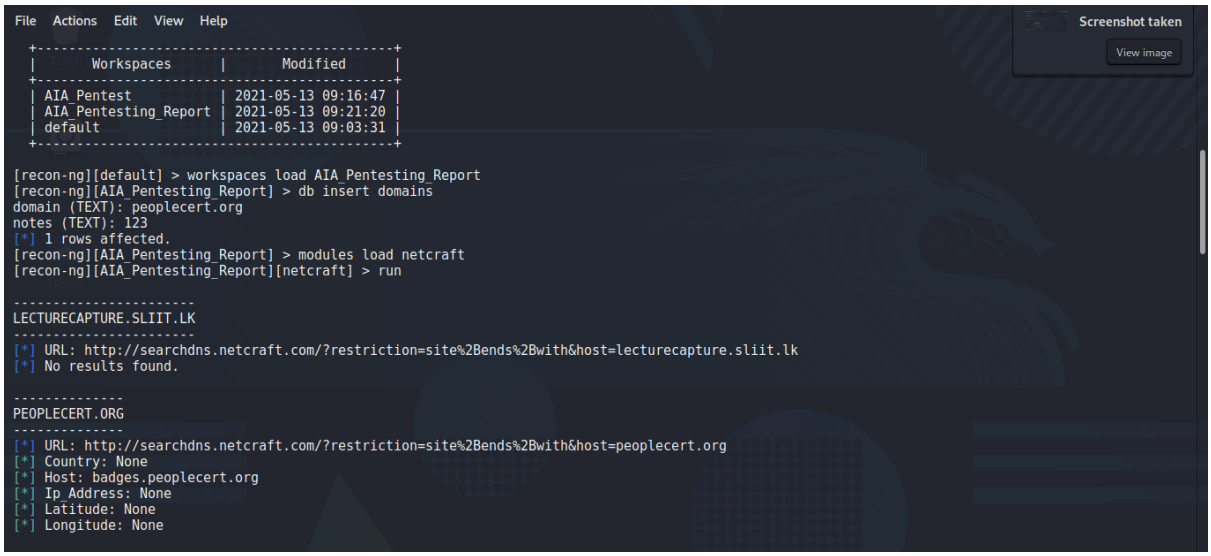

# PENETRATION TEST REPORT

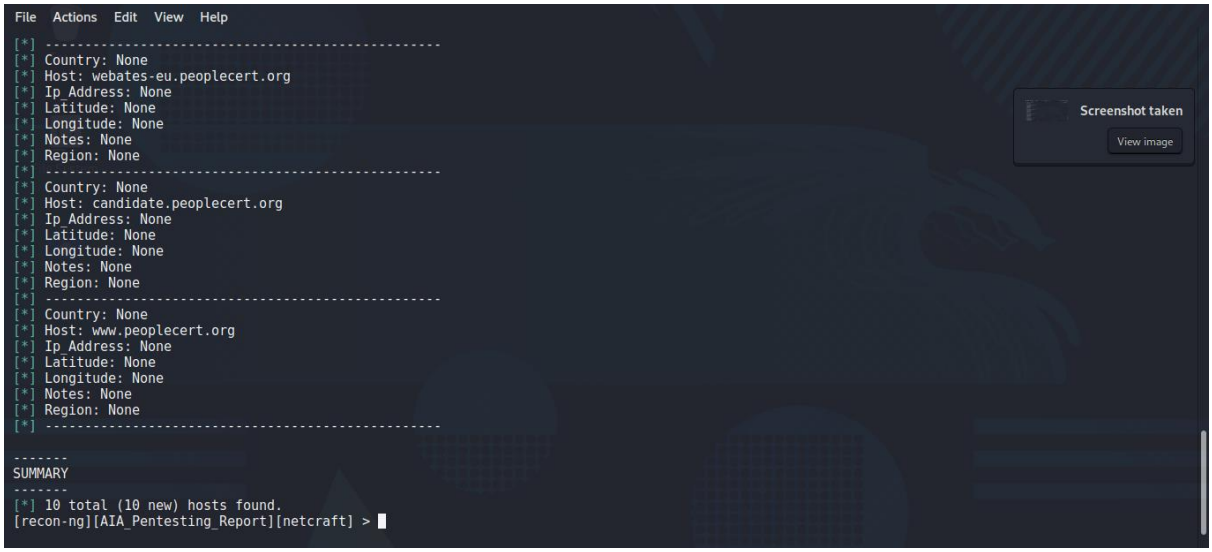
Applied Information Assurance – IE3022

Maleesha Rodrigo IT19001180

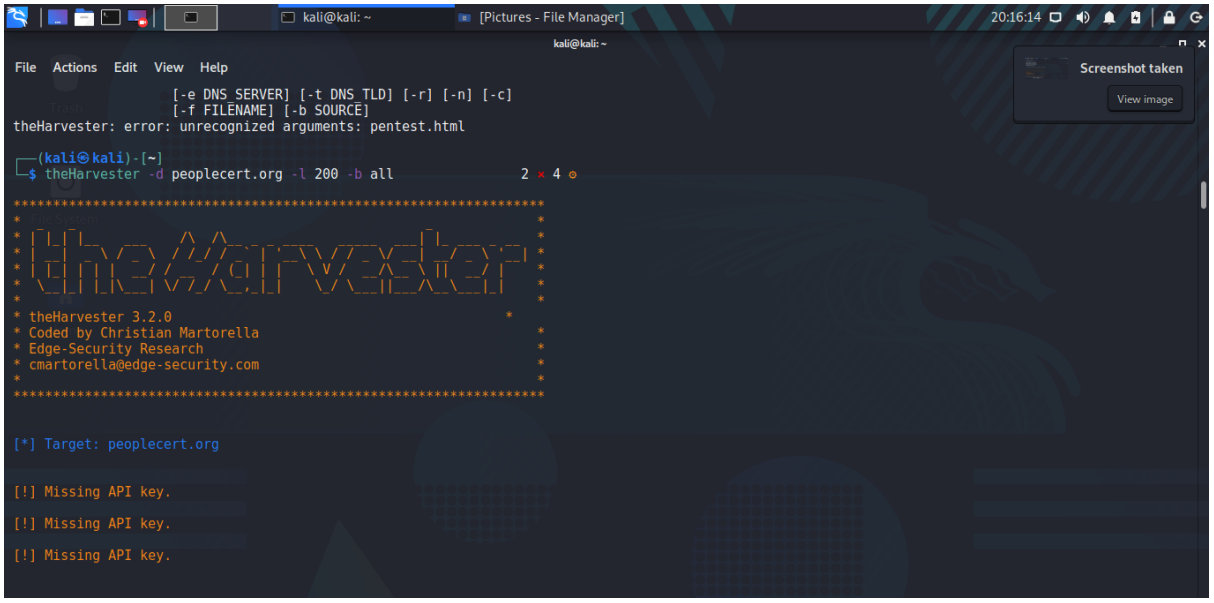
## *Reconnaissance scan on the domain - peoplecert.org*

