high level items are important to mention.

1. Ensure that strong credentials are use everywhere in the organization

2. Establish trust boundaries

3. Implement and enforce implementation of change control across all systems

4. Implement a patch management program

5. Conduct regular vulnerability assessments

Risk Rating

The overall risk identified to certifiedhacker.com One as a result of the penetration test is **High**. A direct path from external attacker to full system compromise was discovered. It is reasonable to believe that a malicious entity would be able to successfully execute an attack against certifiedhacker.com One through targeted attacks.

RAHUL KUMAR
rahulwell1997@gmail.com
Linkedin