DFSC 4338 Cyber Warfare

Assignment 2 (75 points)

Note: Complete assignment by answering all following questions. Submit your completed assignment through Blackboard.

When reliable external sources/works are cited (highly recommended for good grade), you should have both in-text citations and list of references at the end of the document submitted. All citations and references should following standard IEEE format https://pitt.libguides.com/citationhelp/ieee .

1. Reconnaissance Tools (15 points, 5 points each, screenshots expected)

1) **whois**: use whois tool or website to query the information regarding shsu.edu. Paste the result below. Then use whois to query IP address 158.135.1.242 and paste the result.

```
┌──(cyberboss㉿kali)-[~]
└─$ whois shsu.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.
----------------------------------------------------------------------

Domain Name: SHSU.EDU

Registrant:
        Sam Houston State University
        Information Technology
        P.O. Box 2449
        Huntsville, TX 77341-2449
        USA

Administrative Contact:
        Domain Admin
        Sam Houston State University
        Information Technology
        P.O. Box 2449
        Huntsville, TX 77341-2449
        USA
        +1.9362941950
        ucs_mca@shsu.edu

Technical Contact:
        Jurden Bruce
        Sam Houston State University
        IT@Sam - Administration
        Box 2449
        Huntsville, TX 77341-2449
        USA
        +1.9362944495
        jeb017@shsu.edu

Name Servers:
        NS3.SHSU.EDU
        NS.SHSU.EDU
        NS2.SHSU.EDU

Domain record activated:    13-Mar-1991
Domain record last updated: 26-Dec-2022
Domain expires:             31-Jul-2023
```

```
┌──(cyberboss㉿kali)-[~]
└─$ whois 158.135.1.242
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#

NetRange:       158.135.0.0 - 158.135.255.255
CIDR:           158.135.0.0/16
NetName:        SAM-HOUSTON-NET
NetHandle:      NET-158-135-0-0-1
Parent:         NET158 (NET-158-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Sam Houston State University (SHSU)
RegDate:        1992-03-06
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/158.135.0.0


OrgName:        Sam Houston State University
OrgId:          SHSU
Address:        Information Technology
Address:        P.O. Box 2449
City:           Huntsville
StateProv:      TX
PostalCode:     77341-2449
Country:        US
RegDate:        1991-01-28
Updated:        2021-06-15
Comment:        http://www.shsu.edu
Ref:            https://rdap.arin.net/registry/entity/SHSU


OrgAbuseHandle: JETER14-ARIN
OrgAbuseName:   Jeter, Garrett
OrgAbusePhone:  +1-936-294-1152
OrgAbuseEmail:  gaj003@shsu.edu
OrgAbuseRef:    https://rdap.arin.net/registry/entity/JETER14-ARIN

OrgTechHandle: JETER14-ARIN
OrgTechName:   Jeter, Garrett
OrgTechPhone:  +1-936-294-1152
OrgTechEmail:  gaj003@shsu.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/JETER14-ARIN

OrgAbuseHandle: FUERM-ARIN
OrgAbuseName:   Fuermann, Jason
OrgAbusePhone:  +1-936-294-4140
OrgAbuseEmail:  jason.f@shsu.edu
OrgAbuseRef:    https://rdap.arin.net/registry/entity/FUERM-ARIN

OrgTechHandle: FUERM-ARIN
OrgTechName:   Fuermann, Jason
OrgTechPhone:  +1-936-294-4140
OrgTechEmail:  jason.f@shsu.edu
OrgTechRef:    https://rdap.arin.net/registry/entity/FUERM-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
```

