Penetration Testing Report

Applied Information Assurance – IE3022

IT19122410 – W. P. T. Pamalka

Contents

Table of Contents

Executive Summery

An extensive penetration testing was carried out on Gojo Corporation in order to outline the vulnerabilities and weakness that can be found within the company's network and application. As a result, our team divided in to 3 groups in order to analyze the network and applications both internally and externally, analyze the how effective the company is when its under an attack and testing out defense strategies and controls on found vulnerabilities.

The company did not specify any zones to be 0 limits therefore the test and analysis were carried out within the whole system. When the penetration testing was carried out, several vulnerabilities were found with the system. Therefore, an impact assessment outlining the impacts of the newly founded vulnerabilities was created. Furthermore, the analysis of the effectiveness of current controls were also included in the analysis report.

Lastly, the improvements that should be made for the system and the current controls ad mitigation techniques were included in order to provide the best service. Overall, the security of the Gojo Corporation is at a very acceptable level with only common vulnerabilities detected during the penetration testing. It is recommended that the company begins implementing the recommended techniques and improvements in order to achieve a secured system.

Abstract

This report includes the details of a penetration testing that was carried on the system of Gojo Corporation. The purpose of conducting the penetration testing was to:

1. identify vulnerabilities within the system
2. assure that current controls are functioning during threats
3. improvements on current mitigation techniques

Once the penetration testing was completed and all the above requirements were fulfilled the team came up with an impact assessment which outlined the vulnerabilities found within the system, effectiveness of currently placed controls, improvements that need to be made for current mitigation methods and new mitigations that were not available within the systems.

Scenario

Gojo Corporation is leading security manufacturing company that produce home security systems to government inquired security equipment that aren't available on the market. Due to the sudden rise of security breaches because of Covid – 19, the company has reached to a conclusion of carrying out a penetration test on their systems without any limitations to obtain the maximum results of this penetration test.

Teams Red, Blue and Purple will conduct the penetration testing in 3 categories.

- Team Red will carry out an assessment of network both internally and externally.
- Team Blue will analyze the Red teams finding to determined how the company will respond to an attack with current security measures.
- Team Purple will analyze the effectiveness of current defense mechanisms

