

Defansif Windows Temelleri (Defensive Windows Basics)

Windows Dosya Sistemi Yapısı

Sectors: Diskteki en küçük fiziksel depolama birimi

-Windowsta, her sektörün boyutu 512 bayttır.

Cluster(Küme): Bir veya daha fazla bitişik sektör grubuna küme denir.

Volume(Disk): Bir veya daha fazla kümeden oluşan bir diskin mantıksal bölümlenmesi

-Volume(disk) boşluk alanları, dosyaları, sistemi ve sistem bilgilerini içerir.

File Allocation Table (FAT)

Küçük boyutlu diskler için tasarlanmıştır.

NTFS

Her sektör 512 bayttır.

Her küme 2 sektörden oluşur.

NTFS (New Technology File System)

Sıkıştırma ve depolama da daha iyi.

Standard information

File Name

Security Descriptor..

Dosya Sisteminin Performansı

Verimli veri yapılarının kullanımı

Etkili disk ayırma

Önbelleğe alma

Arabelleğe alma

Disk Zamanlayıcı

Command Prompt (CMD.exe)

Dir

Cd, chdir

Md, mkdir

Rm, rmdir

Help

Copy

Move

Ren, rename

Del

Exit

Echo

Type

Fc
Cls
Color
Date
Hostname
Pause
Runas
Sort
Start
Tasklist
Ftp
Ftype
Getmac
Ipconfig
Netsh
Netstat
Nslookup
Pathping
Chkdsk
Chkntfs
Defrag

Çalışan Process ve Servis Bilgilerini Öğrenmek için:

Su anda çalışan tüm işlemleri listeler:

C:\> tasklist

Su anda çalışan tüm işlemleri ve her birinin yüklediği DLL'leri listeler:

C:\> tasklist /m

Belirtilen [dll]lerin çalışan tüm işlemleri listeler:

C:\> tasklist /m dll

Çalışan tüm işlemleri ve bu işlemlerde yer alan servisleri listeler:

C:\> tasklist /svc

Tüm servislerin çalışma durumunu sorgular:

C:\> sc query

Belirtilen servisin konfigürasyonunu sorgular:

C:\> sc qc [ServisAdı]

Kullanışlı Netstat Parametreleri

Tüm TCP ve UDP portlarının kullanımını ve process ID'lerini gösterir

C:\> netstat -nao

N saniyede bir [port] bağlantı noktası kullanımını kontrol eder:

C:\> netstat -nao [N] | find [port]

Ayrıntılı protokol istatistiklerini gösterir :

C:\> netstat -s -p [tcp|udp|ip|icmp]

Kapatma ve Yeniden Başlatma

Windows'u hemen kapatır:

C:\> shutdown /s /t 0

Not: Bu komut donanımı kapatmayabilir.

Windows'u hemen yeniden başlatır:

C:\> shutdown /r /t 0

Kapatma / Yeniden Başlat geri sayımını iptal eder:

C:\> shutdown /a

Komut Satırında Yararlı GUI'leri Çağırarak:	Netsh Kullanarak Ağ ile Etkileşim
<p>Local User Manager(Grup Yöneticisini de içerir) C:\> <u>lusrmgr.msc</u> Services Control Panel: C:\> <u>services.msc</u> Task Manager: C:\> <u>taskmgr.exe</u> Security Policy Manager: C:\> <u>secpol.msc</u> Event Viewer: C:\> <u>eventvwr.msc</u> Control Panel: C:\> <u>control</u></p> <p>ALT+F4 'e basarak gui'yi kapatabilirsiniz.</p>	<p>Windows Firewall'ı kapatır: C:\> <u>netsh firewall set opmode disable</u> [IPAddr] [Netmask] [DefaultGW] ile "Yerel Alan Bağlantısı" arayüzünü yapılandırın C:\> <u>netsh interface ip set address local static [IPAddr] [Netmask] [DefaultGW] 1</u> DNS sunucusunu "Yerel Alan Bağlantısı" için yapılandırın: C:\> <u>netsh interface ip set dns local static [IPAddr]</u> DHCP kullanım arayüzünü yapılandırın : C:\> <u>netsh interface ip set address local dhcp</u></p>
<p>Bütün ve Ayrıntılı Windows Komutları linki: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands</p>	