2) Choose one of the followings:

   i. Use **metagoofil** to extract meta data of a compatible file.

```
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ metagoofil -d kali.org -t pdf -l 100 -n 25 -o kalipdf -f kalipdf.html
*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
*] Results: 100 .pdf files found
ttps://iris.kali.org/trackid?ID=31435&FileName=Termodinamica.pdf
ttps://iris.kali.org/trackid?docid=35212&FileName=Rinascimento.pdf
ttps://iris.kali.org/filedownload?article=89378&FileName=Cristalloterapia.pdf
ttps://iris.kali.org/filedownload?ID=88025&FileName=Courant.pdf
ttps://iris.kali.org/viewcontent?docid=37373&FileName=Misbehaviour.pdf
ttps://iris.kali.org/trackid?dataid=89072&FileName=Porcotstico.pdf
ttps://iris.kali.org/trackid?article=94484&FileName=Sermoni.pdf
ttps://iris.kali.org/filedownload?docid=98402&FileName=Tisane.pdf
ttps://iris.kali.org/viewcontent?dataid=47185&FileName=Microeconomia.pdf
ttps://iris.kali.org/filedownload?docid=17193&FileName=Cristianesimo.pdf
ttps://iris.kali.org/filedownload?article=80474&FileName=Queenie.pdf
ttps://iris.kali.org/filedownload?ID=83157&FileName=Wylder.pdf
ttps://iris.kali.org/filedownload?docid=88135&FileName=Hotbloods.pdf
ttps://iris.kali.org/trackid?article=51080&FileName=Plumber.pdf
ttps://iris.kali.org/fulldisplay?dataid=21697&FileName=DITCHED.pdf
ttps://iris.kali.org/trackid?ID=99725&FileName=Folk.pdf
ttps://iris.kali.org/filedownload?dataid=18761&FileName=Finzioni.pdf
ttps://iris.kali.org/trackid?ID=51493&FileName=Ordeal.pdf
ttps://iris.kali.org/viewcontent?article=90479&FileName=Poesie.pdf
ttps://iris.kali.org/viewcontent?dataid=76138&FileName=Follia.pdf
ttps://iris.kali.org/filedownload?article=52451&FileName=Nonluoghi.pdf
ttps://iris.kali.org/trackid?docid=28017&FileName=Lacchiappavirus.pdf
ttps://iris.kali.org/viewcontent?docid=86208&FileName=Hotbloods.pdf
ttps://iris.kali.org/fulldisplay?article=24076&FileName=Viktoria.pdf
ttps://iris.kali.org/filedownload?article=58889&FileName=Reunited.pdf
ttps://iris.kali.org/fulldisplay?docid=91962&FileName=Cuneiform.pdf
ttps://iris.kali.org/trackid?article=41728&FileName=F4.pdf
ttps://iris.kali.org/trackid?ID=26449&FileName=Magico%20Calcio.pdf
ttps://iris.kali.org/trackid?article=24519&FileName=Passo%20Daddio.pdf
ttps://iris.kali.org/trackid?ID=53266&FileName=Welfare%20Responsabile.pdf
ttps://iris.kali.org/fulldisplay?docid=82076&FileName=Interpretazione%20DellECG.pdf
ttps://iris.kali.org/fulldisplay?dataid=40350&FileName=EMERGENCE%20Infestation.pdf
ttps://iris.kali.org/trackid?ID=88544&FileName=Toghe%20Rotte.pdf
ttps://iris.kali.org/filedownload?docid=43144&FileName=The%20Cows.pdf
ttps://iris.kali.org/fulldisplay?article=15991&FileName=Francesco%20Lojacono.pdf
ttps://iris.kali.org/viewcontent?dataid=94392&FileName=Spider%20Sparrow.pdf
ttps://iris.kali.org/viewcontent?article=31574&FileName=Bassa%20Risoluzione.pdf
ttps://iris.kali.org/filedownload?ID=91617&FileName=Hero%20Tales.pdf
ttps://iris.kali.org/trackid?docid=42075&FileName=Nature%20Cure.pdf
ttps://iris.kali.org/trackid?ID=95351&FileName=Marine%20Investigations.pdf
ttps://iris.kali.org/trackid?docid=30130&FileName=Nave%20Super.pdf
ttps://iris.kali.org/filedownload?article=46548&FileName=Room%2013.pdf
ttps://iris.kali.org/trackid?ID=26143&FileName=Deep%20Lipsia.pdf
ttps://iris.kali.org/fulldisplay?docid=99779&FileName=Connettori%20Coassiali.pdf
ttps://iris.kali.org/viewcontent?dataid=63586&FileName=I%20Hogarth.pdf
ttps://iris.kali.org/viewcontent?article=55946&FileName=The%20Craftsman.pdf
ttps://iris.kali.org/fulldisplay?docid=67535&FileName=Punizione%20Divina.pdf
ttps://iris.kali.org/trackid?ID=16756&FileName=Zero%20Limit.pdf
ttps://iris.kali.org/viewcontent?docid=99844&FileName=Im%20Mighty.pdf
ttps://iris.kali.org/filedownload?article=70710&FileName=Surprise%20Daddy.pdf
ttps://iris.kali.org/trackid?ID=21322&FileName=Passion%20DAmour.pdf
ttps://iris.kali.org/viewcontent?docid=71251&FileName=Liquori%20DErbe.pdf
ttps://iris.kali.org/fulldisplay?dataid=60072&FileName=Cinquecento%20Zuppe.pdf
ttps://iris.kali.org/trackid?ID=95950&FileName=Il%20Maiale.pdf
ttps://iris.kali.org/filedownload?ID=96621&FileName=Girl%20Online.pdf
ttps://iris.kali.org/trackid?docid=60101&FileName=The%20Reunion.pdf
ttps://iris.kali.org/fulldisplay?dataid=99022&FileName=Zanna%20Bianca.pdf
ttps://iris.kali.org/trackid?docid=25099&FileName=Shooting%20Stars.pdf
ttps://iris.kali.org/trackid?ID=16348&FileName=ECDL%20CAD.pdf
ttps://iris.kali.org/fulldisplay?dataid=48480&FileName=Sardegna%201200000.pdf
ttps://iris.kali.org/fulldisplay?ID=81289&FileName=Chiesa%20Sinodale.pdf
ttps://iris.kali.org/filedownload?article=57355&FileName=Microorganisms%20Webquest.pdf
ttps://iris.kali.org/viewcontent?ID=57388&FileName=Starry%20Nights.pdf
ttps://iris.kali.org/viewcontent?ID=28770&FileName=13%20Dates.pdf
ttps://iris.kali.org/filedownload?article=45002&FileName=Birthday%20Cakes.pdf
```