Methodology

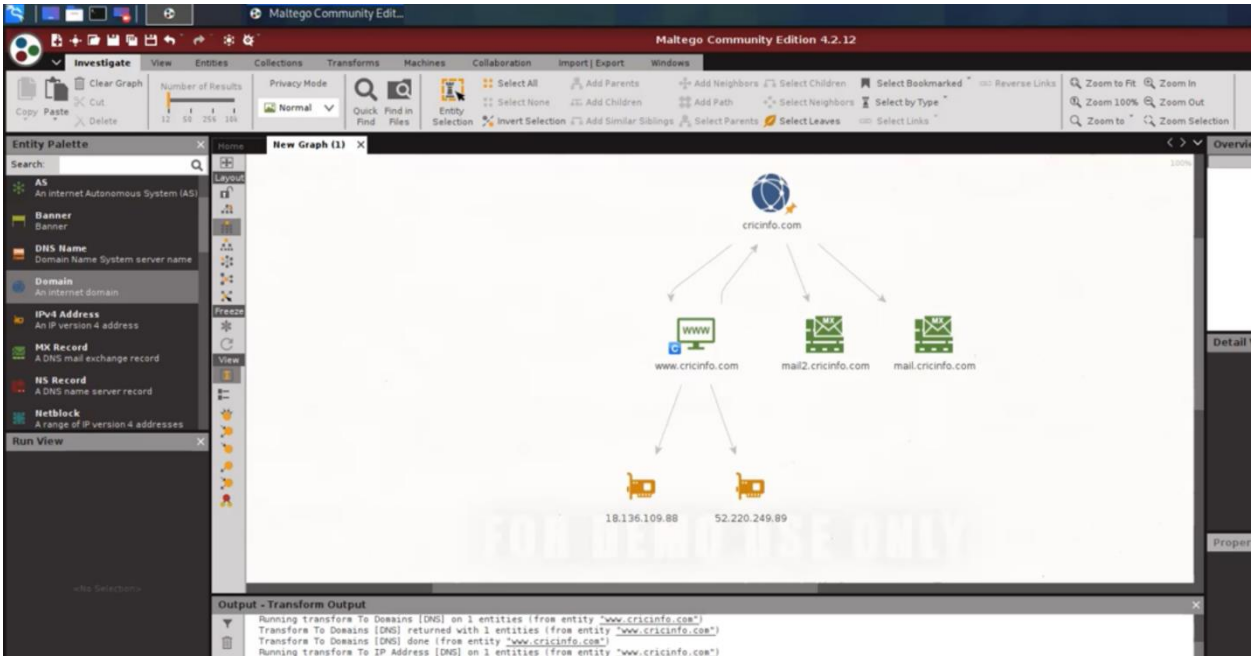
Foot Printing & Reconnaissance

This can be identified as the stage of gathering information. During this period, the penetration testers gather as much publicly available information regarding the target through various sources (hosts, network and people related to the target). This process helps testers to understand the target's functionality and its system.

There are many tools and techniques available to conduct a foot printing and reconnaissance such as Maltego, Recon-ng Framework, Google Hacking, Netcraft, Shodan and more. For this assessment, we have utilized Maltego, Recon-ng Framework and Harvester tools.

Maltego

This tool uncovers people who are linked to the target such as their social media profiles, mutual friends, other companies and websites related to the target.

