



PENETRATION TEST REPORT

Applied Information Assurance – IE3022

Reconnaissance scan on the domain - peoplecert.org

Using recon-ng

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali] (~)  
$ recon-ng  
[*] Version check disabled.  
  
Sponsored by...  
BLACK HILLS  
www.blackhillsinfosec.com  
  
PRACTISEC  
www.practisec.com  
[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]  
[2] Recon modules  
[recon-ng][default] > workspaces list  
+-----+  
| Workspace | Modified |  
+-----+  
| AIA Pentest | 2021-05-13 09:16:47 |  
| AIA Pentesting_Report | 2021-05-13 09:21:20 |  
| default | 2021-05-13 09:03:31 |  
+-----+
```

```
File Actions Edit View Help  
+-----+  
| Workspace | Modified |  
+-----+  
| AIA Pentest | 2021-05-13 09:16:47 |  
| AIA Pentesting_Report | 2021-05-13 09:21:20 |  
| default | 2021-05-13 09:03:31 |  
+-----+  
[recon-ng][default] > workspaces load AIA Pentesting_Report  
[recon-ng][AIA Pentesting_Report] > db insert domains  
domain (TEXT): peoplecert.org  
notes (TEXT): 123  
[*] 1 rows affected.  
[recon-ng][AIA Pentesting_Report] > modules load netcraft  
[recon-ng][AIA_Pentesting_Report][netcraft] > run  
  
LECTURECAPTURE.SLIIT.LK  
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=lecturecapture.sliit.lk  
[*] No results found.  
  
PEOPLECERT.ORG  
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=peoplecert.org  
[*] Country: None  
[*] Host: badges.peoplecert.org  
[*] Ip Address: None  
[*] Latitude: None  
[*] Longitude: None
```

```
File Actions Edit View Help
[*] -----
[*] Country: None
[*] Host: webates-eu.peoplecert.org
[*] Ip Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: candidate.peoplecert.org
[*] Ip Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www.peoplecert.org
[*] Ip Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
SUMMARY
[*] 10 total (10 new) hosts found.
[recon-ng][AIA_Pentesting_Report][netcraft] > 
```

Using harvest

```
File Actions Edit View Help
(kali@kali) ~
$ theHarvester

*****
* theHarvester 3.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c]
[-f FILENAME] [-b SOURCE]
theHarvester: error: the following arguments are required: -d/--domain

(kali@kali) ~
$ theHarvester -d peoplecert.org -l 200 -b google

*****
* theHarvester 3.2.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

File Actions Edit View Help
[*] Target: peoplecert.org
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
[*] Searching Google.
[*] No IPs found.
[*] Emails found: 7
-----
atcustomerservice@peoplecert.org
communication@peoplecert.org
customerservice@peoplecert.org
dataprotection@peoplecert.org
info@peoplecert.org
last@peoplecert.org
vassiliki.mandilara@peoplecert.org
[*] Hosts found: 8
```

```
kali@kali: ~  
[Pictures - File Manager]  
20:16:14  
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 x 4 o  
  
*****  
* 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.
```

```
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 Metcrafft.  
    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
```

```
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 Practitioner 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-itol-9328a1a
https://www.linkedin.com/in/iliass-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/serviceeskacademy
[*] 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 Lamouar - Business Development Associate
nikos thomos
peoplecert.org. Issued Dec 2018. Credential ID 9980019894845441. See cre
dential External link. 20-932
pratik kumbhare - Remedy Consultant
    Searching results.
[*] Searching Exalead.
[*] Searching Owant.
[*] 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 Kampoureilis - 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
```



```
File Actions Edit View Help
[*] IPs found: 40
-----
13.74.62.224
13.74.248.121
18.246.31.131
18.246.31.132
18.246.31.133
20.67.169.208
23.2.16.9
23.7.245.49
23.63.227.160
23.63.227.210
24.143.193.33
24.143.193.40
40.69.86.80
40.112.69.162
45.60.45.233
45.60.47.233
45.60.53.233
52.164.212.106
52.164.231.186
52.169.255.99
52.178.117.235
52.236.93.124
62.1.81.139
62.1.81.146
62.1.81.147
62.38.48.53
62.169.207.237
63.216.54.153
63.216.54.186
```