ii. Use **exiftool** to extract meta data of an image file taken by a digital camera (including smart phone, etc.)

3) How to defend against network reconnaissance?

One can use IPS/IDS within the network, patching servers to the most up-to-date version, and implementing a firewall.

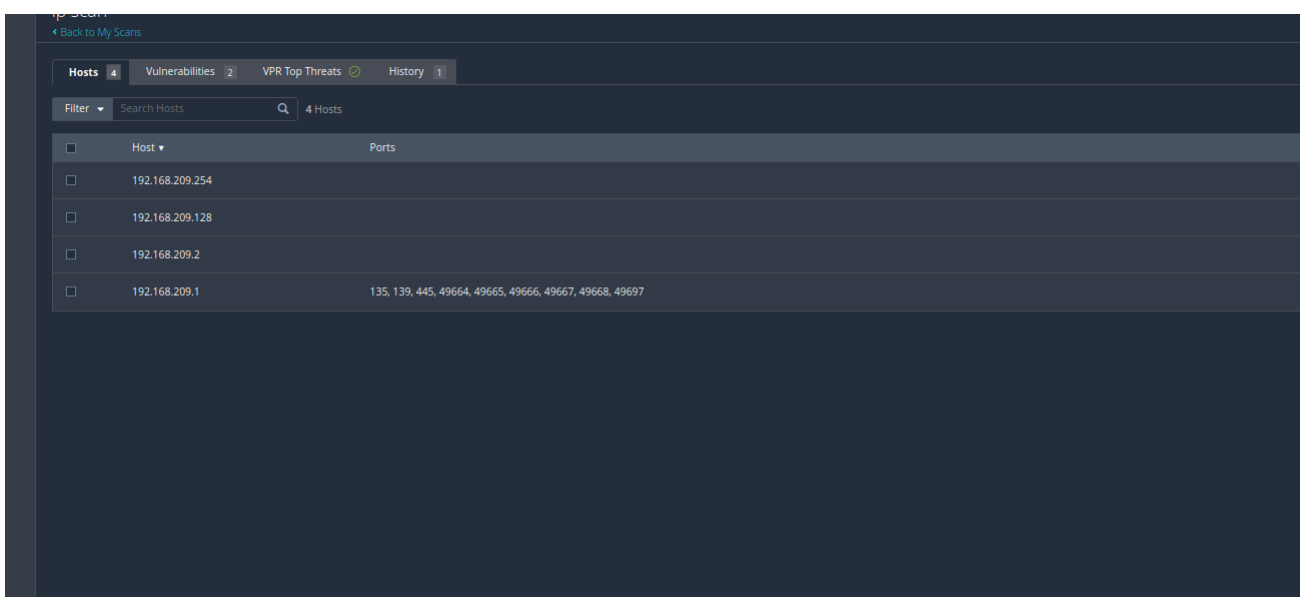
2. Scanning Tools (15 points, 5 points each, screenshots expected)