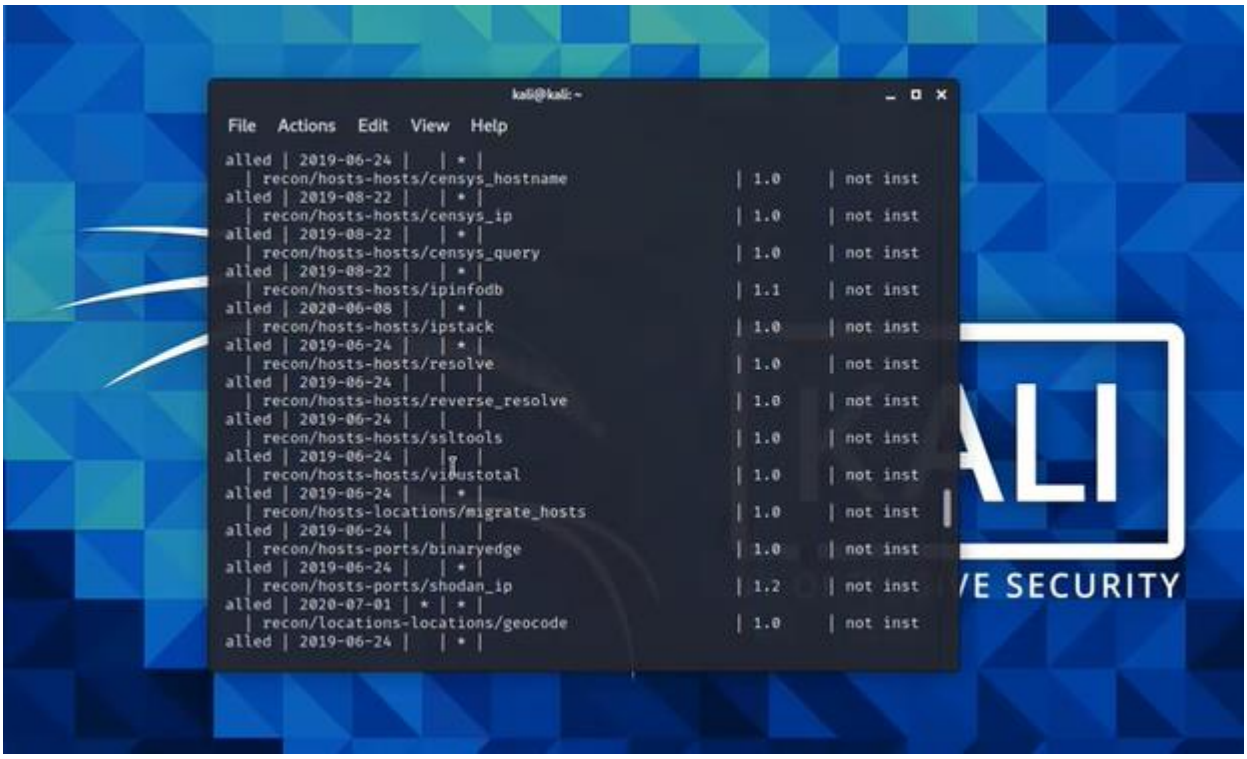


Once the targets domain name was entered to the Maltego, a quick look up on the website was done. Then, a check up was done to check all available DNS and 2 IP addresses were found related to the target website. Later another check up was conducted for mail servers and 2 mail servers relating to the target were found.

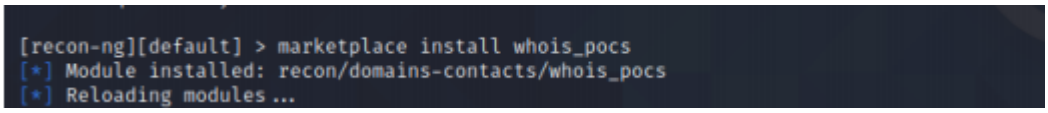
Recon-ng Framework

Recon-ng is a powerful open-source web-based source that can conduct a reconnaissance very quickly and thoroughly due to its complete features such as independent modules, database interactions, built in convenience functions and more

First, and module must be uploaded to the Recon-ng. a module is a task that will be executed based on the parameters the user gives. In order to find all available modules that can be used to find information “marketplace search” command should be entered to the prompt.



To install a module command “marketplace install [whois_pocs]” is entered to the prompt.



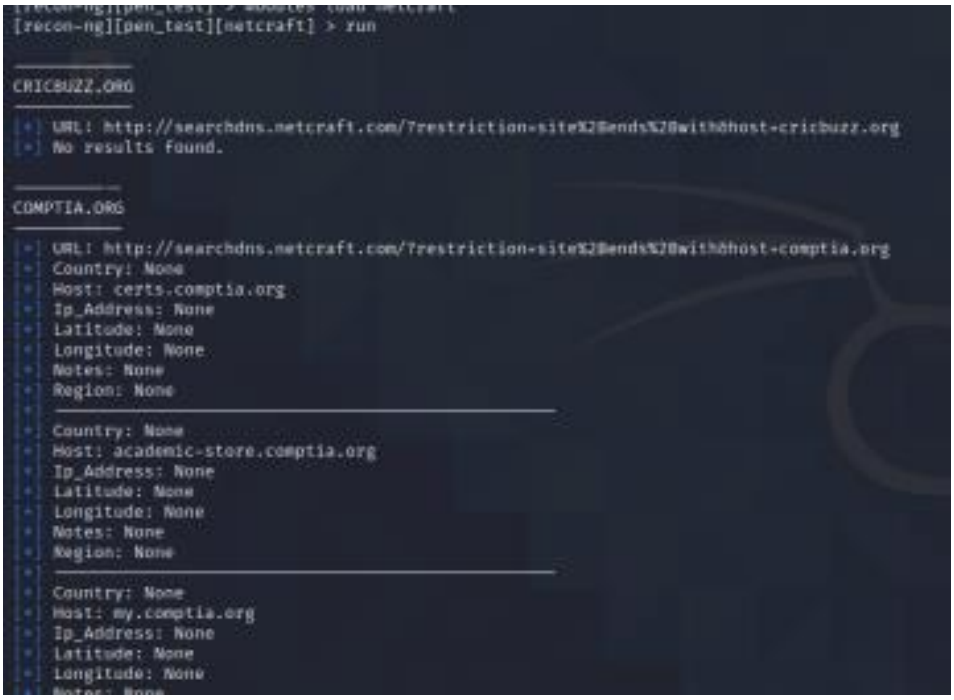
To start the foot printing process a workspace is created using “workspaces create [pen_test]”

```
kali@kali: ~
File  Actions  Edit  View  Help

  Reporting
  ---------
    reporting/html

[recon-ng][default] > workspaces create pen_test
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail
at runtime. See 'keys add'.
[!] 'github_api' key not set. github_users module will likely fail at runti
me. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at
runtime. See 'keys add'.
[!] Module 'recon/companies-contacts/censys_email_address' disabled. Depend
ency required: ''censys''.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency requir
ed: ''PyPDF3''.
[!] 'hunter_io' key not set. hunter_io module will likely fail at runtime.
See 'keys add'.
[!] 'github_api' key not set. github_commits module will likely fail at run
time. See 'keys add'.
[!] 'fullcontact_api' key not set. fullcontact module will likely fail at r
untime. See 'keys add'.
[!] 'hibp_api' key not set. hibp_breach module will likely fail at runtime.
 See 'keys add'.
[!] 'hibp_api' key not set. hibp_paste module will likely fail at runtime.
See 'keys add'.
[recon-ng][pen_test] >
```