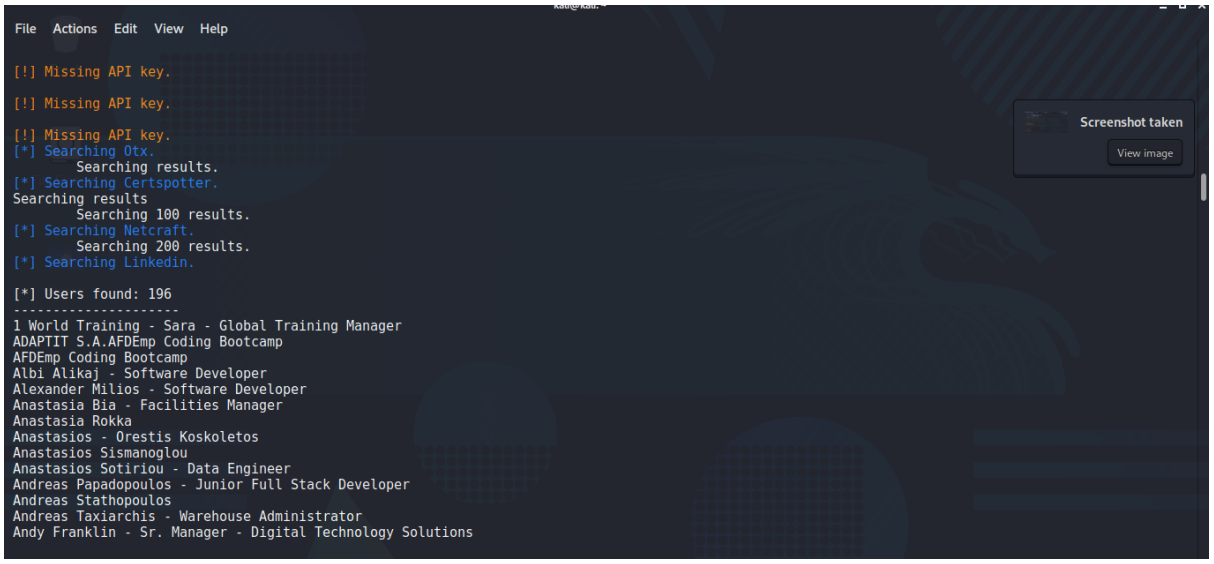
### Using recon -ng

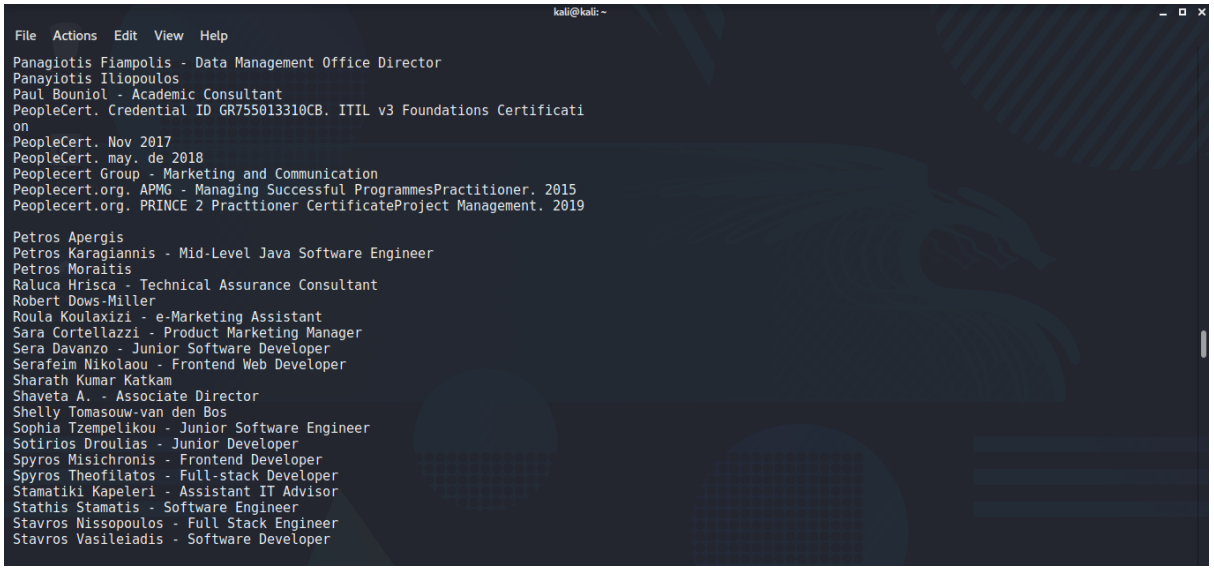






## Using harvest


kali@kali: ~
[Pictures - File Manager]
20:16:14
kali@kali: ~
File Actions Edit View Help
[-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c]
[-f FILENAME] [-b SOURCE]
theHarvester: error: unrecognized arguments: pentest.html
┌──(kali㉿kali)-[~]
└─$ theHarvester -d peoplecert.org -l 200 -b all 2 ✖ 4
* theHarvester 3.2.0 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
[*] Target: peoplecert.org
[!] Missing API key.
[!] Missing API key.
[!] Missing API key.
Screenshot taken
View image