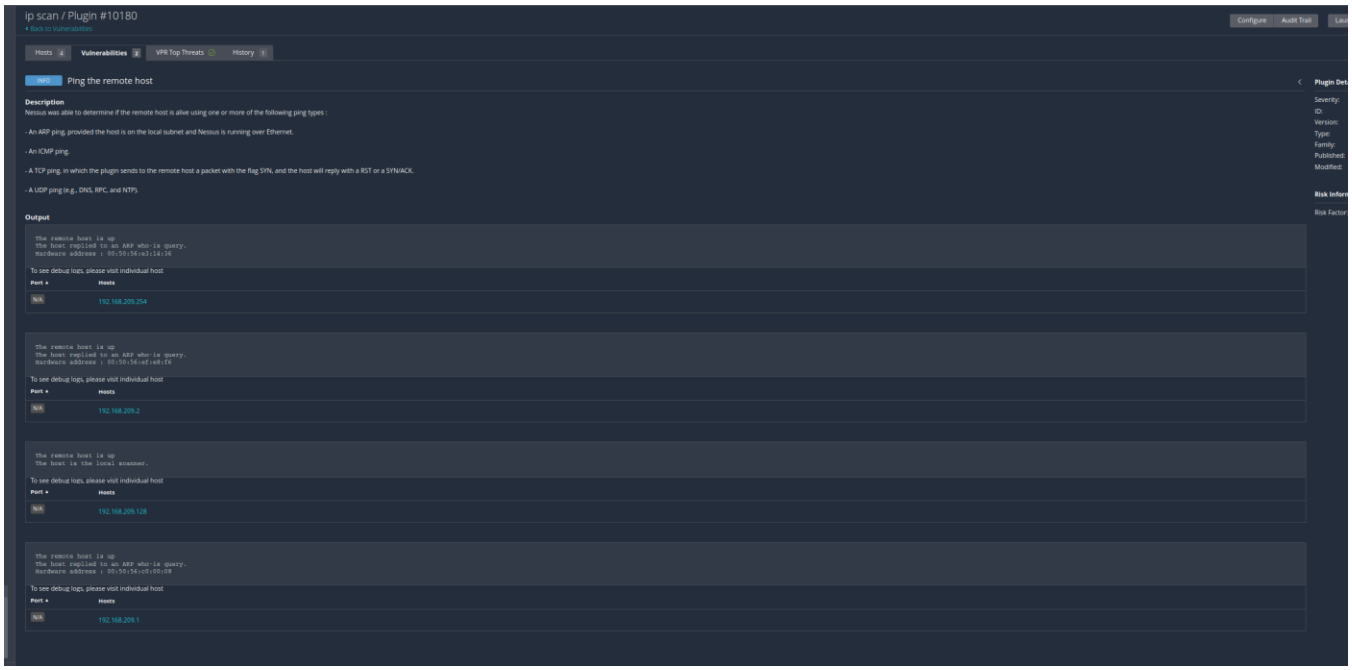
1) **nmap**: use nmap to conduct a local area network scanning for OS fingerprints and version detection where you are authorized to do so.

