



SAKARYA
ÜNİVERSİTESİ

BSM 441

Sistem Yöneticiliği

Dr. Öğr. Üyesi HÜSEYİN ESKİ
heski@sakarya.edu.tr

~ **SUNUCU GÜVENLİĞİ** ~

SUNUCU GÜVENLİĞİ

- Sunucu güvenliği her yıl şirketler, hükümetler, organizasyonlar ve kişiler için daha önemli bir konu haline gelmektedir.
- Hackerlar da her geçen gün daha bilgili bir hale gelmektedir ve organizasyon, şirketler, hükümet ile kişilerin güvenlik açıklarını yakalayabilmektedirler. Bu sebeple birçok kişi bu tehdit ile karşı karşıya kalmaktadır.
- Siber saldırılar sebebi ile birçok şirket ve kişi hem bilgi kaybına hem de maddi kayıtlarla karşılaşmaktadır.
- Bunun sebeplerinden birisi de kişi ve şirketlerin hala eski teknoloji kullanmış olmalarıdır. Bu da korsanların işini kolaylaştırmaktadır. Dijitalleşen dünyada şirketler ve kişiler sunucu güvenliğine önem vererek sistemlerini geliştirmelidir; böylece saldırılara karşı korunmalarını sağlayabilmektedirler.

ALINACAK TEDBİRLER

Bilgisayar sistemlerinin güvenli olması için birçok çalışma yapılabilmektedir.

Genellikle kullanılan çözümler arasında:

- Güvenlik duvarları sağlamak
- Güvenli iletişim protokolleri sağlamak
- Saldırı tespiti kurmak
- Zarar verici kodlara karşı yazılımlar kullanmak
- Güncel işletim sistemi kullanmak

ALINACAK TEDBİRLER

- RDP (3389) ve önemli portları değiştirin
- Network ayarlarından sadece IPv4 aktif olsun

ALINACAK TEDBİRLER

Bu önlemlere rağmen, sisteme saldıranların faydalanabileceği açıklar olabilmektedir.

- Çeşitli güvenlik araçları kullanarak sunuculardaki açıklar tespit edilebilmektedir ve böylece gerekli önlemler alınabilmektedir.
- Genellikle bilgisayar sistemlerine saldırması amacı ile geliştirilen güvenlik araçları sistemi izleme olanağı da sunmaktadır. Asıl geliştirilme amaçları da budur. Temel düşünce, sistemin açığını saldırgandan önce ortaya çıkartarak gerekli önlemleri almaktır.

GÜVENLİK TARAMA UYGULAMALARI

- Nessus
- Nmap
- Ethereal

GÜVENLİK TARAMA UYGULAMALARI

NESSUS

Uzaktan tarama aracı olarak kullanılan güncel ve güçlü bir uygulamadır.

Windows ve UNIX türevi üzerinde çalışabilmektedir. Nessus, uyumlu ek yazılımları ile Gtk arayüzü çok kullanışlıdır. Yakaladığı 1200'den fazla güvenlik açığını çeşitli biçimde raporlar sunabilmektedir. Nessus, bilinen kurallara bağlı olmadan tarama yapabilmektedir.



GÜVENLİK TARAMA UYGULAMALARI

NMAP

Açık kaynak kodlu bir programdır. Güvenlik denetlemelerinde ve ağ araştırmasında kullanılabilmektedir. Tek bir konak üzerinde çalışabildiği gibi geniş ölçekli ağ tarama amacı ile de kullanılabilmektedir. Alışılmıştan farklı olarak IP paketleri yollayarak ağ üzerinde canlı bilgisayarı göstermektedir. İlaveten bilgisayar üzerinde ağa sunulan uygulamaları da tespit edebilmektedir. Hangi işletim sistemi ve hangi güvenlik duvarının kullanıldığını bulabilmektedir.