File Actions Edit View Help
[!] Missing API key.
[!] Missing API key.
[!] Missing API key.
[*] Searching Otx.
Searching results.
[*] Searching Certspotter.
Searching results
Searching 100 results.
[*] Searching Netcraft.
Searching 200 results.
[*] Searching Linkedin.
[*] Users found: 196
1 World Training - Sara - Global Training Manager
ADAPTIT S.A.AFDEmp Coding Bootcamp
AFDEmp Coding Bootcamp
Albi Alikaj - Software Developer
Alexander Milios - Software Developer
Anastasia Bia - Facilities Manager
Anastasia Rokka
Anastasios - Orestis Koskoletos
Anastasios Sismanoglou
Anastasios Sotiriou - Data Engineer
Andreas Papadopoulos - Junior Full Stack Developer
Andreas Stathopoulos
Andreas Taxiarchis - Warehouse Administrator
Andy Franklin - Sr. Manager - Digital Technology Solutions
Screenshot taken
View image


kali@kali: ~
File Actions Edit View Help
Panagiotis Fiampolis - Data Management Office Director
Panayiotis Iliopoulos
Paul Bouniol - Academic Consultant
PeopleCert. Credential ID GR755013310CB. ITIL v3 Foundations Certificati
on
PeopleCert. Nov 2017
PeopleCert. may. de 2018
Peoplecert Group - Marketing and Communication
Peoplecert.org. APMG - Managing Successful ProgrammesPractitioner. 2015
Peoplecert.org. PRINCE 2 Practtioner CertificateProject Management. 2019
Petros Apergis
Petros Karagiannis - Mid-Level Java Software Engineer
Petros Moraitis
Raluca Hrisca - Technical Assurance Consultant
Robert Dows-Miller
Roula Koulaxizi - e-Marketing Assistant
Sara Cortellazzi - Product Marketing Manager
Sera Davanzo - Junior Software Developer
Serafeim Nikolaou - Frontend Web Developer
Sharath Kumar Katkam
Shaveta A. - Associate Director
Shelly Tomasouw-van den Bos
Sophia Tzempelikou - Junior Software Engineer
Sotirios Droulias - Junior Developer
Spyros Misichronis - Frontend Developer
Spyros Theofilatos - Full-stack Developer
Stamatiki Kapeleri - Assistant IT Advisor
Stathis Stamatis - Software Engineer
Stavros Nissopoulos - Full Stack Engineer
Stavros Vasileiadis - Software Developer

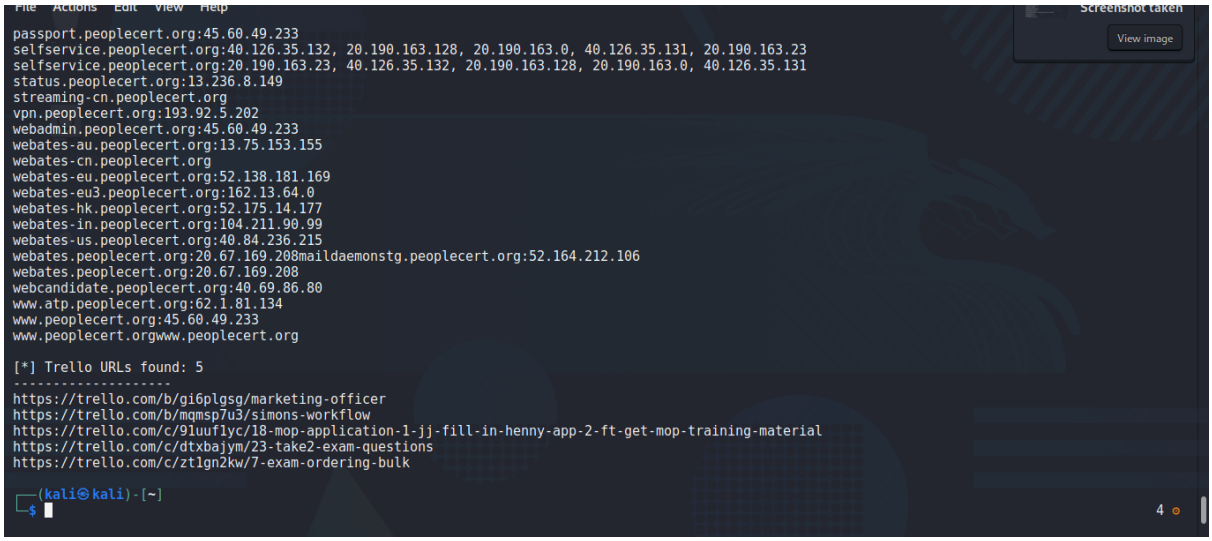
```
File  Actions  Edit  View  Help
[*] Searching Dnsdumpster.
[*] Searching Rapiddns.
        Searching 200 results.
[*] Searching Linkedin.

[*] Links found: 13
--------------------
https://www.linkedin.com/in/aespinal
https://www.linkedin.com/in/andreasstathop
https://www.linkedin.com/in/andy-franklin-39196b4
https://www.linkedin.com/in/bill-martindill-ph-d-5806482b
https://www.linkedin.com/in/byronnicolaides/
https://www.linkedin.com/in/charlottebeck
https://www.linkedin.com/in/clay-clark
https://www.linkedin.com/in/debbie-ann-facey-mba-pmp-csm-itil-9328a1a
https://www.linkedin.com/in/ilias-papargiris-165616173
https://www.linkedin.com/in/jerry-koyne-a07ab913
https://www.linkedin.com/in/mixalis-gikas
https://www.linkedin.com/in/okurtulus
https://www.linkedin.com/in/servicedeskacademy
[*] Searching Bufferoverun.
[*] Searching Baidu.
substring not found
substring not found
        Searching 0 results.
[*] Searching Trello.

[*] IPs found: 40
-------------------
13.74.62.224
13.74.248.121
```

```
File  Actions  Edit  View  Help
Yiouli Iglezou - Global Sales Manager
Youssef Lamnouar - Business Development Associate
nikos thomos
peoplecert.org. Issued Dec 2018. Credential ID 9980019894845441. See cre
dential External link. Z0-932
pratik kumbhare - Remedy Consultant
        Searching results.
[*] Searching Exalead.
[*] Searching Qwant.
[*] Searching Urlscan.
[*] Searching Virustotal.
[*] Searching CRTsh.
        Searching 0 results.
[*] Searching Sublist3r.
[*] Searching Threatcrowd.
An exception has occurred: 0, message='Attempt to decode JSON with unexp
ected mimetype: ', url=URL('https://public.intelx.io/phonebook/search')
An exception has occurred: string indices must be integers
[*] Searching Intelx.
[*] Searching Hackertarget.
        Searching 100 results.
[*] Searching Duckduckgo.
[*] Searching Threatminer.
        Searching 200 results.
[*] Searching Google.
        Searching 100 results.
        Searching 0 results.
[*] Searching Bing.
[*] Searching Dnsdumpster.
[*] Searching Rapiddns.
        Searching 200 results.
```

```
File  Actions  Edit  View  Help
Andy Franklin - Sr. Manager - Digital Technology Solutions
Andy Harrison
Anna-Maria Lyri
Antonios Thanasis - Junior Full Stack Web Developer
Apostolos Skoteiniotis - Associate Software Engineer
Arnaldo Espinal - IT Manager
Atefeh Razavi
Athanasios Katsiaounis
Athanasios Nektarios Tsianis - Associate Solution Engineer
Babis Markos
Bill Douros
Byron Nicolaides
Charalampos Kourkoulis - Software Engineer
Charalampos Papakonstantinou - Software Developer
Charlotte Beck - Assistant Vice President
Chris Mageirias - Developer
Christina Belitsou - Java Developer
Christopher Avgerinos - Senior Software Engineer
Christopher Kampourelis - Hellenic Open University
Christos Karanikos - Business Development Manager
Christos Katsoulas
Christos Markoulis - Software Engineer
Clay Clark - Business Support Manager
Constantinos Dafalias
Damien Byrne
Danai Bafa - Learning and Development Associate
Dimitra Kyriakopoulou - Talent Acquisition Associate
Dimitris Aggelopoulos
Dimitris Nicolaides
Dimitris Spiliotopoulos - Supervisor
Dimitris Thanos - Electronic Engineer
```