The next step is to set a target domain. The command “db insert domains [gojo.com]” is used to gather information regarding the target’s domain.

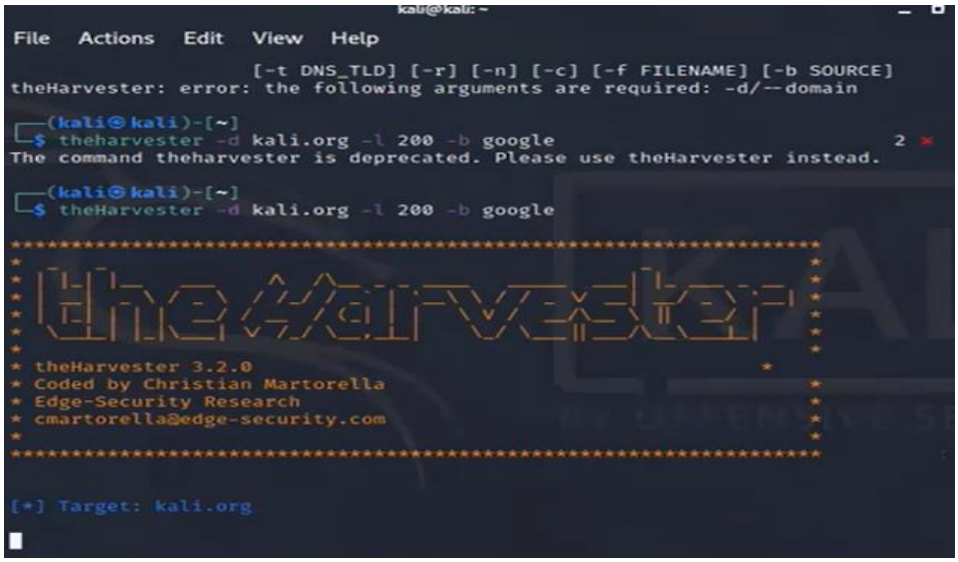
```
[recon-ng][pen_test] > db insert domain
[*] Invalid table name.
[recon-ng][pen_test] > db insert domains
domain (TEXT): kali.org
notes (TEXT): 123
[*] 1 rows affected.
[recon-ng][pen_test] >
```