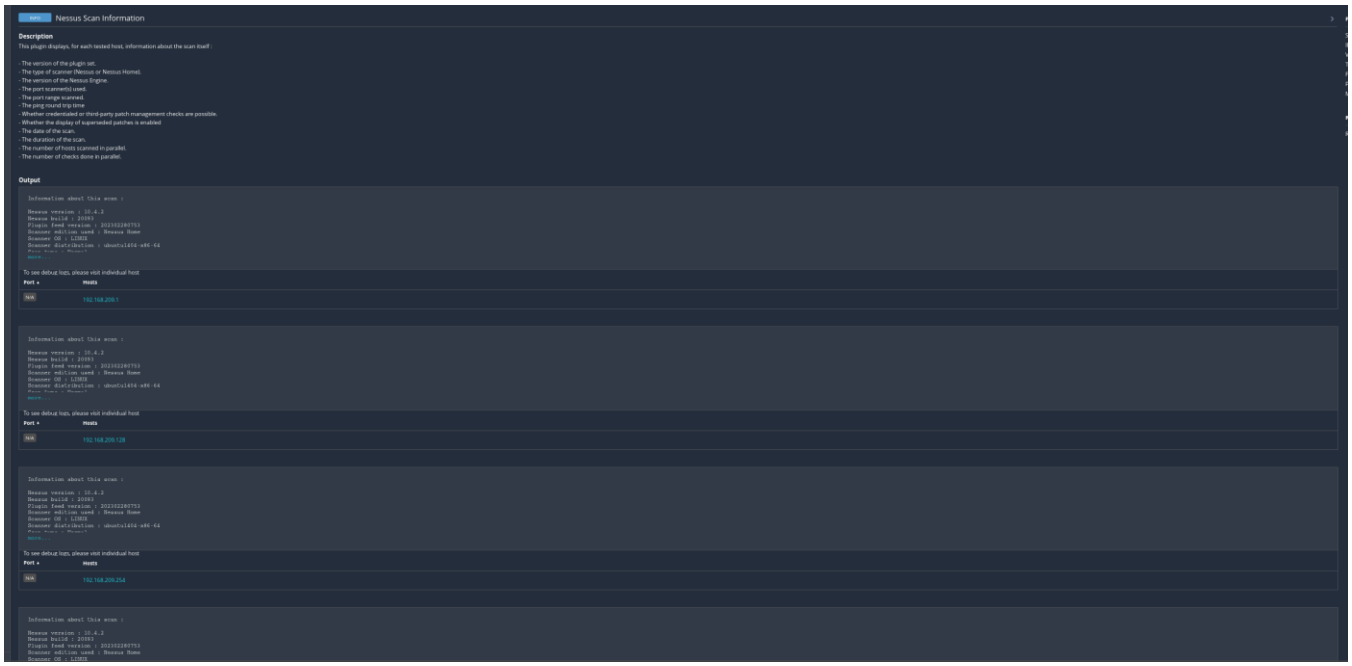
```
┌──(cyberboss㉿kali)-[~]
└─$ sudo nmap -sV  192.168.209.128/24 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 10:31 CST
Nmap scan report for 192.168.209.1
Host is up (0.00097s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, S
OAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SO
AP)
1042/tcp open  afrog?
1043/tcp open  ssl/boinc?
2 services unrecognized despite returning data. If you know the service/versi
on, please submit the following fingerprints at https://nmap.org/cgi-bin/subm
it.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1042-TCP:V=7.93%I=7%D=2/28%Time=63FE2C86%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Origin\r\nCo
SF:ntent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefetch-Contr
SF:ol:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAMEORIGIN
SF:\r\nStrict-Transport-Security:\x20max-age=15552000;\x20includeSubDomain
SF:s\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20nosnif
SF:f\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Policy:\x20
SF:no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text/html;\x2
SF:0charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Tue,\x2028\x20Feb\
SF:x202023\x2016:32:07\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20
SF:html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">\n<tit
SF:le>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\n</bod
SF:y>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Content\r\n
SF:Vary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-Control-Al
SF:low-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Length:\x200\
SF:r\nDate:\x20Tue,\x2028\x20Feb\x202023\x2016:32:07\x20GMT\r\nConnection:
SF:\x20close\r\n\r\n")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nConnection:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP
SF:,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n
SF:")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConn
SF:ection:\x20close\r\n\r\n")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:t\r\nConnection:\x20close\r\n\r\n")%r(SSLSessionReq,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerC
SF:ookie,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\
SF:n\r\n")%r(TLSSessionReq,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConne
SF:ction:\x20close\r\n\r\n")%r(Kerberos,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,2F,"HTTP/1\.1\x2040
SF:0\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(X11Probe,2F,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1043-TCP:V=7.93%T=SSL%I=7%D=2/28%Time=63FE2C91%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,27E,"HTTP/1\.1\x20404\x20Not\x20Found\r\nVary:\x20Origin
SF:\r\nContent-Security-Policy:\x20default-src\x20'self'\r\nX-DNS-Prefetch
SF:-Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-Options:\x20SAME
SF:ORIGIN\r\nStrict-Transport-Security:\x20max-age=15552000;\x20includeSub
SF:Domains\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20