## Vulnerabilities/ findings

Information has been disclosed

## Risk level

*High*

## Business impact

3rd parties can use these information since user details are disclosed

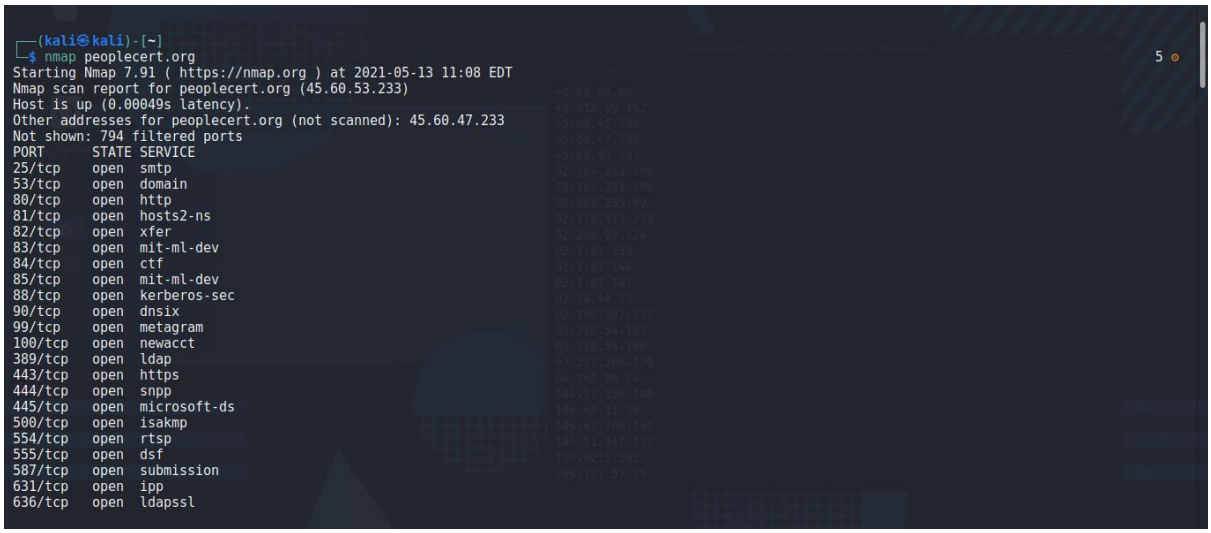
Users' confidentiality is in danger

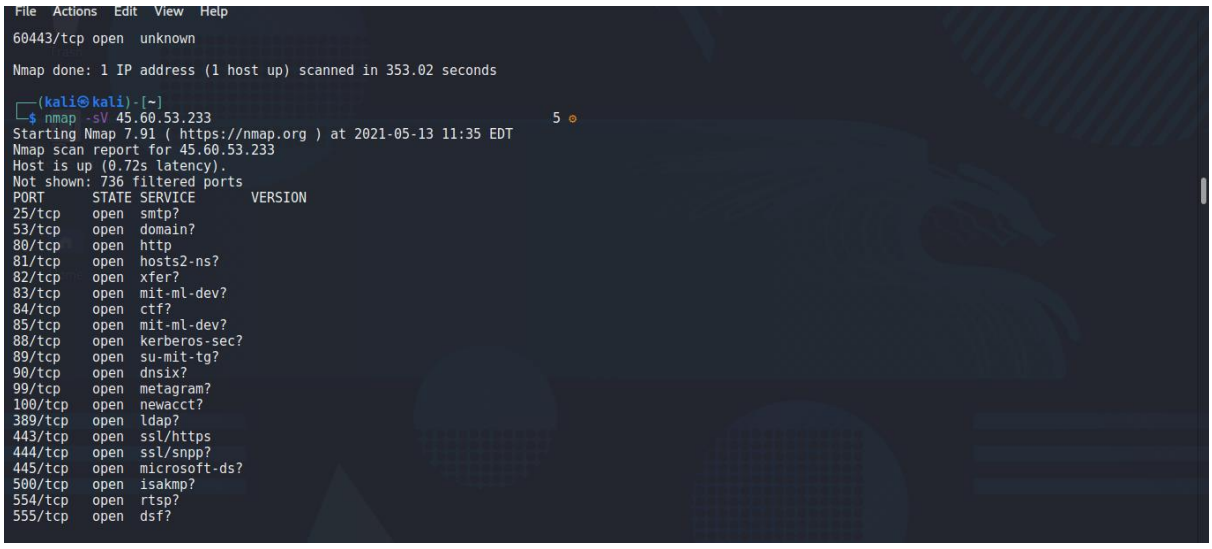
**Recommendations for mitigation**

Encrypt the user details

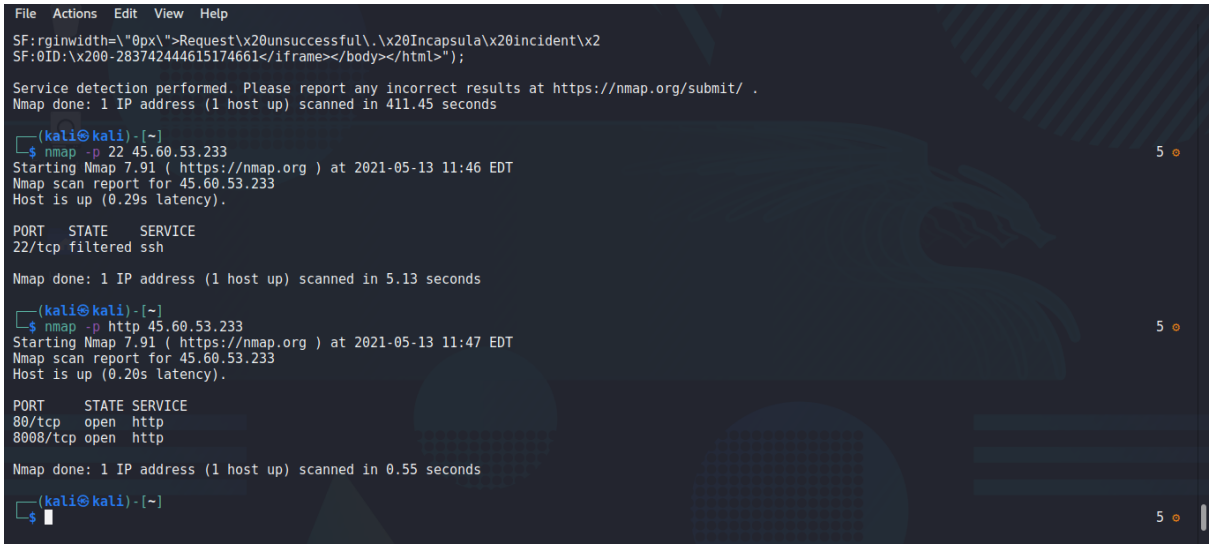
# Scanning the network

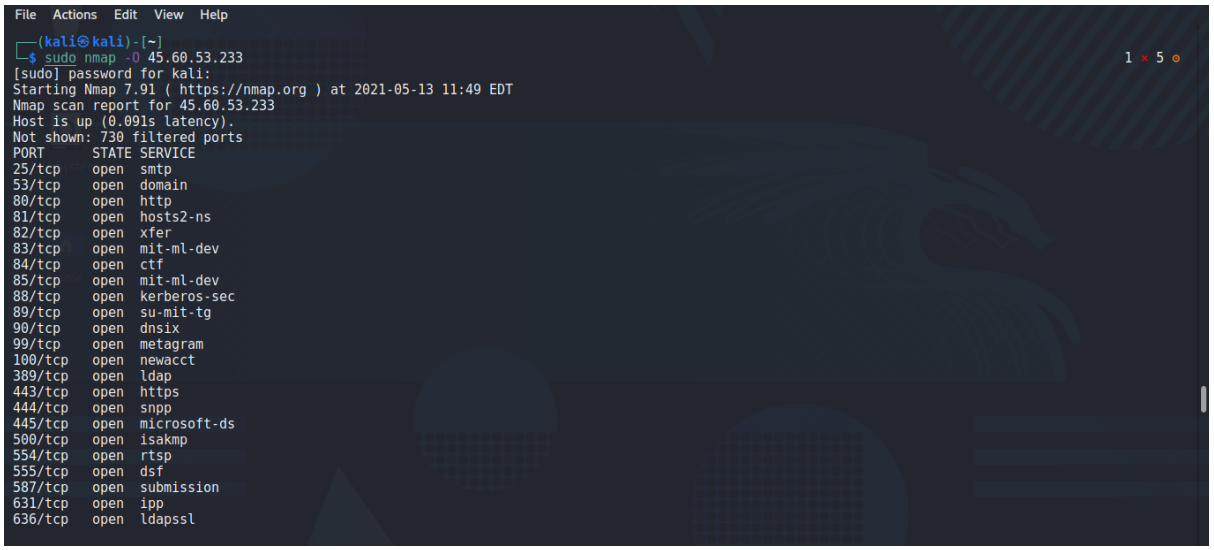