PowerShell

Özelleştirilebilir (cmdlet)

PowerShell vs CMD

PowerShell	Command Prompt(CMD)
.NET Framework ile yazılmış bir görev tabanlı komut satırı arayüzü ve komut dosyası(Scripting) ortamıdır.	Microsoft Windows işletim sistemleri için komut satırı yorumlayıcısıdır.
"Cmdlet" adı verilen çok daha güçlü işlevler kullanır	Çoğunlukla dize tabanlıdır ve standart işlevlere sahip eski "batch dili" dir. (bash-script gibi düşünün)
Batch Komutlarını(cmd komutları) ve PowerShell komutlarını yorumlayabilir.	Yalnızca Batch Komutları yorumlayabilir.
Üretilen çıktı yalnızca bir metin akışı değil, aynı zamanda bir nesne topluluğudur.	Oluşturulan çıktı sadece bir karakter akışıdır (metin).

PowerShell Temel komutları

Komut Adı	Alias	Kullanımı
Set-Location	cd, chdir, sl	Geçerli çalışma konumunu belirtilen bir konuma ayarlar.
Get-Content	cat, gc, type	Belirtilen konumdaki öğenin içeriğini alır.
Add-Content	ac	Belirtilen öğelere, dosyaya sözcük ekleme gibi içerik ekler.
Set-Content	sc	Bir öğedeki içeriği yeni içerikle yazar veya değiştirir.
Copy-Item	copy, cp, cpi	Bir öğeyi bir konumdan diğerine kopyalar.
Remove-Item	del, erase, rd, ri, rm, rmdir	Belirtilen öğeleri siler.
Move-Item	mi, move, mv	Bir öğeyi bir konumdan diğerine taşır.
Set-Item	si	Bir öğenin değerini komutta belirtilen değere değiştirir.
New-Item	ni	Yeni bir öğe oluşturur.
Start-Job	sajb	Windows PowerShell arka plan işini başlatır.

Komut Adı	Alias	Kullanımı
Compare-Object	compare, dif	İki nesne kümesini karşılaştırır.
Group-Object	group	Belirtilen özellikler için aynı değeri içeren nesneleri gruplandırır.
Add-Content	ac	Belirtilen öğelere, dosyaya sözcük ekleme gibi içerik ekler.
Invoke-WebRequest	curl, iwr, wget	İnternetteki bir web sayfasından içerik alır.
Measure-Object	measure	Nesnelerin sayısal özelliklerini ve dosyalar gibi dize nesnelerindeki karakterleri, kelimeleri ve çizgileri hesaplar.
Resolve-Path	rvpa	Bir dosya yolundaki özel karakterleri çözer ve yol içeriğini görüntüler.
Resume-Job	rujb	Askıya alınmış bir işi yeniden başlatma
Set-Variable	set, sv	Değişkenin değerini ayarlar. İstenen ada sahip bir değişken yoksa değişkeni oluşturur.
Show-Command	shcm	Grafiksel komut penceresinde Windows PowerShell komutları oluşturur.

Komut Adı	Alias	Kullanımı
Start-Service	sasv	Durdurulmuş bir veya daha fazla hizmeti başlatır.
Start-Process	saps, start	Yerel bilgisayarda bir veya daha fazla işlem başlatır.
Suspend-Job	sujb	İş akışı işlerini geçici olarak durdurur.
Wait-Job	wj	Oturumda çalışan Windows PowerShell arka plan işlerinden biri veya tümü yüklenene kadar komut istemini bastırır.
Where-Object	?, where	Bir koleksiyondaki nesneleri özellik değerlerine göre seçer.
Write-Output	echo, write	Belirtilen nesneleri ardışık düzende bir sonraki komuta gönderir. Komut, ardışık düzendeki son komutsa, nesneler konsolda görüntülenir.
Sort-Object	sort	Nesneleri özellik değerlerine göre sıralar.