```
File Actions Edit View Help
passport.peoplecert.org:45.60.49.233
selfservice.peoplecert.org:40.126.35.132, 20.190.163.128, 20.190.163.0, 40.126.35.131, 20.190.163.23
selfservice.peoplecert.org:20.190.163.23, 40.126.35.132, 20.190.163.128, 20.190.163.0, 40.126.35.131
status.peoplecert.org:13.236.8.149
streaming-cn.peoplecert.org
vpn.peoplecert.org:193.92.5.202
webadmin.peoplecert.org:45.60.49.233
webates-au.peoplecert.org:13.75.153.155
webates-cn.peoplecert.org
webates-eu.peoplecert.org:52.138.181.169
webates-eu3.peoplecert.org:162.13.64.0
webates-hk.peoplecert.org:52.175.14.177
webates-in.peoplecert.org:104.211.90.99
webates-us.peoplecert.org:40.84.236.215
webates.peoplecert.org:20.67.169.208maildaemonstg.peoplecert.org:52.164.212.106
webates.peoplecert.org:20.67.169.208
webcandidate.peoplecert.org:40.69.86.80
www.atp.peoplecert.org:62.1.81.134
www.peoplecert.org:45.60.49.233
www.peoplecert.orgwww.peoplecert.org

[*] Trello URLs found: 5
-----
https://trello.com/b/gi6plgsg/marketing-officer
https://trello.com/b/mqmsp7u3/simons-workflow
https://trello.com/c/9luuflyc/18-mop-application-1-jj-fill-in-henny-app-2-ft-get-mop-training-material
https://trello.com/c/dtxbajym/23-take2-exam-questions
https://trello.com/c/zt1gn2kw/7-exam-ordering-bulk