## Using nmap

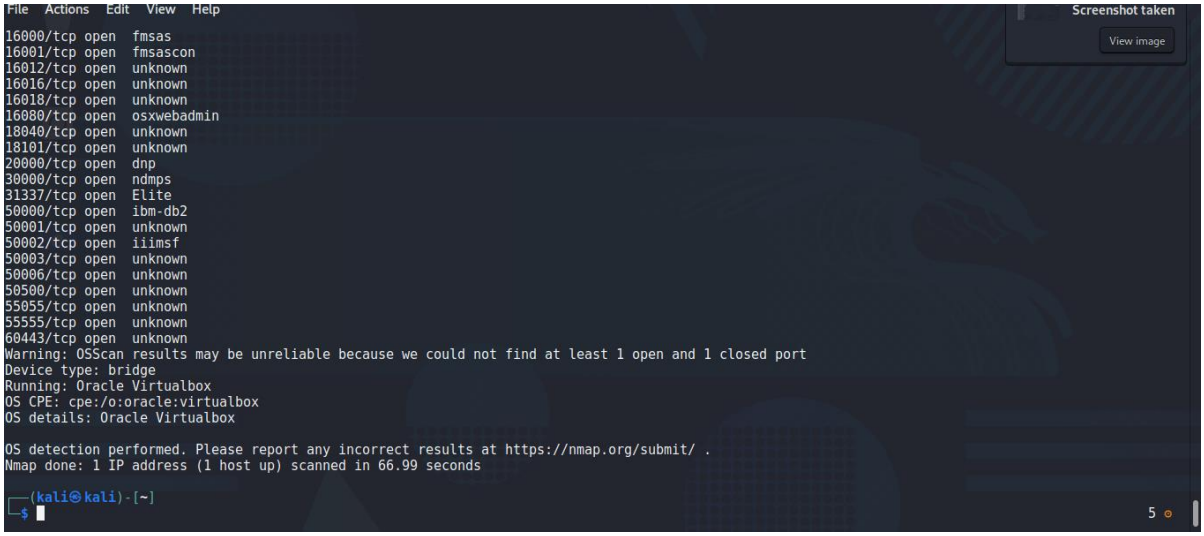


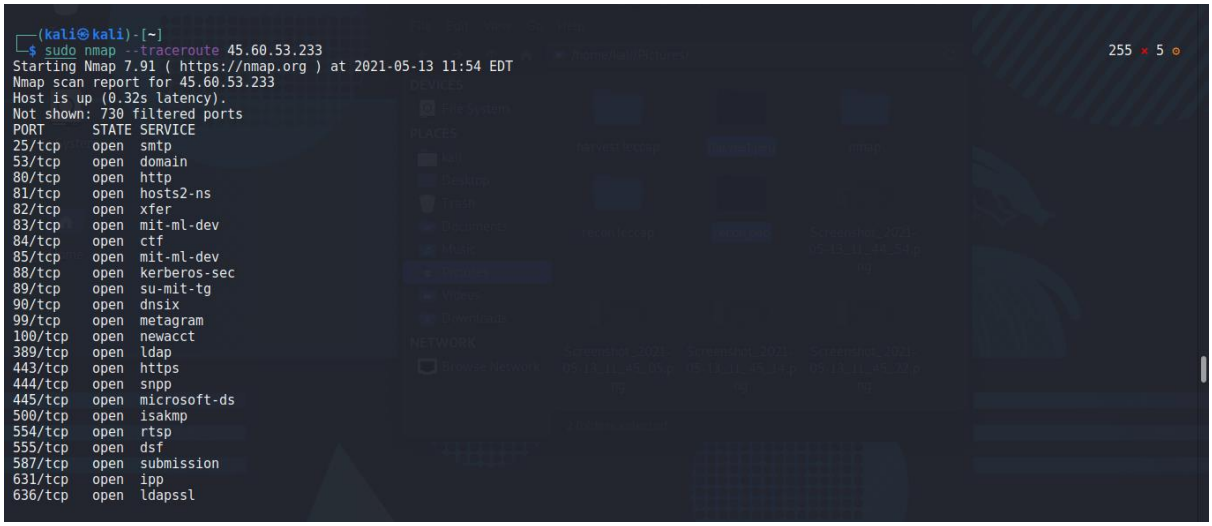



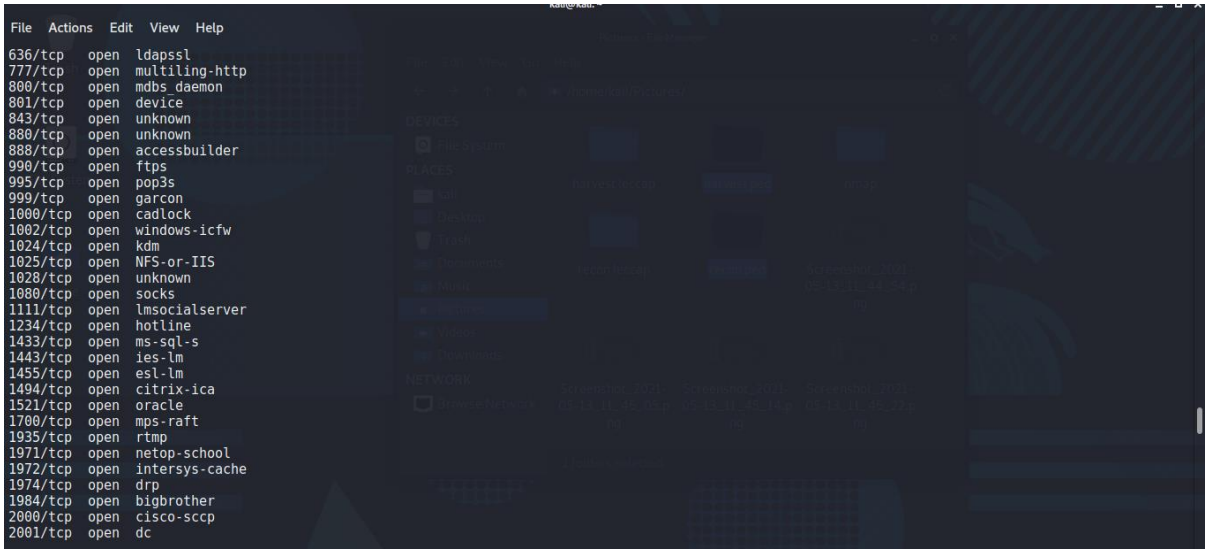

File Actions Edit View Help
3389/tcp open tcpwrapped
3404/tcp open tcpwrapped
3551/tcp open tcpwrapped
3580/tcp open tcpwrapped
4000/tcp open tcpwrapped
4001/tcp open tcpwrapped
4002/tcp open tcpwrapped
4343/tcp open tcpwrapped
4443/tcp open tcpwrapped
4444/tcp open tcpwrapped
4445/tcp open tcpwrapped
4449/tcp open tcpwrapped
4848/tcp open tcpwrapped
5000/tcp open tcpwrapped
5001/tcp open tcpwrapped
5002/tcp open tcpwrapped
5003/tcp open tcpwrapped
5004/tcp open tcpwrapped
5009/tcp open tcpwrapped
5050/tcp open tcpwrapped
5051/tcp open tcpwrapped
5060/tcp open tcpwrapped
5061/tcp open tcpwrapped
5080/tcp open tcpwrapped
5100/tcp open tcpwrapped
5120/tcp open tcpwrapped
5222/tcp open tcpwrapped
5225/tcp open tcpwrapped
5226/tcp open tcpwrapped
5269/tcp open tcpwrapped
5280/tcp open tcpwrapped
Screenshot taken
View image