Hatalar

Zayıf Şifreler

Virüs bulaşmış olan yazılım

Eksik veri şifrelemesi

Eriřim izinlerinin düzenlenmesi
Güncellik
Standartlar
Network koruma önlemlerinin kullanılması
Çalışan eğitilmesi

IloveYou
Goggle (phishing)
180Solutions.SerachAssistant

BitTorrent.exe
(%18 malware)

StuxNet
SCADA sistemleri ve İran nükleer saldırısı

WannaCry
Ransomware

Hardening (sıkılařtırma)

Kullanılan sistemin kontrol edilmesi
Sistemin sıkılařtırılması için stratejisi oluşturulması
Açıkların kapatılması
Network ve sunucu sıkılařtırması

Konu Başlığı	Sebebi
<u>Kullanıcı Yapılandırılması</u>	<u>Kimlik bilgilerinizi korumak</u>
<u>Network Yapılandırılması</u>	<u>Networkü kontrol etmek</u>
<u>Özelliklerin ve Rollerin Yapılandırılması</u>	<u>İhtiyacınız olanı ekleyin, yapmadığınızı kaldırın</u>
<u>Kurulumları Güncelleme</u>	<u>Güvenlik açıklarının yamalarını güncellemek etmek</u>
<u>NTP Yapılandırılması</u>	<u>Clock Skew'i(Zaman kaynağındaki gecikme/kayma) önleyin.</u>
<u>Firewall Yapılandırılması</u>	<u>Güvenlik duvarından maksimum verim almak</u>
<u>Uzaktan Eriřim Yapılandırılması</u>	<u>Administrator sessionlarını uzaktan erişim için sıkılařtırmak</u>
<u>Servislerin Yapılandırılması</u>	<u>Saldırı yüzeyinizi en aza indirin</u>
<u>İleri seviye sıkılařtırma</u>	<u>İřletim sistemini ve diğeri uygulamaları koruyun</u>
<u>Loglama ve İzleme</u>	<u>Sisteminizde neler olup bittiğini bilin</u>

Kullanıcı yapılandırması

Güçlü parola
Parola geçerlilik süresi

Network Yapılandırılması

- Sunucular, istemcilerin güvenilir bir şekilde bulabilmeleri için stabil bir IP'ye sahip olmalıdır.
- Bu IP, güvenlik duvarının arkasına korumalı bir segmentte bulunmalıdır.
- En az iki tane DNS sunucusunu hazırda tutun ve komut isteminden "nslookup" kullanarak ad çözümlemesini(name resolution) iki kere kontrol edin.
- Sunucunun DNS'de istediğiniz adla geçerli bir kaydı olduğuna ve reverse lookups için PTR kaydı (Pointer Record) olduğuna emin olun.
- DNS değişikliklerin internette yayılması birkaç saat sürebilir, bu yüzden değişiklikler, sistem canlıya çıkmadan daha önce yapılandırılmalıdır.
- Son olarak, sunucunun IPv6 gibi kullanılmayan tüm ağ hizmetlerini devre dışı bırakın.

Portların kontrolü,

Uzaktan erişimin sınırlandırılması

Wsus(Windows server update services)

RDP kullanılıyorsa, VPN üzerinden erişilebilir, powershell ssh kilitlenmelidir.

FTP içinde geçerli

1102 - The audit log was cleared.