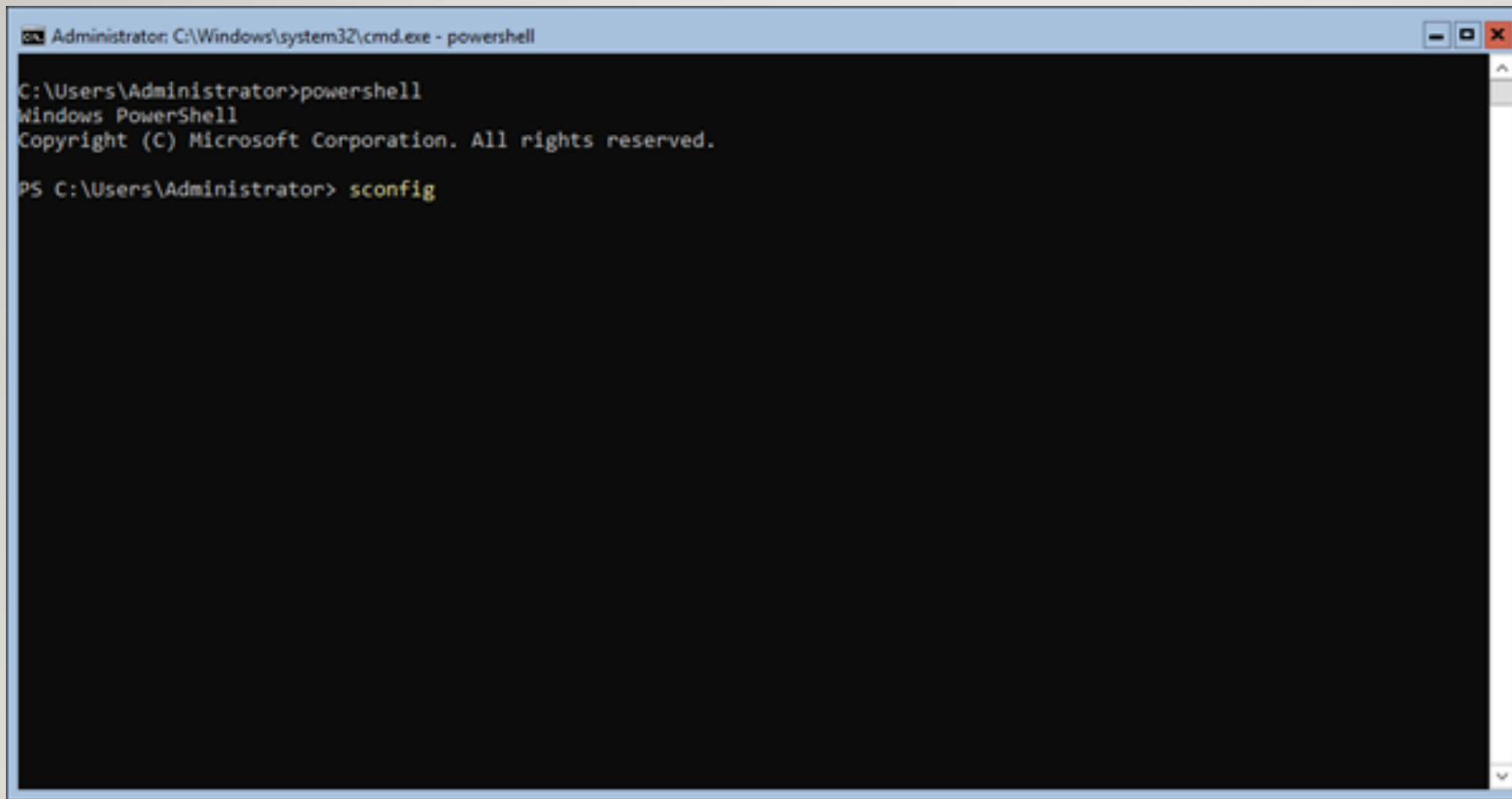


GÜVENLİK TARAMA UYGULAMALARI ETHERREAL

Ücretsiz olan bu güvenlik aracı, Windows ve UNIX için ağ analizcisidir. Canlı bir ağ ile ya da daha önceden kaydedilmiş bir ağ verisi ile çalışarak ağ incelemesini gerçekleştirebilmektedir. İnteraktif olarak incelenen veri hakkında kullanıcı ayrıntılı bilgi alabilmektedir. Zengin süzme diline ve TCP oturumu birleştirerek analiz imkanı tanınması özellikleri arasındadır.