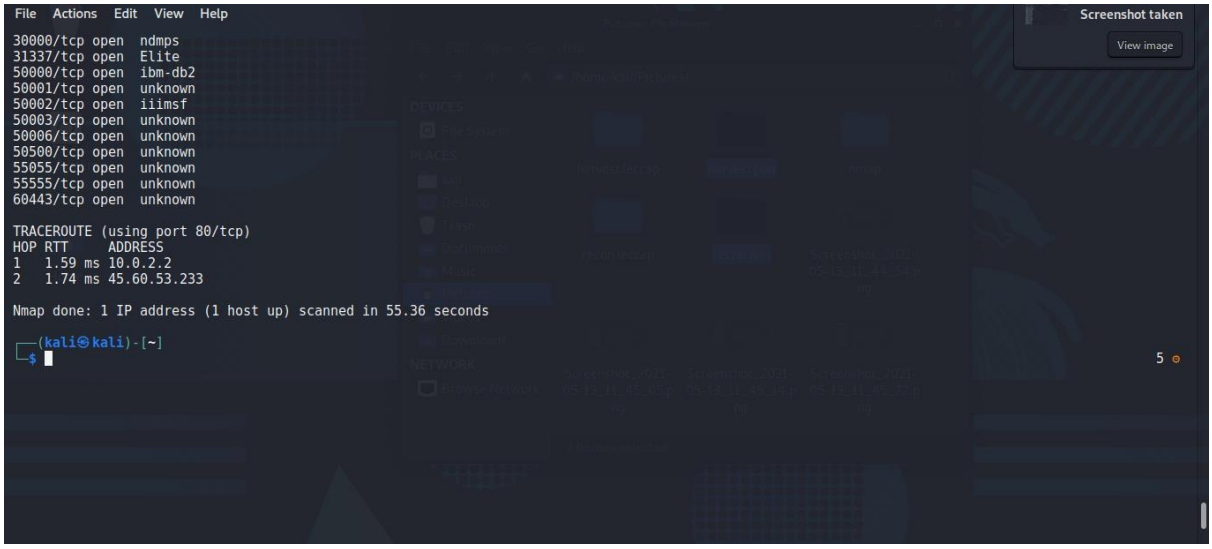

File Actions Edit View Help
SF:rginwidth=\"0px\">Request\x20unsuccessful\.\x20Incapsula\x20incident\x2
SF:0ID:\x200-283742444615174661</iframe></body></html>");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 411.45 seconds
(kali㉿kali)-[~]
$ nmap -p 22 45.60.53.233
5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:46 EDT
Nmap scan report for 45.60.53.233
Host is up (0.29s latency).
PORT STATE SERVICE
22/tcp filtered ssh
Nmap done: 1 IP address (1 host up) scanned in 5.13 seconds
(kali㉿kali)-[~]
$ nmap -p http 45.60.53.233
5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:47 EDT
Nmap scan report for 45.60.53.233
Host is up (0.20s latency).
PORT STATE SERVICE
80/tcp open http
8008/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
(kali㉿kali)-[~]
$
5


File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo nmap -O 45.60.53.233
1 × 5
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:49 EDT
Nmap scan report for 45.60.53.233
Host is up (0.091s latency).
Not shown: 730 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev
84/tcp open ctf
85/tcp open mit-ml-dev
88/tcp open kerberos-sec
89/tcp open su-mit-tg
90/tcp open dnsix
99/tcp open metagram
100/tcp open newacct
389/tcp open ldap
443/tcp open https
444/tcp open snpp
445/tcp open microsoft-ds
500/tcp open isakmp
554/tcp open rtsp
555/tcp open dsf
587/tcp open submission
631/tcp open ipp
636/tcp open ldapssl


File Actions Edit View Help
16000/tcp open fmsas
16001/tcp open fmsascon
16012/tcp open unknown
16016/tcp open unknown
16018/tcp open unknown
16080/tcp open osxwebadmin
18040/tcp open unknown
18101/tcp open unknown
20000/tcp open dnp
30000/tcp open ndmps
31337/tcp open Elite
50000/tcp open ibm-db2
50001/tcp open unknown
50002/tcp open iiimsf
50003/tcp open unknown
50006/tcp open unknown
50500/tcp open unknown
55055/tcp open unknown
55555/tcp open unknown
60443/tcp open unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.99 seconds
(kali㉿kali)-[~]
$
Screenshot taken
View image
5


(kali㉿kali)-[~]
$ sudo nmap --traceroute 45.60.53.233
255 × 5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:54 EDT
Nmap scan report for 45.60.53.233
Host is up (0.32s latency).
Not shown: 730 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp open domain
80/tcp open http
81/tcp open hosts2-ns
82/tcp open xfer
83/tcp open mit-ml-dev
84/tcp open ctf
85/tcp open mit-ml-dev
88/tcp open kerberos-sec
89/tcp open su-mit-tg
90/tcp open dnsix
99/tcp open metagram
100/tcp open newacct
389/tcp open ldap
443/tcp open https
444/tcp open snpp
445/tcp open microsoft-ds
500/tcp open isakmp
554/tcp open rtsp
555/tcp open dsf
587/tcp open submission
631/tcp open ipp
636/tcp open ldapssl


File Actions Edit View Help
636/tcp open ldapssl
777/tcp open multiling-http
800/tcp open mdbs_daemon
801/tcp open device
843/tcp open unknown
880/tcp open unknown
888/tcp open accessbuilder
990/tcp open ftps
995/tcp open pop3s
999/tcp open garcon
1000/tcp open cadlock
1002/tcp open windows-icfw
1024/tcp open kdm
1025/tcp open NFS-or-IIS
1028/tcp open unknown
1080/tcp open socks
1111/tcp open lmsocialserver
1234/tcp open hotline
1433/tcp open ms-sql-s
1443/tcp open ies-lm
1455/tcp open esl-lm
1494/tcp open citrix-ica
1521/tcp open oracle
1700/tcp open mps-raft
1935/tcp open rtmp
1971/tcp open netop-school
1972/tcp open intersys-cache
1974/tcp open drp
1984/tcp open bigbrother
2000/tcp open cisco-sccp
2001/tcp open dc




## Vulnerabilities/ findings

Information has been disclosed

Open ports

SSH

Operating system information

## Risk level

*High*

## Business impact

3rd parties can use these information since technical details are disclosed and they can implement attacks and gain the access to the system