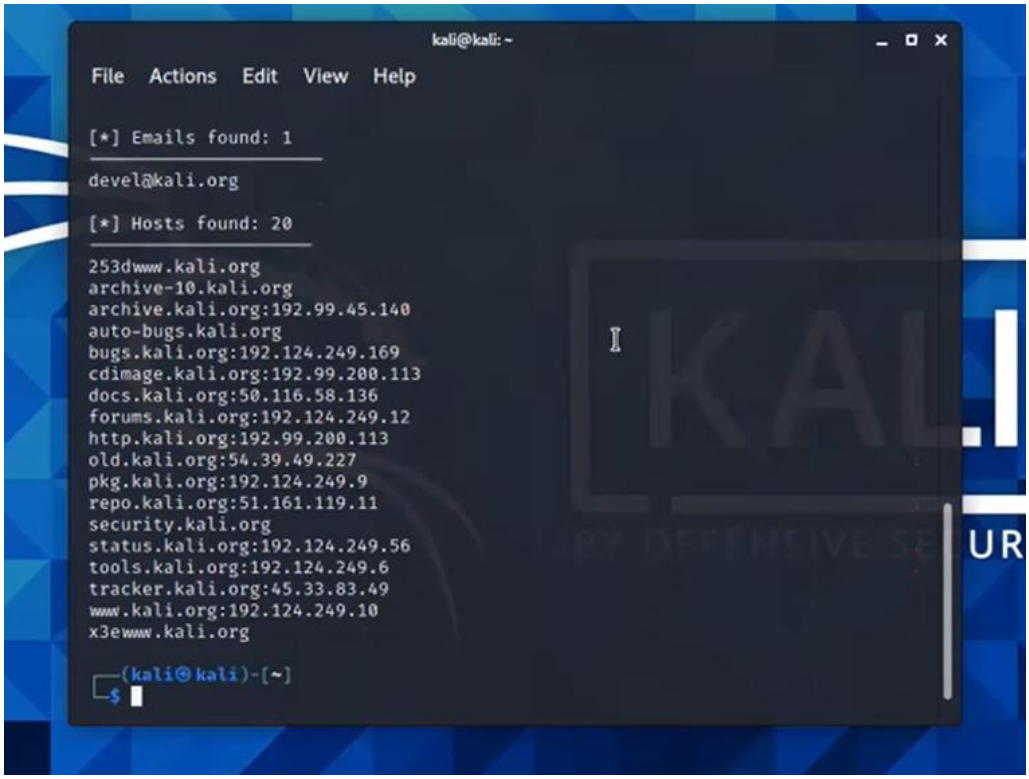
Lastly, the necessary modules are entered in order to get the desired results needed. First enter the command “modules load [module name]” and then enter “run” to complete the process.



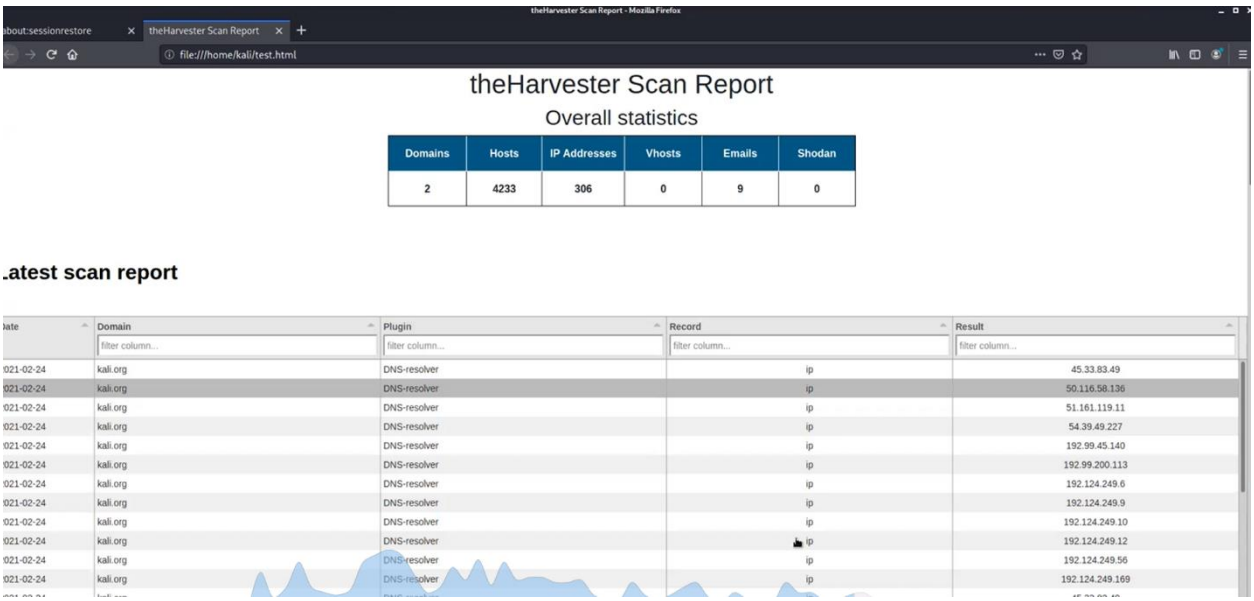
The Harvester

This tool collects information regarding emails, subdomains, hosts, open ports and more through various public sources such as search engines and PGP key servers. To search email id using a search engine “theharvester -d gojo.com -l 200 -b google”