SF:nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r\nReferrer-Polic
SF:y:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nContent-Type:\x20text/ht
SF:ml;\x20charset=utf-8\r\nContent-Length:\x20139\r\nDate:\x20Tue,\x2028\x
SF:20Feb\x202023\x2016:32:18\x20GMT\r\nConnection:\x20close\r\n\r\n<!DOCTY
SF:PE\x20html>\n<html\x20lang=\"en\">\n<head>\n<meta\x20charset=\"utf-8\">
SF:\n<title>Error</title>\n</head>\n<body>\n<pre>Cannot\x20GET\x20/</pre>\
SF:n</body>\n</html>\n")%r(HTTPOptions,D2,"HTTP/1\.1\x20204\x20No\x20Conte
SF:nt\r\nVary:\x20Origin,\x20Access-Control-Request-Headers\r\nAccess-Cont
SF:rol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nContent-Length:
SF:\x200\r\nDate:\x20Tue,\x2028\x20Feb\x202023\x2016:32:18\x20GMT\r\nConne
SF:ction:\x20close\r\n\r\n")%r(FourOhFourRequest,2B6,"HTTP/1\.1\x20404\x20
SF:Not\x20Found\r\nVary:\x20Origin\r\nContent-Security-Policy:\x20default-
SF:src\x20'self';script-src\x20'self'\x20'unsafe-inline';style-src\x20'sel
```

```
SF:c\x20'self'\x20blob:\x20127\.0\.0\.1:1042\x20127\.0\.0\.1:1043;img-src\
SF:x20'self'\x20data:\x20blob:\x20127\.0\.0\.1:1042\x20127\.0\.0\.1:1043\r
SF:\nX-DNS-Prefetch-Control:\x20off\r\nExpect-CT:\x20max-age=0\r\nX-Frame-
SF:Options:\x20SAMEORIGIN\r\nStrict-Transport-Security:\x20max-age=1555200
SF:0;\x20includeSubDomains\r\nX-Download-Options:\x20noopen\r\nX-Content-T
SF:ype-Options:\x20nosniff\r\nX-Permitted-Cross-Domain-Policies:\x20none\r
SF:\nReferrer-Policy:\x20no-referrer\r\nX-XSS-Protection:\x200\r\nDate:\x2
SF:0Tue,\x2028\x20Feb\x202023\x2016:32:18\x20GMT\r\nConnection:\x20close\r
SF:\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x2
SF:0close\r\n\r\n");
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (95%), Microsoft Windows 10|2008 (93%),
Juniper JUNOS 12.X|10.X (86%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microso
ft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008 cpe:/o:fre
ebsd:freebsd:6.3 cpe:/o:juniper:junos:12.1 cpe:/o:juniper:junos:10
Aggressive OS guesses: FreeBSD 6.2-RELEASE (95%), Microsoft Windows 10 (93%),
 Microsoft Windows Server 2008 or 2008 Beta 3 (91%), Microsoft Windows Server
 2008 SP1 (87%), m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3) (86%), Juniper SRX-se
ries firewall (JUNOS 12.1) (86%), Microsoft Windows 10 1703 (86%), Microsoft
Windows 10 1511 - 1607 (86%), Juniper SRX100-series or SRX200-series firewall
 (JUNOS 10.4 - 12.1) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.209.2
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  Simple DNS Plus
MAC Address: 00:50:56:EF:E8:F6 (VMware)
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.209.254
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.209.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:14:36 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.209.128
Host is up (0.000098s latency).
All 1000 scanned ports on 192.168.209.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 38.11 seconds

┌──(cyberboss㉿kali)-[~]
```