Reputation of the company is in danger

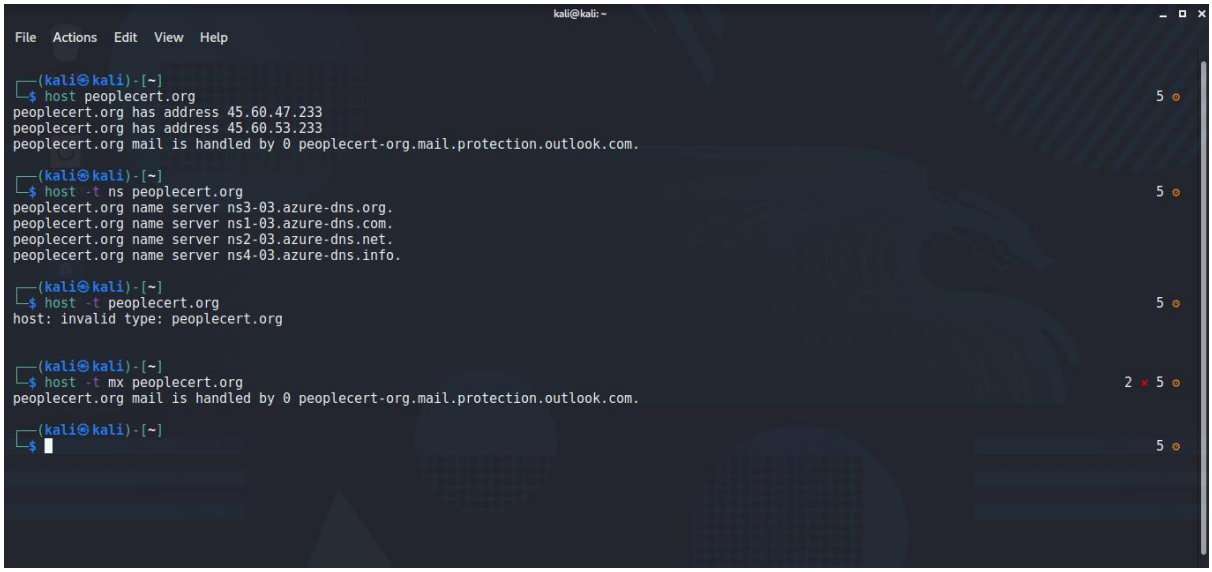
## Recommendations for mitigation

Update the software

Block ICMP ping requests

# Enumeration scan

## Using host



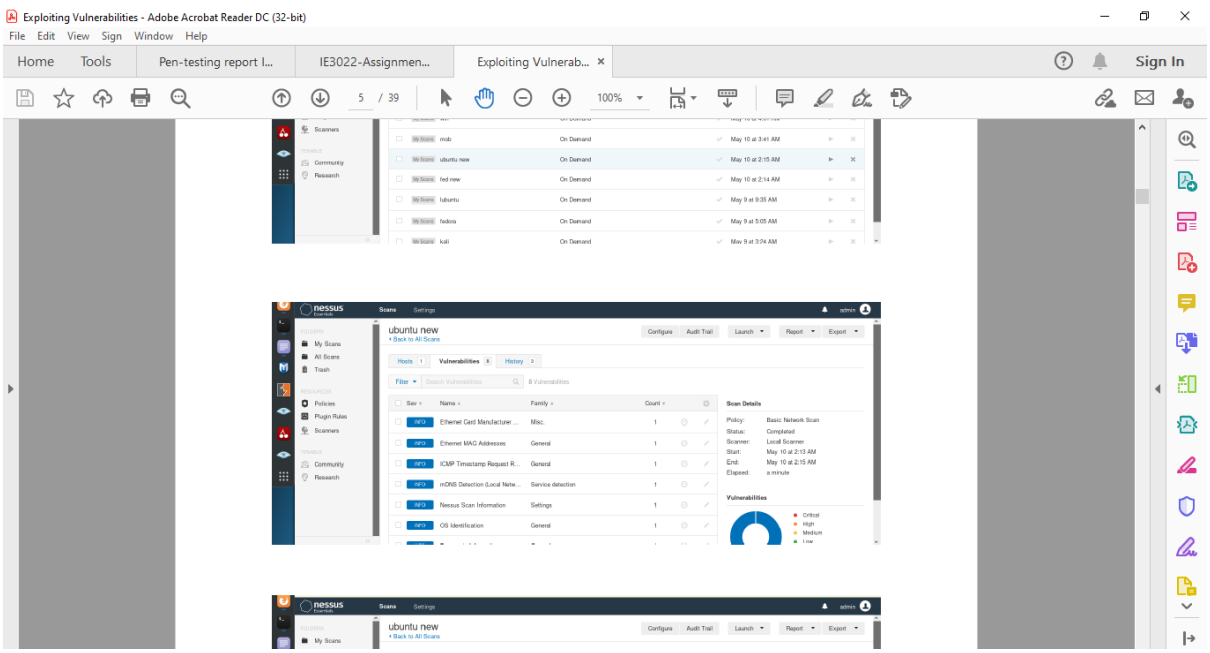

Using “host” public IP and mail server of peoplecert.org has been identified

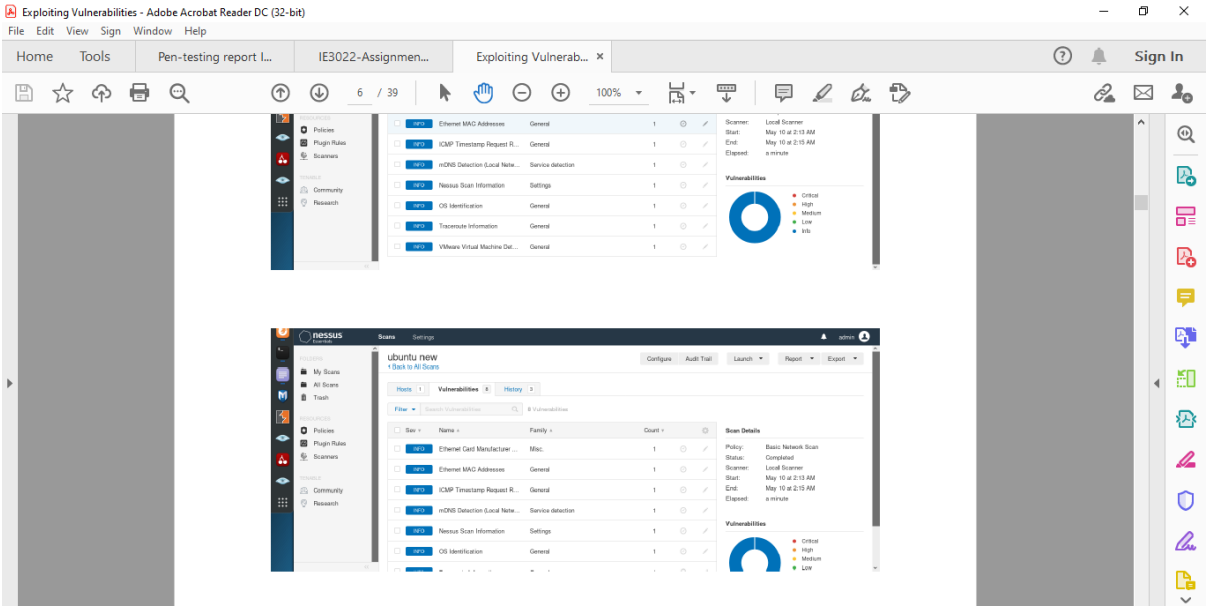
Using “host -t ns” name servers of peoplecert.org has been identified

Using “host -t mx” mail servers of peoplecert.org has been identified

# Nessus scan on the target

Due to the change of the Nessus version, I wasn’t able to launch the software. But for the reference I drop a screen shot of one of my assignments when I was in 2nd year 1st semester.






## *Exploit the target using Metasploit framework*

Due to the change of the Nessus version, I wasn't able to launch the software. But for the reference I drop a screen shot of one of my assignments when I was in 2nd year 1st semester.