(kali@kali) - [~]
$
```

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

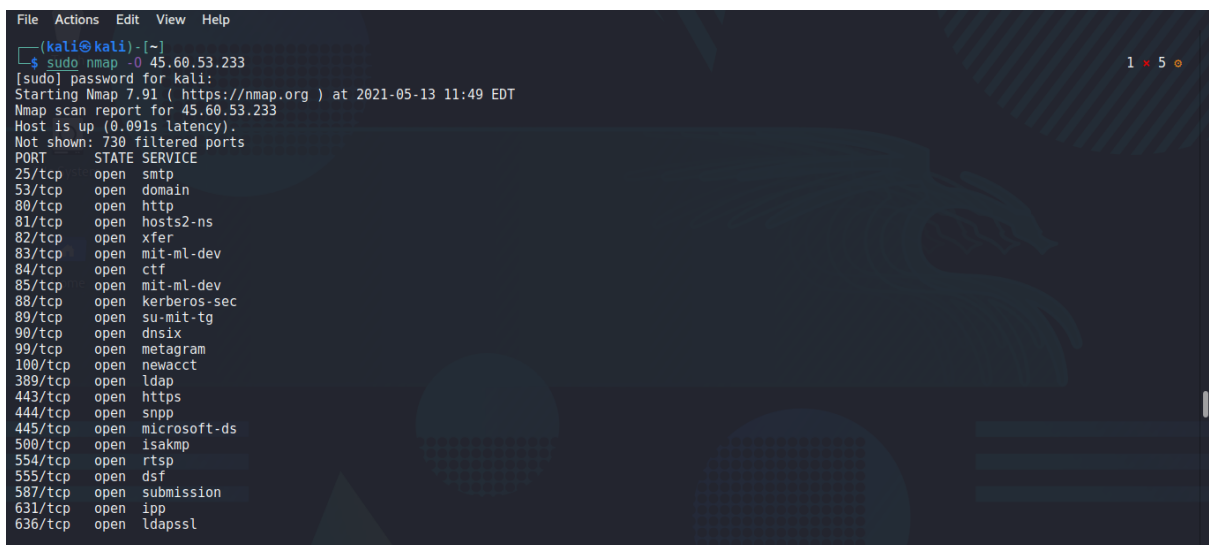
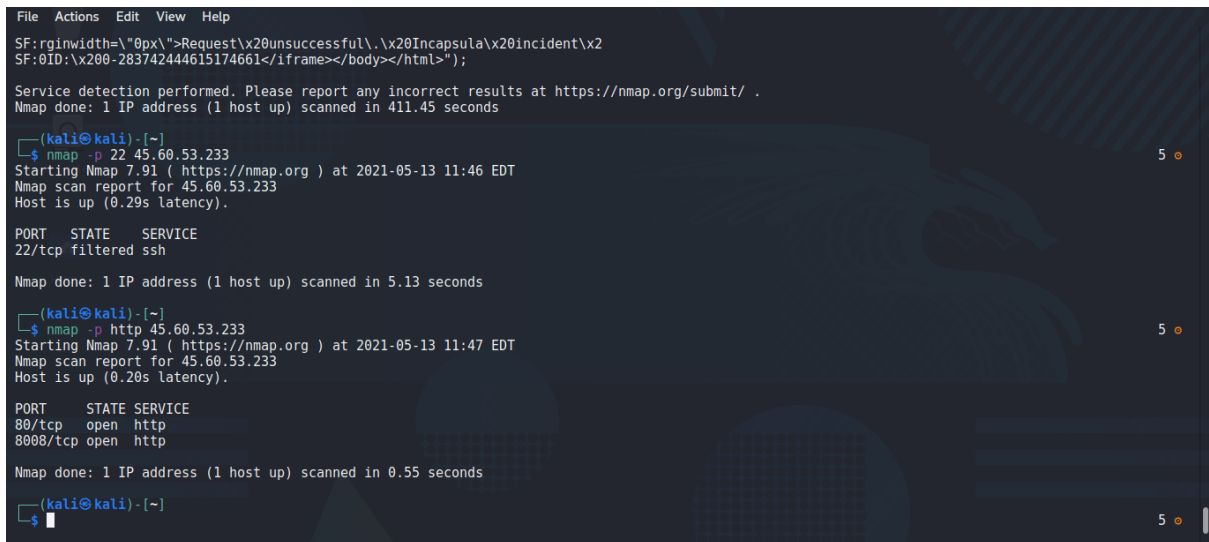
Using nmap

```
(kali㉿kali) [~]
$ nmap peoplecert.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:08 EDT
Nmap scan report for peoplecert.org (45.60.53.233)
Host is up (0.00049s latency).
Other addresses for peoplecert.org (not scanned): 45.60.47.233
Not shown: 794 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
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
60443/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 353.02 seconds