WINDOWS CORE YAPILANDIRMASI

- **sconfig**



```
Administrator: C:\Windows\system32\cmd.exe - powershell
C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> sconfig
```

WINDOWS CORE YAPILANDIRMASI

```
Administrator: C:\Windows\system32\cmd.exe - powershell
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

=====
                        Server Configuration
=====

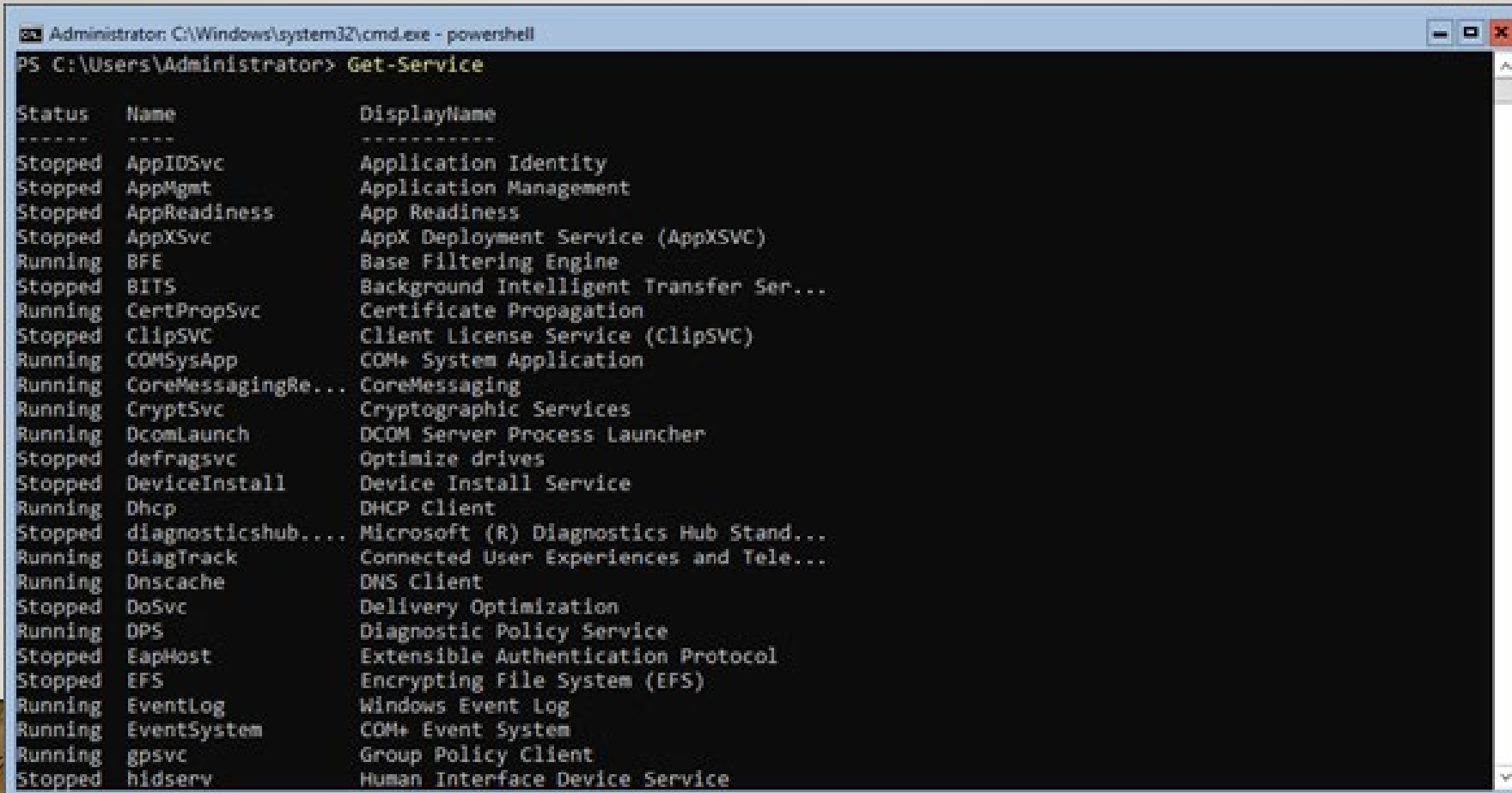
1) Domain/Workgroup:                Workgroup: WORKGROUP
2) Computer Name:                   WIN-58QLF7G306H
3) Add Local Administrator
4) Configure Remote Management      Enabled
5) Windows Update Settings:         DownloadOnly
6) Download and Install Updates
7) Remote Desktop:                  Disabled
8) Network Settings
9) Date and Time
10) Telemetry settings               Unknown
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option: 
```