Log Yönetimi

ÖNEMLİ OLAY KİMLİKLERİNDEN BAZILARI:	
Event ID – Açıklama	
4624 – Başarılı Login	
4625 – Başarısız Login	
4672 – Admin Hesabı Logini	
4634,4647 – Başarılı Logoff	
4771 – Etki alanında ön kimlik doğrulama başarısız oldu	
4768 – Kerberos Ticket istemi	
4776 – Etki alanında başarılı ya da başarısız login	
7034 – Servis beklenmedik bir şekilde çöktü	
7035 – Servis, başlatma veya durdurma komutu gönderdi	
7036 – Servis durdu veya başladı	
7040 – Servis başlangıç tipi değiştirildi (Başlangıçta, elle vs.)	
5140 – Ağ paylaşımı planlandı	
4778 – RDP oturum isteği	
4779 – RDP oturumu kapandı	
Event ID'ler hakkında daha detaylı bilgi edinmek için https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/ URL adresini ziyaret edebilirsiniz.	

Windows Server 2000/2003	
Event ID	Açıklama
528	Başarılı logon işlemi
529	Başarısız logon işlemi
538	Başarılı logoff işlemi
540	Network üzerinden başarılı logon işlemi

Windows Server 2008	
Event ID	Açıklama
4624	Başarılı logon işlemi
4625	Başarısız logon işlemi

Şüpheli

Event ID'leri incelerken birbirleriyle ilişkilendirmek oldukça önemlidir.

- Örneğin 4624 akabinde görülen 4634/4647 ID'leri tamamlanmış bir oturum fikri verebilir.
- Çok fazla 4625 ID'si görmek bir şifre tahmin saldırısının olduğuna işaret edebilir.

4624 : Başarılı Login
4634/4647 : Başarılı Logoff
4625 : Başarısız Login



Zamanlı Görev

ZAMANLANMIŞ GÖREVLER:

- 106 Görev zamanlandı
- 200 Görev başlatıldı
- 201 Görev tamamlandı
- 141 Görev silindi

Windows içerisinde "zamanlanmış görev" logları bilgisayarın ele geçirilip geçirilmediği hususunda fikir verebilir. Örnek vermek gerekirse bir servisin günün belli saatlerinde oturum açılması için görev zamanlaması gerçekleştirmesi şüpheli bir harekettir.



Windows Server 2008 Brute Force Saldırısı ve Log Kayıtları

ÖRNEK: "WINDOWS SERVER 2008 BRUTE FORCE SALDIRISI VE LOG KAYITLARI"

Yorumlama: Başlangıçta gelen 4625 Event ID ler bize başarılı bir şekilde oturum açamadığını göstermektedir. Çok kısa bir sürede bu kadar şifre denenmiş olması bir uygulama/program yasıtasıyla brute force (şifre saldırısı) yapıldığını yönelik bir fikir oluşturmaktadır.

Sonrasında gelen;

- 4776 Event ID numarası; DC'nin bir hesap için kimlik bilgilerini doğrulamayı denediğini,
- 4648 kimlik bilgileri kullanılarak bir oturum açma girişiminde bulunulduğunu,
- 4624 hesabın başarılı bir şekilde açıldığını,
- 4672 Admin Hesabı (Oturum açmaya ayrılan özel ayrıcalıklar)
- 4634 ise bir hesabın kapatıldığını bildiriyor.

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	23.05.2018 14:12:17	Microsoft Windows security auditing	4634	Logoff
Audit Success	23.05.2018 14:12:16	Microsoft Windows security auditing	4672	Special Logon
Audit Success	23.05.2018 14:12:16	Microsoft Windows security auditing	4624	Login
Audit Success	23.05.2018 14:12:16	Microsoft Windows security auditing	4648	Login
Audit Success	23.05.2018 14:12:15	Microsoft Windows security auditing	4776	Credential Validation
Audit Success	23.05.2018 14:12:15	Microsoft Windows security auditing	4672	Special Logon
Audit Success	23.05.2018 14:12:15	Microsoft Windows security auditing	4624	Login
Audit Success	23.05.2018 14:12:15	Microsoft Windows security auditing	4648	Login
Audit Success	23.05.2018 14:12:15	Microsoft Windows security auditing	4776	Credential Validation