Penetration Test Report

FSociety

April 09th, 2023

Optex

Anastasiya Sousa
4716-099
Rua da Ribeira n45
Braga
Portugal
Tel: 351-965-364-815
Email: info@optex.pt
Web: http://www.optex.pt

Table of Contents

Executive Summary

Anastasiya Sousa was contracted by FSociety to conduct a penetration test to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against FSociety with the goals of:

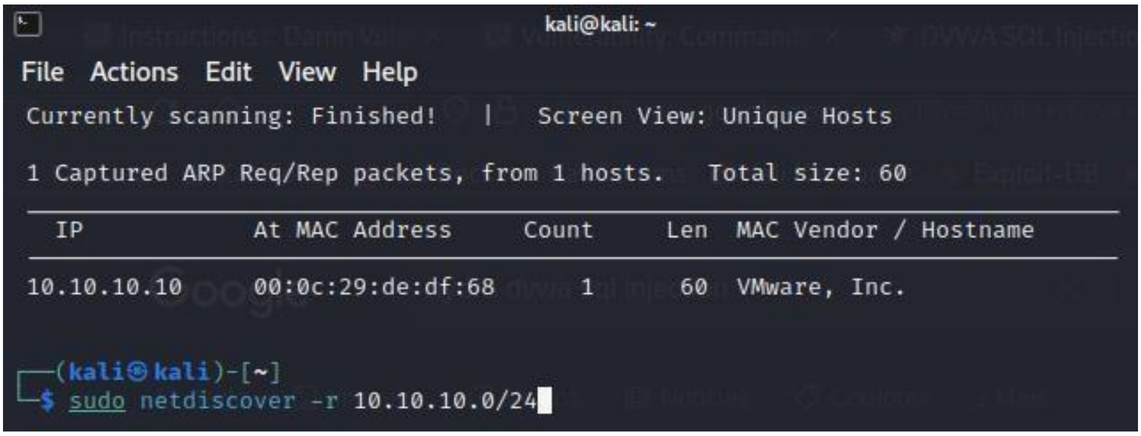
- Identifying if a remote attacker could penetrate FSociety's defenses
- Determining the impact of a security breach on:
    - Confidentiality of the company's private data
    - Internal infrastructure and availability of FSociety's information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-1151 with all tests and actions being conducted under controlled conditions.

Remote System Acknowledge

For the purposes of this assessment, FSociety provided minimal information: network address 10.10.10.0/24. The intent was to discover the Debian virtual machine's IP address, knowing only network address. To identify the correct IP address, we ran the acknowledge command.

(Figure 1).



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.10.10.10     00:0c:29:de:df:68     1       60  VMware, Inc.

┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 10.10.10.0/24
```

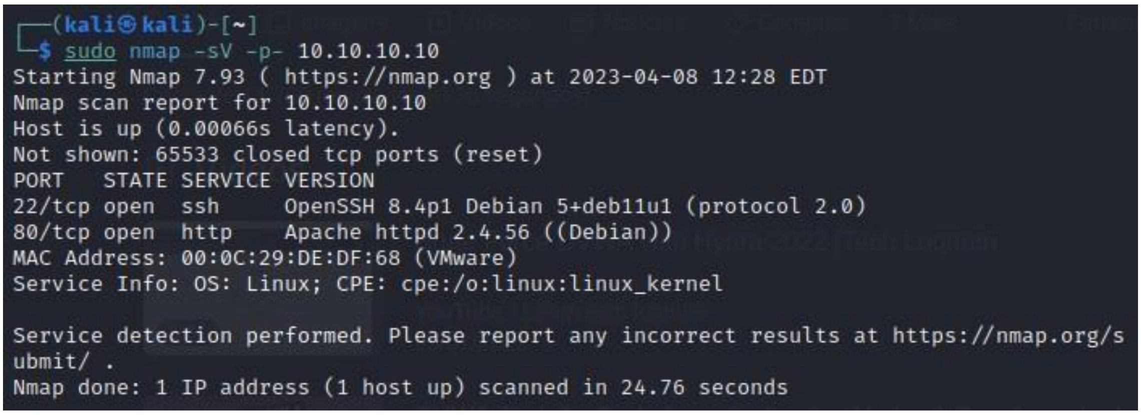
Figure 1 – Acknowledge command for network 10.10.10.0/24 to identify IP address

Information gathered for 10.10.10.0/24 reveals one active IP address 10.10.10.10 with a VMware hostname, which is eventually Debian virtual machine.

Scanning information about IP address

Next step was to conduct scanning of 10.10.10.10 to discover opened ports and running services' versions.

To perform scanning, we ran a scanning command (Figure 2).



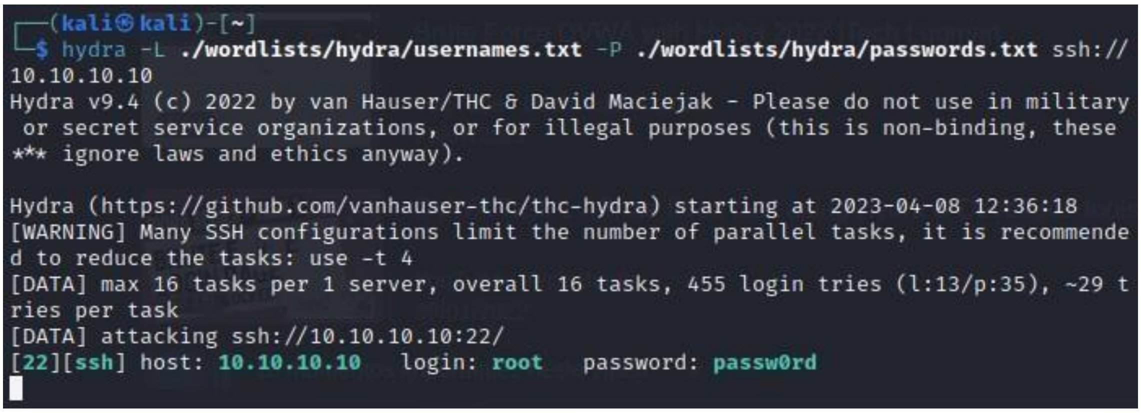
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- 10.10.10.10
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 12:28 EDT
Nmap scan report for 10.10.10.10
Host is up (0.00066s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
MAC Address: 00:0C:29:DE:DF:68 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.76 seconds
```

Figure 2 – Scanning 10.10.10.10 to identify opened ports

Information gathered for 10.10.10.10 reveals that Debian virtual machine has 2 opened ports with running services: ssh and http. So, after we can use this information to perform vulnerability attack of ssh service.

Brute-force attack

The next step was to prepare a targeted brute-force attempt against the system. We compiled custom files based on the content of thegoodpirate repositories from https://github.com/thegoodpirate. As a result, 2 files were created: 1 with passwords and another one with usernames. Each file consisted of 5 words (Figure 3).