WINDOWS CORE YAPILANDIRMASI

- Get-service komutu ile çalışan servislerinizi görüntüleyebilirsiniz.

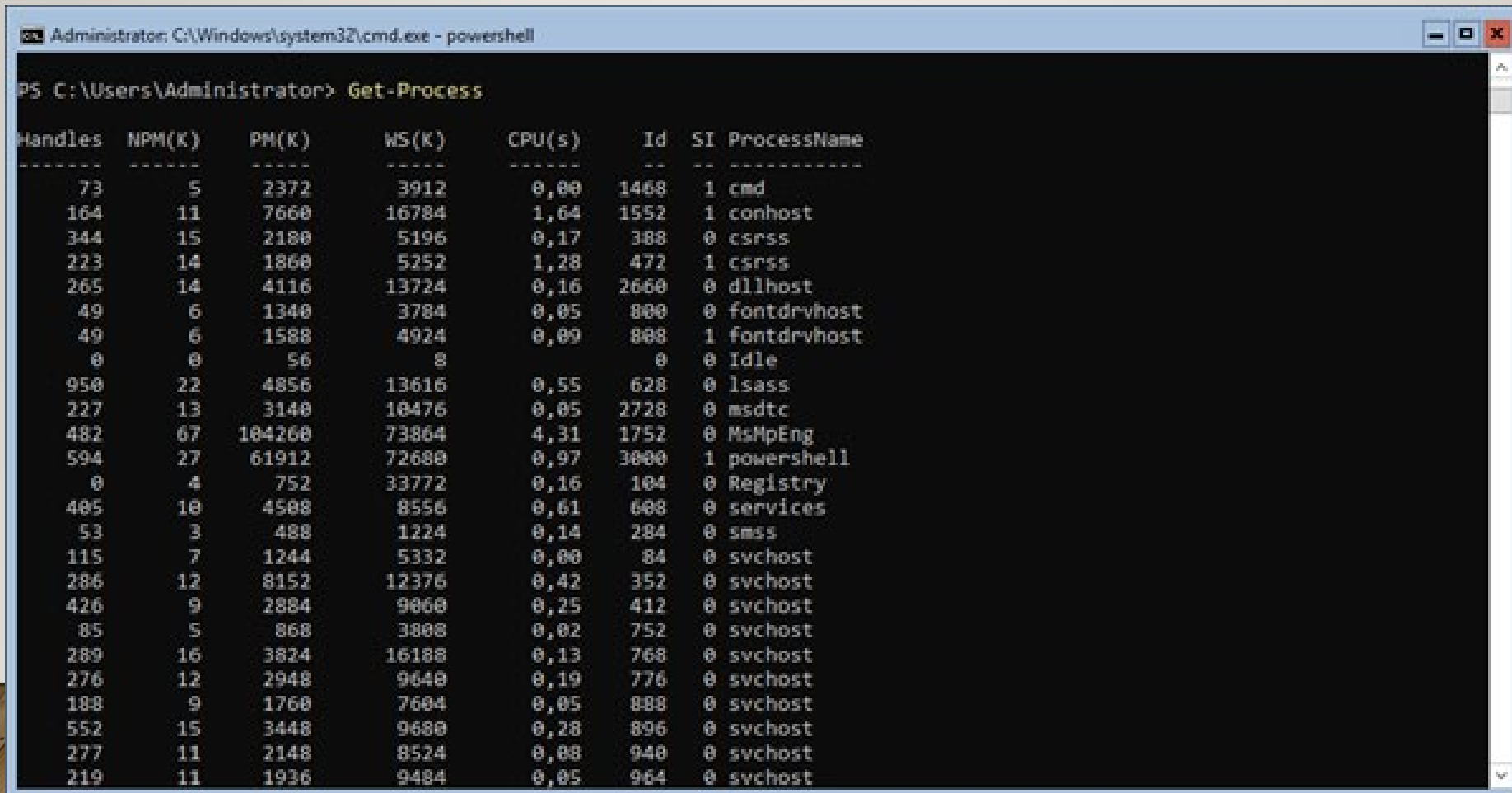


```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\Users\Administrator> Get-Service

Status      Name                DisplayName
-----
Stopped     AppIDSvc            Application Identity
Stopped     AppMgmt             Application Management
Stopped     AppReadiness        App Readiness
Stopped     AppXSvc             AppX Deployment Service (AppXSVC)
Running     BFE                 Base Filtering Engine
Stopped     BITS                Background Intelligent Transfer Ser...
Running     CertPropSvc         Certificate Propagation
Stopped     ClipSVC             Client License Service (ClipSVC)
Running     COMSysApp            COM+ System Application
Running     CoreMessagingRe...  CoreMessaging
Running     CryptSvc             Cryptographic Services
Running     DcomLaunch          DCOM Server Process Launcher
Stopped     defragsvc           Optimize drives
Stopped     DeviceInstall       Device Install Service
Running     Dhcp                DHCP Client
Stopped     diagnosticshub....  Microsoft (R) Diagnostics Hub Stand...
Running     DiagTrack           Connected User Experiences and Tele...
Running     Dnscache            DNS Client
Stopped     DoSvc               Delivery Optimization
Running     DPS                 Diagnostic Policy Service
Stopped     EapHost             Extensible Authentication Protocol
Stopped     EFS                 Encrypting File System (EFS)
Running     EventLog            Windows Event Log
Running     EventSystem         COM+ Event System
Running     gpsvc               Group Policy Client
Stopped     hidserv             Human Interface Device Service
```