(kali㉿kali) [~]
$ nmap -sV 45.60.53.233
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-13 11:35 EDT
Nmap scan report for 45.60.53.233
Host is up (0.72s latency).
Not shown: 736 filtered ports
PORT      STATE SERVICE      VERSION
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  ssl/https
444/tcp   open  ssl/snpp?
445/tcp   open  microsoft-ds?
500/tcp   open  isakmp?
554/tcp   open  rtsp?
555/tcp   open  dsf?
```



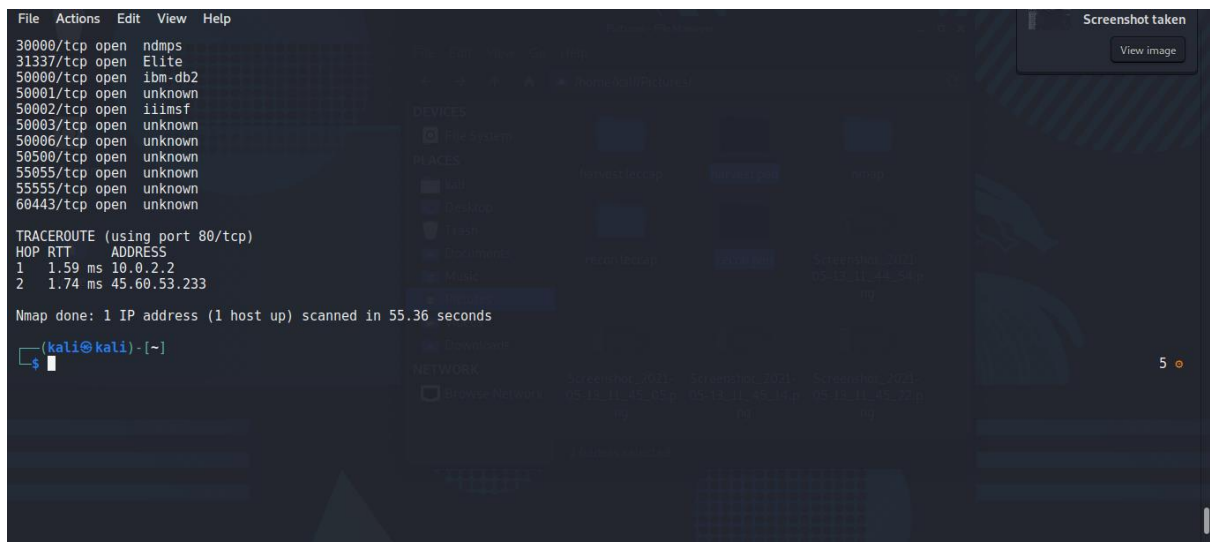

```
File Actions Edit View Help
16000/tcp open fmsas
16001/tcp open fmsascon
16012/tcp open unknown
16016/tcp open unknown
16018/tcp open unknown
16080/tcp open osxwebadmin
18040/tcp open unknown
18191/tcp open unknown
20000/tcp open dnp
30000/tcp open ndmps
31337/tcp open Elite
50000/tcp open ibm-db2
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) - [~]
$
```

```
(kali@kali) - [~]
$ sudo nmap --traceroute 45.60.53.233
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  mdbus-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

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali) ~  
$ host peoplecert.org  
peoplecert.org has address 45.60.47.233  
peoplecert.org has address 45.60.53.233  
peoplecert.org mail is handled by 0 peoplecert.org.mail.protection.outlook.com.  
  
(kali@kali) ~  
$ host -t ns peoplecert.org  
peoplecert.org name server ns3-03.azure-dns.org.  
peoplecert.org name server ns1-03.azure-dns.com.  
peoplecert.org name server ns2-03.azure-dns.net.  
peoplecert.org name server ns4-03.azure-dns.info.  
  
(kali@kali) ~  
$ host -t peoplecert.org  
host: invalid type: peoplecert.org  
  
(kali@kali) ~  
$ host -t mx peoplecert.org  
peoplecert.org mail is handled by 0 peoplecert.org.mail.protection.outlook.com.  
  