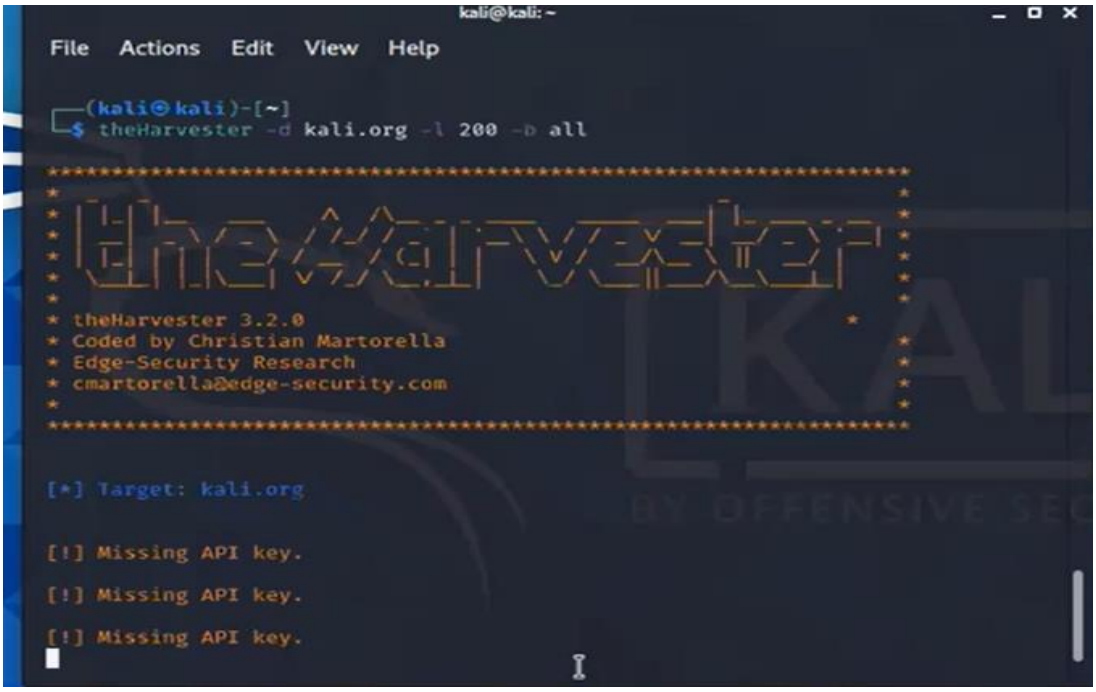


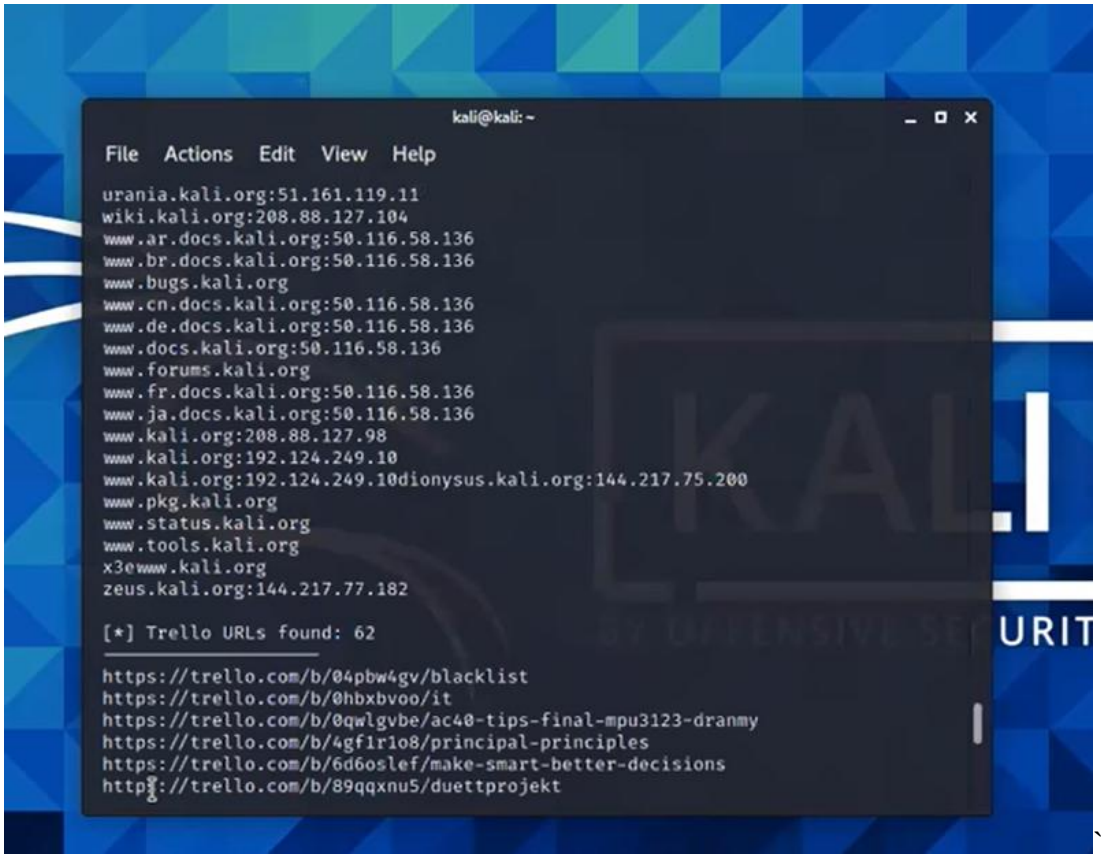


One email was found from the targeted website. Hence, we can use this email for the penetration test that will be conducted in the future. The detail form of the results can be found within the following image.



In order to find components through all search engines “-d goho.com -l 200 -b all” command is used. This command search information from all available search engine and show the result.