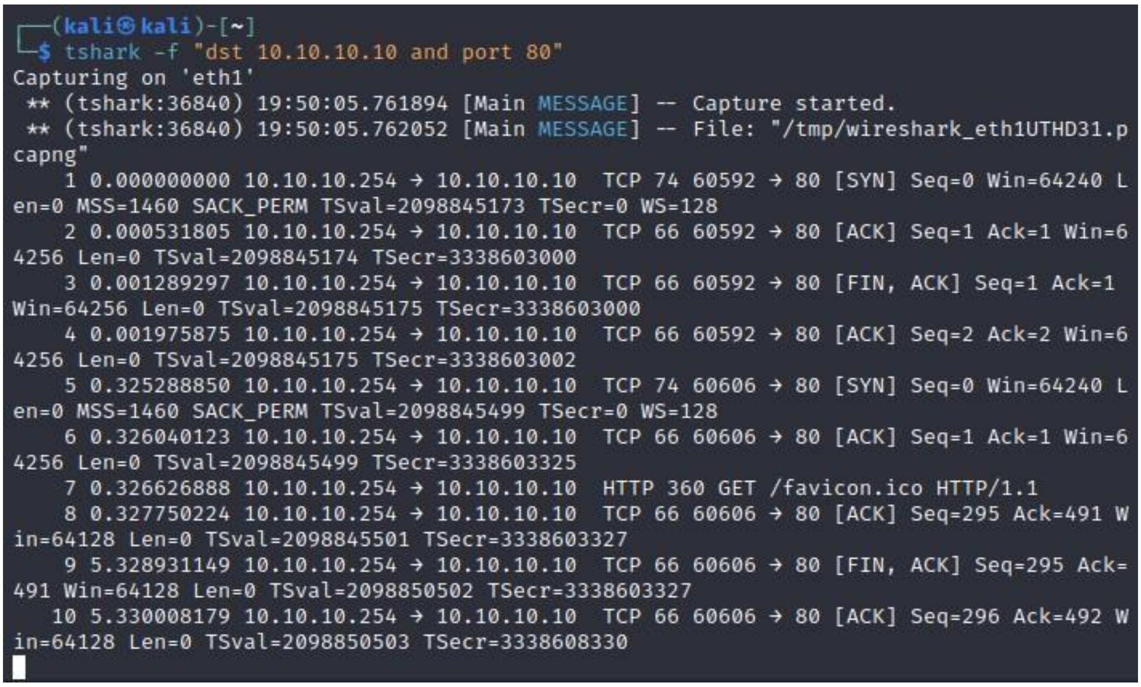
```
┌──(kali㉿kali)-[~]
└─$ hydra -L ./wordlists/hydra/usernames.txt -P ./wordlists/hydra/passwords.txt ssh://
10.10.10.10
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military
 or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-04-08 12:36:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommende
d to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 455 login tries (l:13/p:35), ~29 t
ries per task
[DATA] attacking ssh://10.10.10.10:22/
[22][ssh] host: 10.10.10.10   login: root   password: passw0rd
█
```

Figure 3 – Performing brute-force attack against ssh server to gain unauthorized access to organizational data

This brute-force attack uncovered the password of “passw0rd” and the username of “root”. We were able to leverage these credentials to successfully gain unauthorized access to SSH service of the target attack – Debian virtual machine with IP address 10.10.10.10.