(kali@kali) ~  
$
```

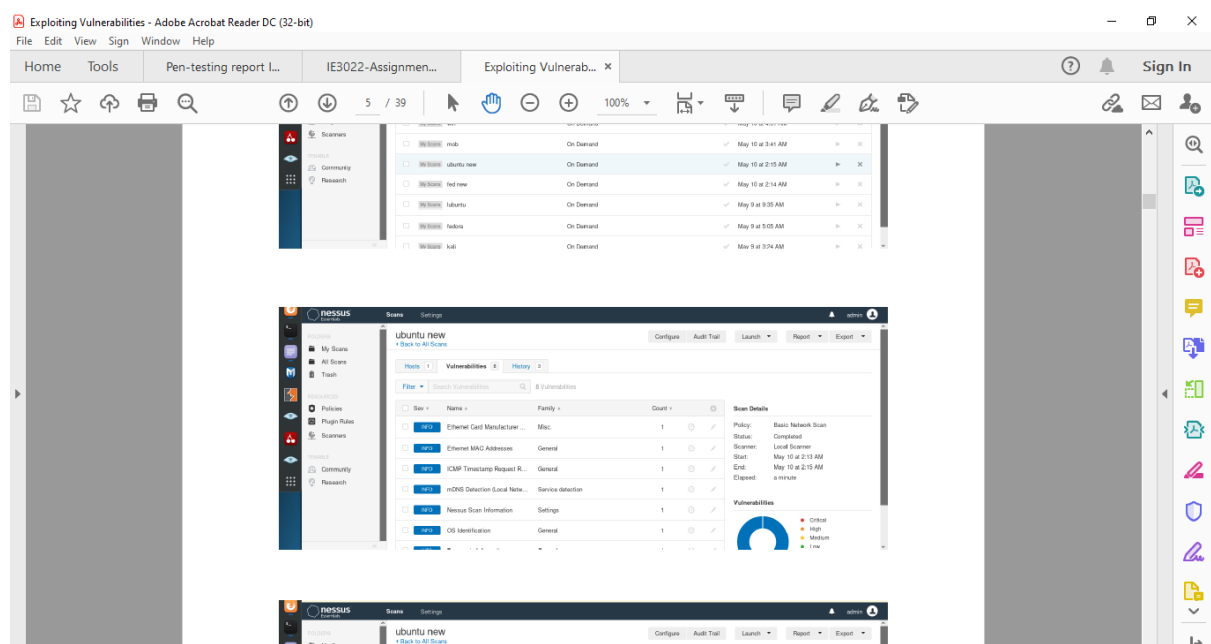
Using “host” public IP and mail server of peoplecert.org has been identified

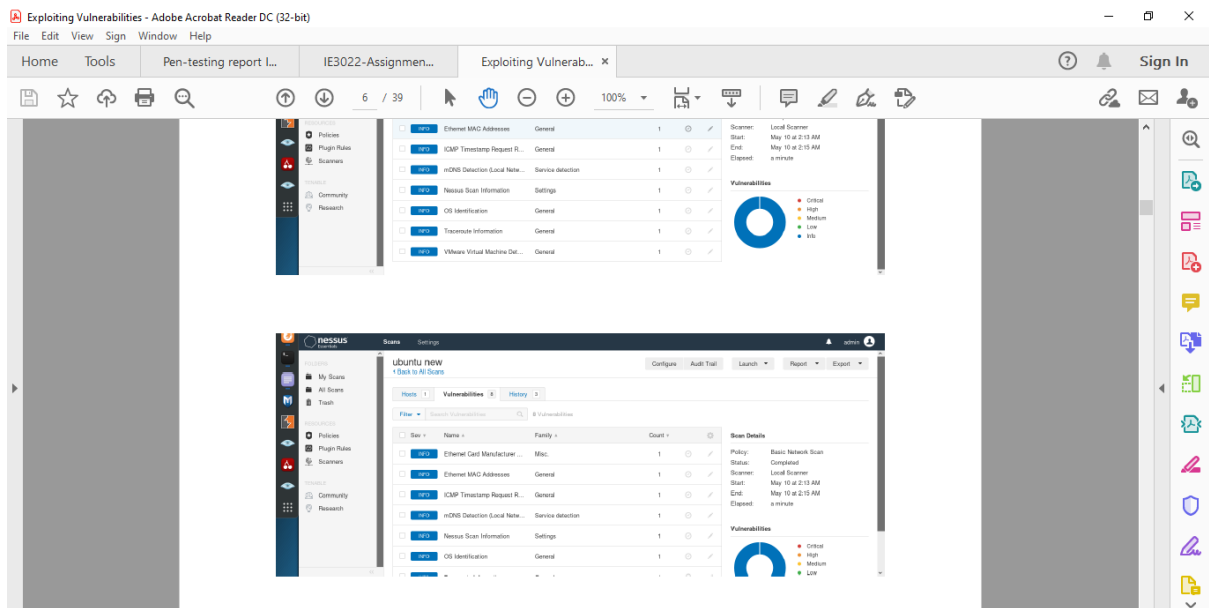
Using “host -t ns” name servers of peoplecert.org has been identified

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.