Threat Modeling and Vulnerability Identification

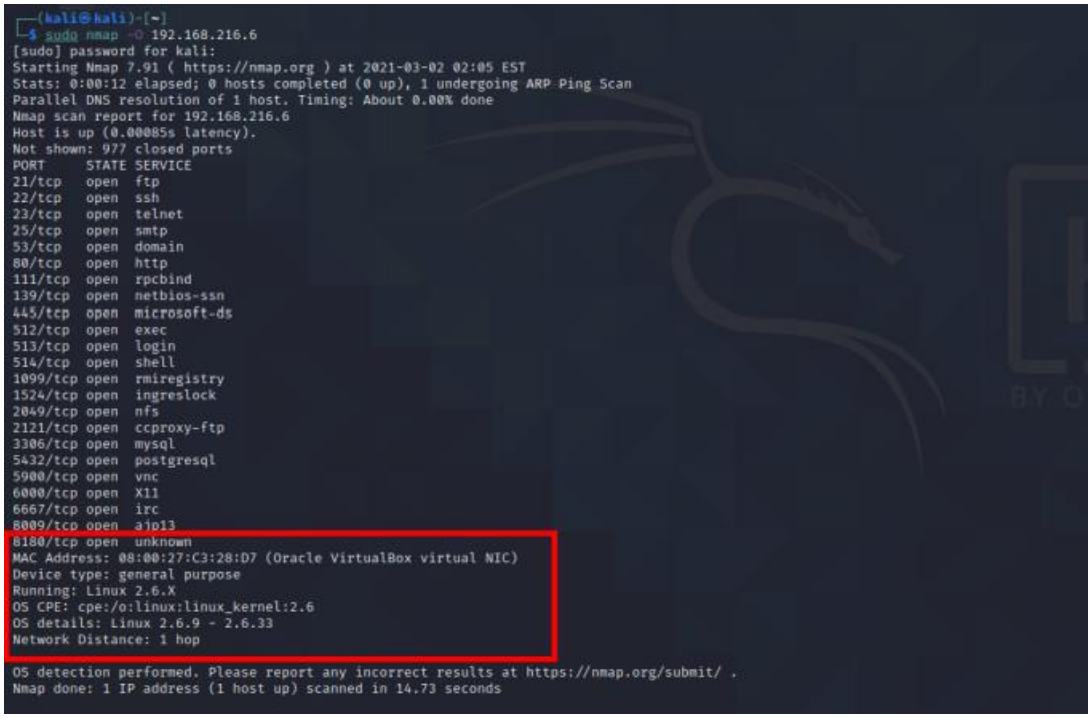
After the information gathering phase has completed, with the gathered information regarding the target, a threat model is created. A threat model contains realistic threats/attacks the clients would face and accordingly vulnerabilities that allows such attacks should be identified.