Real-time traffic monitoring

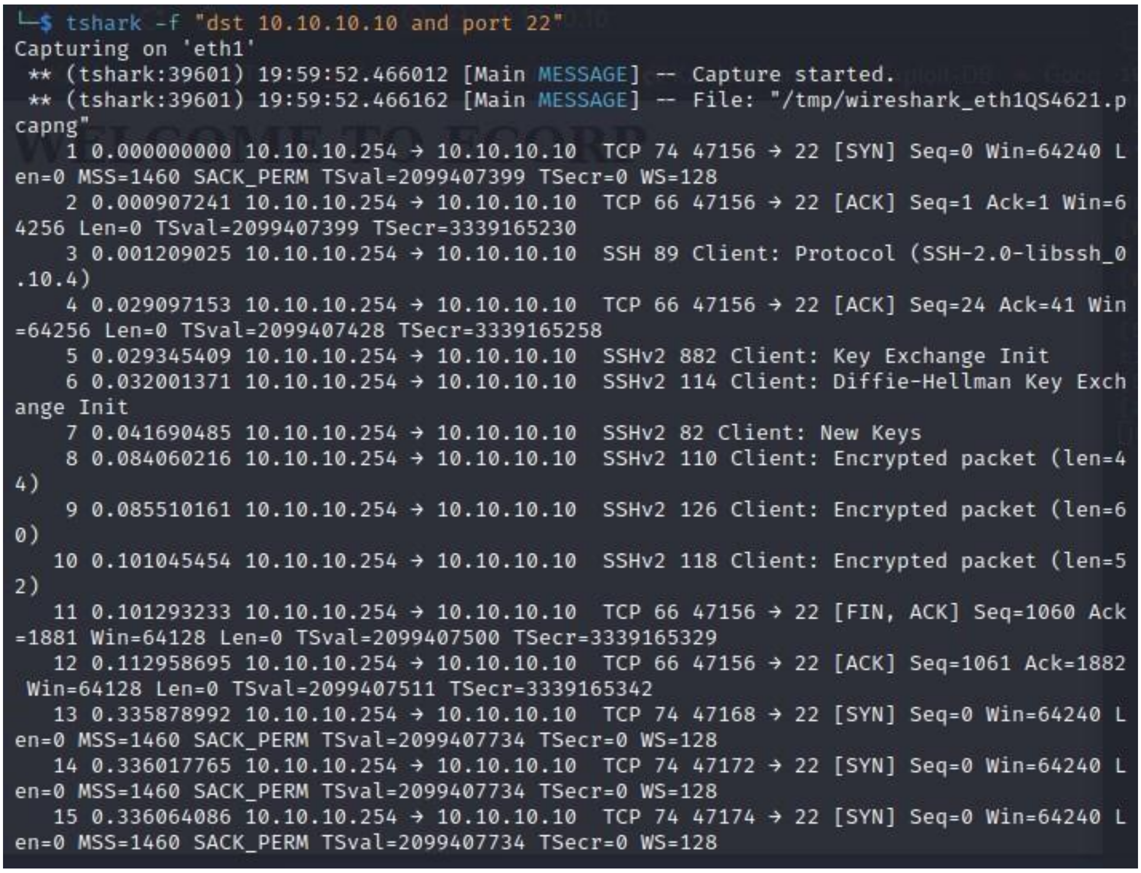
Next, the passive attack command was used to monitor the traffic sent to the http (Figure 4) and ssh services (Figure 5).



```
┌──(kali㉿kali)-[~]
└─$ tshark -f "dst 10.10.10.10 and port 80"
Capturing on 'eth1'
 ** (tshark:36840) 19:50:05.761894 [Main MESSAGE] -- Capture started.
 ** (tshark:36840) 19:50:05.762052 [Main MESSAGE] -- File: "/tmp/wireshark_eth1UTHD31.p
capng"
    1 0.000000000 10.10.10.254 → 10.10.10.10  TCP 74 60592 → 80 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2098845173 TSecr=0 WS=128
    2 0.000531805 10.10.10.254 → 10.10.10.10  TCP 66 60592 → 80 [ACK] Seq=1 Ack=1 Win=6
4256 Len=0 TSval=2098845174 TSecr=3338603000
    3 0.001289297 10.10.10.254 → 10.10.10.10  TCP 66 60592 → 80 [FIN, ACK] Seq=1 Ack=1
Win=64256 Len=0 TSval=2098845175 TSecr=3338603000
    4 0.001975875 10.10.10.254 → 10.10.10.10  TCP 66 60592 → 80 [ACK] Seq=2 Ack=2 Win=6
4256 Len=0 TSval=2098845175 TSecr=3338603002
    5 0.325288850 10.10.10.254 → 10.10.10.10  TCP 74 60606 → 80 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2098845499 TSecr=0 WS=128
    6 0.326040123 10.10.10.254 → 10.10.10.10  TCP 66 60606 → 80 [ACK] Seq=1 Ack=1 Win=6
4256 Len=0 TSval=2098845499 TSecr=3338603325
    7 0.326626888 10.10.10.254 → 10.10.10.10  HTTP 360 GET /favicon.ico HTTP/1.1
    8 0.327750224 10.10.10.254 → 10.10.10.10  TCP 66 60606 → 80 [ACK] Seq=295 Ack=491 W
in=64128 Len=0 TSval=2098845501 TSecr=3338603327
    9 5.328931149 10.10.10.254 → 10.10.10.10  TCP 66 60606 → 80 [FIN, ACK] Seq=295 Ack=
491 Win=64128 Len=0 TSval=2098850502 TSecr=3338603327
   10 5.330008179 10.10.10.254 → 10.10.10.10  TCP 66 60606 → 80 [ACK] Seq=296 Ack=492 W
in=64128 Len=0 TSval=2098850503 TSecr=3338608330
```