WINDOWS CORE YAPILANDIRMASI

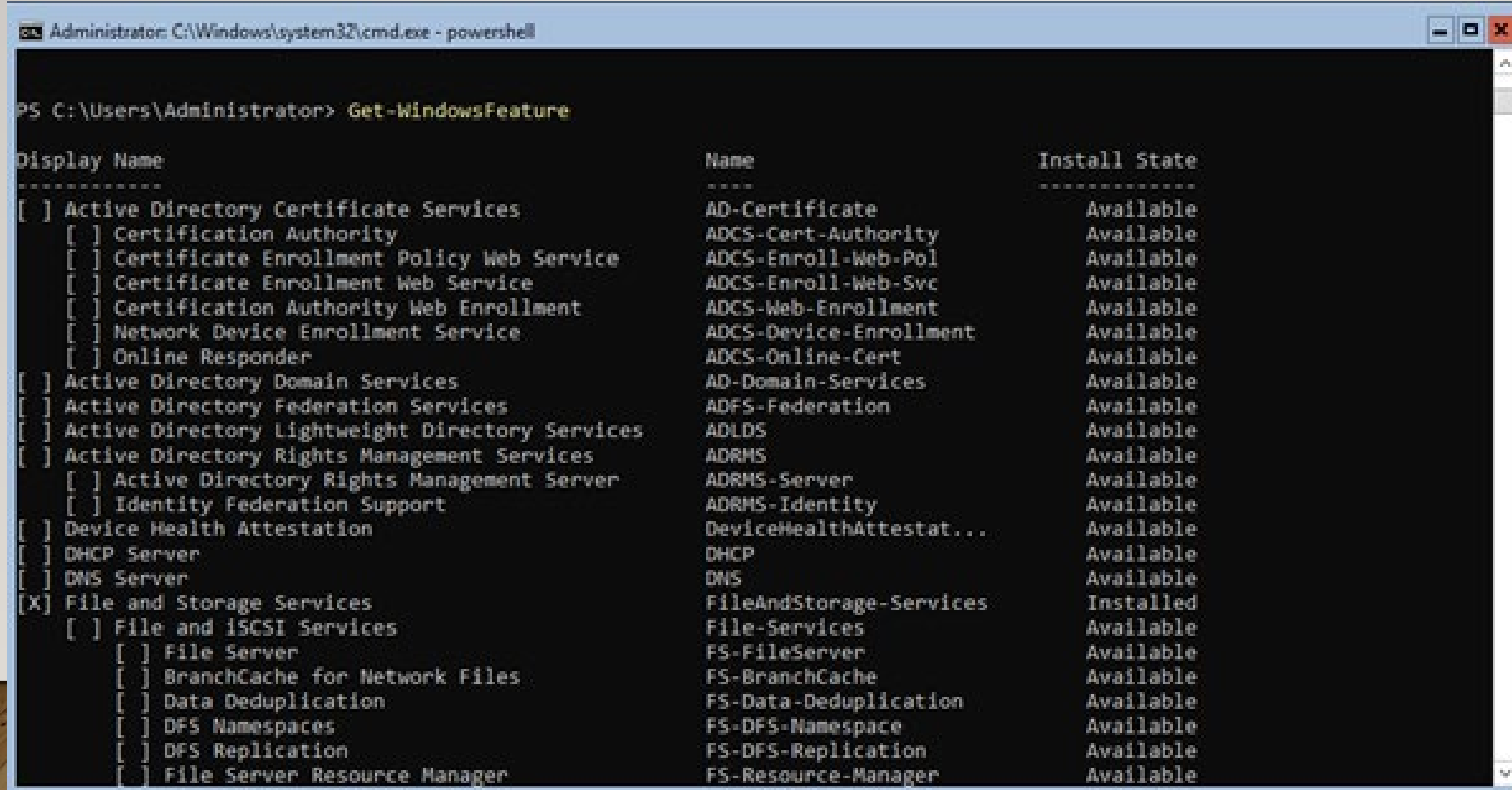
- Get-process komutu ile sunucunuz üzerindeki işlemleri görüntüleyebilirsiniz.



Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
73	5	2372	3912	0,00	1468	1	cmd
164	11	7660	16784	1,64	1552	1	conhost
344	15	2180	5196	0,17	388	0	csrss
223	14	1860	5252	1,28	472	1	csrss
265	14	4116	13724	0,16	2660	0	dllhost
49	6	1340	3784	0,05	800	0	fontdrvhost
49	6	1588	4924	0,09	808	1	fontdrvhost
0	0	56	8		0	0	Idle
950	22	4856	13616	0,55	628	0	lsass
227	13	3140	10476	0,05	2728	0	msdtc
482	67	104260	73864	4,31	1752	0	MsMpEng
594	27	61912	72680	0,97	3000	1	powershell
0	4	752	33772	0,16	104	0	Registry
405	10	4508	8556	0,61	608	0	services
53	3	488	1224	0,14	284	0	smss
115	7	1244	5332	0,00	84	0	svchost
286	12	8152	12376	0,42	352	0	svchost
426	9	2884	9060	0,25	412	0	svchost
85	5	868	3808	0,02	752	0	svchost
289	16	3824	16188	0,13	768	0	svchost
276	12	2948	9640	0,19	776	0	svchost
188	9	1760	7604	0,05	888	0	svchost
552	15	3448	9680	0,28	896	0	svchost
277	11	2148	8524	0,08	940	0	svchost
219	11	1936	9484	0,05	964	0	svchost