Vulnerability Identification

Nmaps

Nmaps is an open-source tool use for vulnerability scanning and network discovery. Nmap can be used to identify what devices are running on their systems, discover available host and finding open ports and detecting risks.

- Identifying the version of the operating systems:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.216.6
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 02:05 EST
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.216.6
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C3:28:D7 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.73 seconds
```

- Scanning a specific port:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 192.168.216.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 01:51 EST
Stats: 0:00:07 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.216.6
Host is up (0.0010s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p http 192.168.216.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 01:52 EST
Stats: 0:00:11 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.216.6
Host is up (0.00096s latency).

PORT     STATE  SERVICE
80/tcp   open   http
8008/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
```

- Reaching your target using traceroute:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --traceroute 192.168.216.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 02:13 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.00% done; ETC: 02:13 (0:00:00 remaining)
Nmap scan report for 192.168.216.6
Host is up (0.000085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:C3:28:D7 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1   0.09 ms 192.168.216.6

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds
```

- Find all the details of target:

```
└─$ nmap -A 192.168.216.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-02 02:34 EST
Nmap scan report for 192.168.216.6
Host is up (0.00020s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.216.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-03-02T07:35:03+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
```

Vulnerability analysis

1. Vulnerability: Weak or default passwords

   Severity: High

   Impact: A week or a system default password can be easily guessable using a brute force attack using all possible passwords such as dictionary words, names and pre written password files.

   Mitigation: Enforcing a strong password policy. Do not permit any passwords that falls under the weak category such as dictionary-based passwords, names etc.

2. Vulnerability: Unpatched Windows System.

   CVE Details: CVE-2020-0796, CVE-2019-0708

   Severity: Critical

   Impact: Allow to obtain remote code execution (RCE) on the target system with the highest privileges

   Mitigation: Install security patches and update system regularly.

3. Vulnerability: IPMI v2.0 Password hash disclosure

   CVE Details: CVE-2013-4786

   Severity: High

   Impact: A remote attacker can obtain the password hash information for valid user accounts via HMAC from a RAKP message 2 response from a BCM

   Mitigation: There is no patch for this vulnerability as of yet. The suggested mitigations are:

   - Disabling IPMI over LAN if it is not needed

- Using ACLs or isolated network to limit access to the IPMI management interface
- Using a strong password

4. Vulnerability: SMB 1.0 Protocol

Severity: High

Impact: SMBv1 is insecure therefore the system is prone to multiple vulnerabilities such as:

- Remote code execution (RCE)
- Denial of Service
- Man in the middle

Mitigation: It is strongly advice that SMBv1 should be disable on all windows systems (client and server)

5. Vulnerability: SNMP Agent Default Community Name (public)

CVE Details: CVE-1999-0517

Severity: Medium

Impact: An attacker can use this information to gain more knowledge regarding the remote host or to change the configuration of the remote system if the default community allow such modification

Mitigation: Disable SNMP service in the remote host if it does not get used, filter incoming UDP packets going to the ports, change the default community string.

Conclusion

Overall, the target system was well designed and had many security implements to protect itself from cyber-attacks. However, during the penetration testing, several medium to critical risk vulnerabilities were found. As a result, the target is vulnerable towards a few common cyber-attacks that could be seen at present such as Denial of Service attack.

Since the target is in a high valued and a very competitive market, it would in best interest to swiftly implement the recommended security practices recognized by the penetration testing

.