Figure 4 – Traffic monitoring sent to http service (port 80)

In Figure 4 we don't see anything unusual. What we can notice is that the client firstly sends SYNs and responds with ACKs before the connection starts and then ends the connection with FINs and ACKs (3-way handshake of TCP protocol).



```
└─$ tshark -f "dst 10.10.10.10 and port 22"
Capturing on 'eth1'
 ** (tshark:39601) 19:59:52.466012 [Main MESSAGE] -- Capture started.
 ** (tshark:39601) 19:59:52.466162 [Main MESSAGE] -- File: "/tmp/wireshark_eth1QS4621.p
capng"
    1 0.000000000 10.10.10.254 → 10.10.10.10  TCP 74 47156 → 22 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2099407399 TSecr=0 WS=128
    2 0.000907241 10.10.10.254 → 10.10.10.10  TCP 66 47156 → 22 [ACK] Seq=1 Ack=1 Win=6
4256 Len=0 TSval=2099407399 TSecr=3339165230
    3 0.001209025 10.10.10.254 → 10.10.10.10  SSH 89 Client: Protocol (SSH-2.0-libssh_0
.10.4)
    4 0.029097153 10.10.10.254 → 10.10.10.10  TCP 66 47156 → 22 [ACK] Seq=24 Ack=41 Win
=64256 Len=0 TSval=2099407428 TSecr=3339165258
    5 0.029345409 10.10.10.254 → 10.10.10.10  SSHv2 882 Client: Key Exchange Init
    6 0.032001371 10.10.10.254 → 10.10.10.10  SSHv2 114 Client: Diffie-Hellman Key Exch
ange Init
    7 0.041690485 10.10.10.254 → 10.10.10.10  SSHv2 82 Client: New Keys
    8 0.084060216 10.10.10.254 → 10.10.10.10  SSHv2 110 Client: Encrypted packet (len=4
4)
    9 0.085510161 10.10.10.254 → 10.10.10.10  SSHv2 126 Client: Encrypted packet (len=6
0)
   10 0.101045454 10.10.10.254 → 10.10.10.10  SSHv2 118 Client: Encrypted packet (len=5
2)
   11 0.101293233 10.10.10.254 → 10.10.10.10  TCP 66 47156 → 22 [FIN, ACK] Seq=1060 Ack
=1881 Win=64128 Len=0 TSval=2099407500 TSecr=3339165329
   12 0.112958695 10.10.10.254 → 10.10.10.10  TCP 66 47156 → 22 [ACK] Seq=1061 Ack=1882
 Win=64128 Len=0 TSval=2099407511 TSecr=3339165342
   13 0.335878992 10.10.10.254 → 10.10.10.10  TCP 74 47168 → 22 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2099407734 TSecr=0 WS=128
   14 0.336017765 10.10.10.254 → 10.10.10.10  TCP 74 47172 → 22 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2099407734 TSecr=0 WS=128
   15 0.336064086 10.10.10.254 → 10.10.10.10  TCP 74 47174 → 22 [SYN] Seq=0 Win=64240 L
en=0 MSS=1460 SACK_PERM TSval=2099407734 TSecr=0 WS=128
```

Figure 5 – Traffic monitoring sent to ssh service (port 22)

In Figure 5 we can notice that someone was trying to gain unauthorized access to organizational data by brute-forcing the username and password.

Recommendations

Due to the impact on 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.

Optex recommends the following:

1. Ensure that strong credentials are used everywhere in the organization. The compromise of FSociety system has drastically impacted using weak password and username.

2. Conduct regular vulnerability assessments. As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are properly installed, operating as intended, and producing the desired outcome.