WINDOWS CORE YAPILANDIRMASI

- Get-WindowsFeature komutu ile sunucunuz üzerinde kurulu olan ve kurulmak için uygun olan tüm roles and features görüntüleyebilirsiniz.



```
Administrator: C:\Windows\system32\cmd.exe - powershell

PS C:\Users\Administrator> Get-WindowsFeature

Display Name                                Name                                Install State
-----
[ ] Active Directory Certificate Services    AD-Certificate                      Available
[ ] Certification Authority                  ADCS-Cert-Authority                Available
[ ] Certificate Enrollment Policy Web Service ADCS-Enroll-Web-Pol                Available
[ ] Certificate Enrollment Web Service       ADCS-Enroll-Web-Svc                Available
[ ] Certification Authority Web Enrollment   ADCS-Web-Enrollment                Available
[ ] Network Device Enrollment Service        ADCS-Device-Enrollment             Available
[ ] Online Responder                        ADCS-Online-Cert                    Available
[ ] Active Directory Domain Services         AD-Domain-Services                 Available
[ ] Active Directory Federation Services     ADFS-Federation                     Available
[ ] Active Directory Lightweight Directory Services ADLDS                               Available
[ ] Active Directory Rights Management Services ADRMS                               Available
[ ] Active Directory Rights Management Server ADRMS-Server                       Available
[ ] Identity Federation Support              ADRMS-Identity                     Available
[ ] Device Health Attestation                DeviceHealthAttestat...            Available
[ ] DHCP Server                             DHCP                                Available
[ ] DNS Server                              DNS                                 Available
[X] File and Storage Services                FileAndStorage-Services             Installed
[ ] File and iSCSI Services                  File-Services                       Available
[ ] File Server                             FS-FileServer                      Available
[ ] BranchCache for Network Files            FS-BranchCache                     Available
[ ] Data Deduplication                      FS-Data-Deduplication               Available
[ ] DFS Namespaces                          FS-DFS-Namespaces                   Available
[ ] DFS Replication                         FS-DFS-Replication                  Available
[ ] File Server Resource Manager             FS-Resource-Manager                 Available
```

WINDOWS SUNUCU KONTROL LİSTESİ

- Destek verilen güncel Windows işletim sistemleri kullanının.
- Basic Input Output System(BIOS)** ayarları alanını parola ile koruyun.
- Sunucuları yerel modda kullanmaya çalışın(mümkünse).
- Otomatik Güncellemeleri aktif etmeli, **SSCM** kullanılmalı(mümkünse).
- Sunucu üzerinde yetkileri belirleyen listeler olmalı ve bu hiyerarjiye uyulmalı.
- Sunucuların düzenli olarak yedekleri alınmalı.
- Sunucular **Active Directory** üzerine aktarılmalı.

WINDOWS SUNUCU KONTROL LİSTESİ

- Sunucular arası iletişim için VPN kullanılmalı .
- Parolaların sık aralıklarla değiştirilmesi (3–6 Ay).
- Büyük ve küçük harfler, sayılar ve özel karakterler (!, #, \$ Ve% gibi) içeren en az 12 ila 14 karakterden oluşan güçlü parolalar kullanılmalı.
- Belli bir zaman aralığında 3 ya da daha fazla geçersiz parola denemesinde user devre dışı bırakılmalı.
- Logların belli aralıklar ile takip edilmeli.

WINDOWS SUNUCU KONTROL LİSTESİ

- Sistemde kurulu anti-virüs uygulaması ile belli aralıklarla tarama yapılmalı
- Güvenlik Duvarını aktif edilmeli.
- Kullanılmayan portlara erişim kalıcı olarak kapatılmalı.
- RDP bağlantısı yapılıyorsa default portu değiştirilmeli.