2) **Port Scanning**: use Nessus to scan ports of a certain IP or a range of IPs where you are authorized to do so.





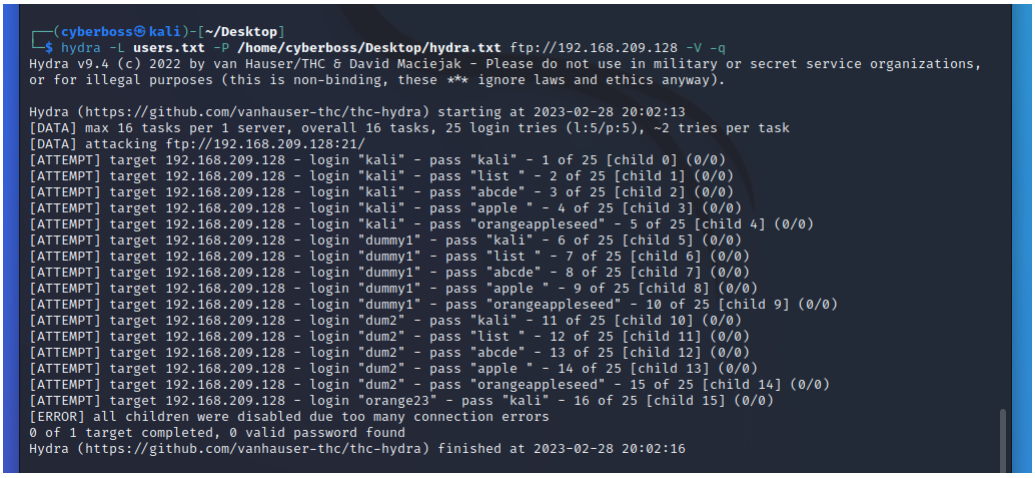


3) How to defend against scanning?

One is able to defend against scanning by implementing a firewall and closing unnecessary ports.

3. Access and Escalation Tools (10 points, 5 points each, screenshots expected)

1) Choose one of the following tools to crack a 6-digit user password in your system: Hydra, John the Ripper, or Cain and Abel, or any other password crack tool runs on your system. You must be authorized to do this, e.g. create a dummy user with random 6-digit password.



```
┌──(cyberboss㉿kali)-[~/Desktop]
└─$ hydra -L users.txt -P /home/cyberboss/Desktop/hydra.txt ftp://192.168.209.128 -V -q
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 2023-02-28 20:02:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://192.168.209.128:21/
[ATTEMPT] target 192.168.209.128 - login "kali" - pass "kali" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.209.128 - login "kali" - pass "list " - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.209.128 - login "kali" - pass "abcde" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.209.128 - login "kali" - pass "apple " - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.209.128 - login "kali" - pass "orangeappleseed" - 5 of 25 [child 4] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dummy1" - pass "kali" - 6 of 25 [child 5] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dummy1" - pass "list " - 7 of 25 [child 6] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dummy1" - pass "abcde" - 8 of 25 [child 7] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dummy1" - pass "apple " - 9 of 25 [child 8] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dummy1" - pass "orangeappleseed" - 10 of 25 [child 9] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dum2" - pass "kali" - 11 of 25 [child 10] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dum2" - pass "list " - 12 of 25 [child 11] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dum2" - pass "abcde" - 13 of 25 [child 12] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dum2" - pass "apple " - 14 of 25 [child 13] (0/0)
[ATTEMPT] target 192.168.209.128 - login "dum2" - pass "orangeappleseed" - 15 of 25 [child 14] (0/0)
[ATTEMPT] target 192.168.209.128 - login "orange23" - pass "kali" - 16 of 25 [child 15] (0/0)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-28 20:02:16
```

2) How to defend against unauthorized access and escalation?