WINDOWS SUNUCU KONTROL LİSTESİ

- Uzak masaüstü bağlantılarında VPN kullanılmalı.
- Sunucunun kullanılmayan bütün özellikleri devre dışı bırakılmalı(yazıcı paylaşımı, dosya paylaşımı vb.)
- Mümkünse tüm internet tarayıcıları kaldırılmalı.
- Phishing(Oltalama) saldırılarına mağruz kalmamak için tüm e-posta istemcileri kaldırılmalı

WINDOWS SUNUCU KONTROL LİSTESİ

- Kullanıcı hesap denetimini etkinleştirilmeli ve kuralları operatörlere göre düzenlenmeli.
- Web sunucusu üzerinde kullanılacak bütün web sitelerinde TLS kullanımına özen gösterilmeli.
- Yedekleme için en az iki DNS sunucusu ve komut isteminden nslookup kullanarak çift onay ad çözümlemesi yapılandırılmalı.
- Sunucunun, istediğiniz adla birlikte DNS'de geçerli bir A kaydının yanı sıra geriye doğru aramalar için bir PTR kaydının olduğundan emin olunmalı.

WINDOWS SUNUCU KONTROL LİSTESİ

- Telnet, FTP gibi şifrelenmemiş protokoller kullanılmamalı.
- Dosya yükleme işlemleri mümkün olduğunca SFTP üzerinden gerçekleştirilmeli.
- Sunucumuzda önemli olan servisler otomatik başlayacak şekilde ayarlanmalı.
- Misafir hesaplar devre dışı bırakılmalı
- Kullanılmayan user'lar hemen devre dışı bırakılmalı ya da silinmeli.
- Ncacn_ip_tcp kaldırılmalı.
- TCP / IP üzerinden NetBIOS'u devre dışı bırakılmalı.

WINDOWS SUNUCU KONTROL LİSTESİ

- LAN Manager kimlik doğrulama seviyesini sadece NTLMv2'ye izin vermeli ve LM ile NTLM'yi reddetmek için ayarlanmalı.
- NTFS veya BitLocker ile yerleşik dosya şifrelemesini etkinleştirin.
- Windows Server lisans anahtarları mutlaka girilmeli.
- Ek olarak fiziksel faktörlerede dikkat edilmeli (Örn: Su baskını, yüksek ısı, kitli odada muhafaza etme, statik elektrik vb.)

LINUX İÇİN BİRKAÇ ÖNERİ

- Root erişimlerini kaldırın
- SSH Portunun Değiştirilmesi
- SSH Anahtar Çifti Kullanımı
- Firewall Uygulamasının Kurulumu
- Fail2Ban Kullanmak
- Gereksiz Servisleri Kapatın
- Açık Portları Kontrol Edin
- /var, /usr, /home dizinlerini ayrı disklerle bağlamak

LINUX İÇİN BİRKAÇ ÖNERİ

- **Kurulduktan sonra kullanılmayacak bileşenler silinmeli**
 - git ve mc, rsh, rlogin, rcp, rdate, rdist, rusers, rwall, rwho, ntalk, talk, telnet sunucu, Xwindows ile ilgili her türlü program, KDE, QT kütüphaneleri C, C++, tk, derleyici ve yorumlayıcıları, Snmpd yazılımı, NFS ve NIS ile ilgili herşey.

LINUX İÇİN BİRKAÇ ÖNERİ

- **Kullanıcı hesapları**
 - Hackleme işleminde yapılan saldırılardan çoğu kullanıcı ve parola ile yapılmaktadır
 - Parola güvenlik politikaları belirlenmeli
- **Hosts.deny veya host.allow**
 - `sshd: 195.244.37.241 trlinux.com`

KAYNAKÇA

-
- <https://webdunya.com/sunucu-guvenliginin-onemi/>
 - <https://yakupseker.medium.com/windows-sunucu-g%C3%BCvenli%C4%9Fi-dikkat-edilmesi-gereken-ad%C4%B1mlar-c69f0ddf04b8>