One way to defend against unauthorized access and escalation is by multi-factor authentication and a strong password. When creating a strong password, the confirm that the password is not common enough for a dictionary attack, as well as adding a salt to the password.

4. Exfiltration Tools (10 points, 5 points each)

1) What are the main methods and tools for data exfiltration?

Main methods and tools of data exfiltration is social engineering attacks, inbound emails, and outbound emails. One of the most popular methods within social engineering being phishing attacks. Phishing attacks is an adversary is able to reveal sensitive and important data deceiving untrained users without common cybersecurity knowledge. With social engineering there are many tools that can be used, one being the social engineering toolkit that can be installed within Kali Linux.

-inbound emails

-outbound emails

-social engineering

Tools:

2) How to defend against data exfiltration?

To defend against data exfiltration an organization can disable unauthorized and un-used channels and protocols, educate users, and detection systems. With disabling unauthorized and used channels, there is not an opportunity for adversaries to gain access to ports knowing an organization is not analyzing. With educating users of cyber security best practices, this minimizes the social engineering attacks that happens to many organizations. Finally, with having an IDS/IPS if an organization is to get attack they are able to create a plan for response of the attack.

- Disable unauthorized channels and protocols
- Educate users
- IDS/IPS

5. Sustainment tools (10 points, 5 points each)

1) What are the main methods and tools for continuous access to the systems and networks?

A common method for continuous access to a system a network is a remote access trojan (RAT). With a simple installation of a file by a untrained user, an adversary is able to have access. With creating this RAT, one can create from botnets in a system to a whole C2 server.

-snort

-SolarWinds

-tenable

2) What are the main methods and tools used against backdoors?

According to the book, a backdoor is "any mechanism that bypasses a normal security check, that may allow unauthorized access." [6] W. Stallings and L. Brown, *Computer security*. s.l.: Pearson Education (US), 2017. By this definition, main methods and tools to use against backdoors would be antiviruses, firewalls, and up to date patches within the system.

6. Assault Tools (5 points)

1) What are the most commonly seen assaulting methods and tools?

The most commonly used assaulting methods and tools are malware, phishing and spear phishing attacks. Using malware as a tool, for example a rootkit, once the

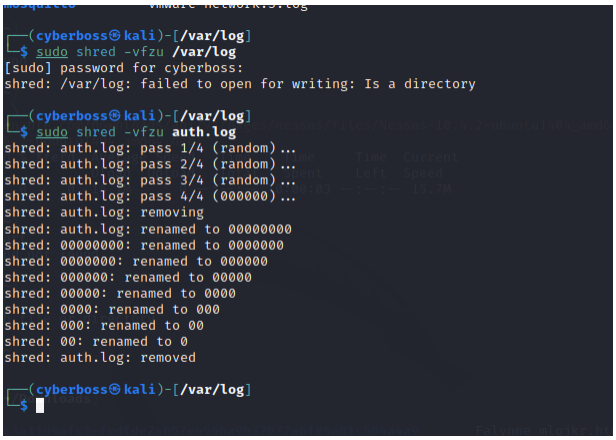
rootkit is installed on the system the adversary is able to gain control to the entire system of a device, and gain admin credentials.

7. **Obfuscation Tools (10 points, 5 points each)**

   1) What is the most common way to obscure location? Give examples.

      The most common way to obscure a location is using a VPN(virtual private network). A simple example would be an adversary hacking into a system within the United States but using a VPN could track back that the adversary is in maybe Europe instead of the actual location.

   2) Attach screenshots to show that you can use proper tool to manipulate system logs.



Works Cited

W. Stallings and L. Brown, *Computer security*. s.l.: Pearson Education (US), 2017.