PurpleBox

The Adventure of an Attacker: Digital Forensic

www.prplbx.com

Okan KURTULUŞ

PurpleBox Europe | Sr. Cyber Security Engineer

OSWE & OSCP & eMAPT & Sertifikalı TSE

okan_kurtuluss

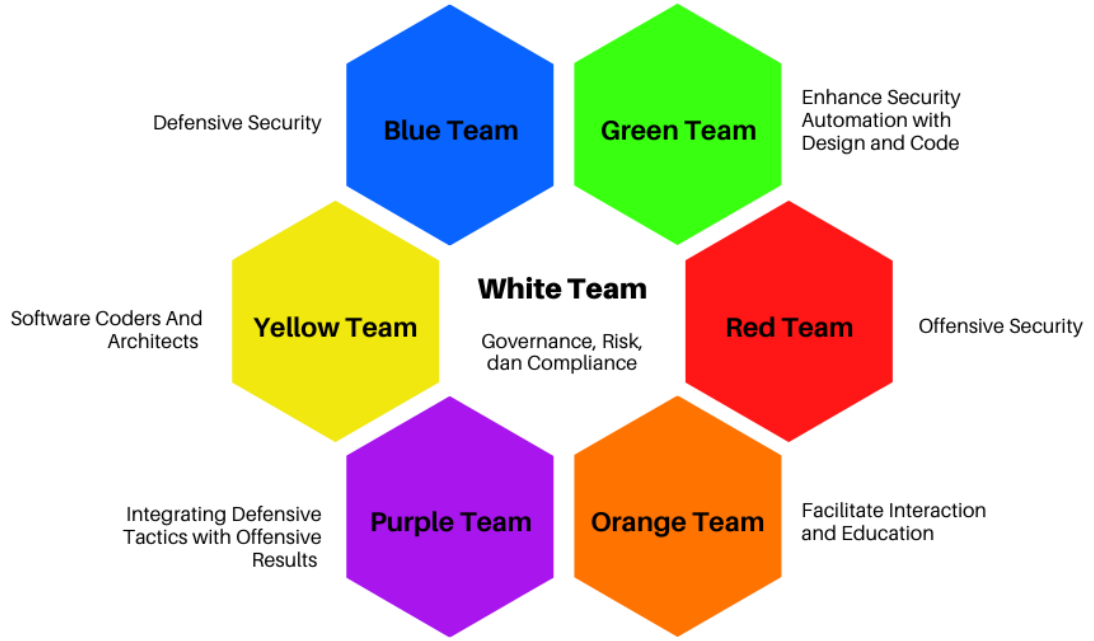
okankurtuluss

Digital Forensic Nedir?

- Bir saldırı sonucu bilgisayar kanıtlarının korunması, tanımlanması, çıkarılması ve belgelenmesi sürecidir.
- Digital Forensic başlangıçta Computer Forensic olarak kullanıldı fakat teknolojinin ilerlemesi ile bu kavram yerini daha genel olan Digital Forensic'e bıraktı.

Takımlar

- Kırmızı Takım
- Mor Takım
- Mavi Takım
- Sarı Takım
- Turuncu Takım
- Yeşil Takım
- Beyaz Takım



Sıkça Duyabileceğimiz Kavramlar

- Cyber Kill Chain
- Advanced Persistent Threats (APT)
- Dwelling Time
- Indicators of Compromise (IOC)
- Mitre ATT&CK Framework
- SIEM
- Log
- Security Operation Center (SOC)

Cyber Kill Chain

- Pasif Bilgi Toplama
- Kuruluş Şemaları
- IP Adresleri
- Port Taramaları
- İnternet Servis Sağlayıcısı Bilgileri
- Dışarıya Açık Sistemler

- İstismar Kodunun Hazırlanması
- Zararlı Yazılım

- Hedefli Oltalama Saldırısı
- Zararlı İçerikli Web Sayfası
- İnternet Servis Sağlayıcısı

- Kodun Çalıştırılması
- Hedef Sistemle Bağlantı Kurma
- Üçüncü Tarafların İstismarı

- Trojan veya Arka Kapı
- Kalıcı Erişim Kurabilme
- Yetki Yükseltme
- Kullanıcı Adlarını ve Parolalarını Çalma

- Hedefle İletişim Yolunun Açılması
- Yatay Hareket
- İç Ağda Bilgi Toplama
- Erişimi Kalıcı Hale Getirme

- Derinleşme
- Bağlantıyı ve Erişimi Kalıcı Hale Getirecek Ek Yöntemler
- Veri Sızdırma

Advanced Persistent Threat (APT)

- İleri bilgi ve düzeye sahip hackerlar tarafından oluşturulan gruplardır. Bu gruplar zeroday dediğimiz sömürü (exploit) kodları kullandıklarından, zararlı yazılımları karmaşıklaştırdıkları için ve en önemlisi finansal açıdan güçlü oldukları için tehlikelidir. Genel olarak devlet destekli olurlar.
- İncelemelerde saldırıların çoğunluğu DMZ'te bulunan web sunucular üzerinden ve sosyal mühendislik kullanılarak karmaşıklaştırılan zararlı yazılımların sistemlere bulaştırılması ile başlamaktadır.
- Şu zamana kadar tespit edilmiş APT gruplarının listesine ulaşmak isterseniz: https://www.fireeye.com/current-threats/apt-groups.html

Dwelling Time

- Dwelling Time saldırganların bir sisteme erişikleri zaman farkedilene kadar içeride kalma süreleridir.
- Mandiant’e göre bu süre ortalama 215 gündür.

Indicators of Compromise (IOC)

- Bir ağda veya bir cihazda gözlemlenen, sisteme yetkisiz erişim olasılığının yüksek olduğunu, bir başka deyişle sistemin güvenliğinin ihlal edildiğini gösteren bir nesne veya etkinliktir.
- Bu tür göstergeler, kötü niyetli faaliyetleri erken aşamalarında tespit etmek ve bilinen tehditleri önlemek için kullanılır.

Mitre ATT&CK Framework

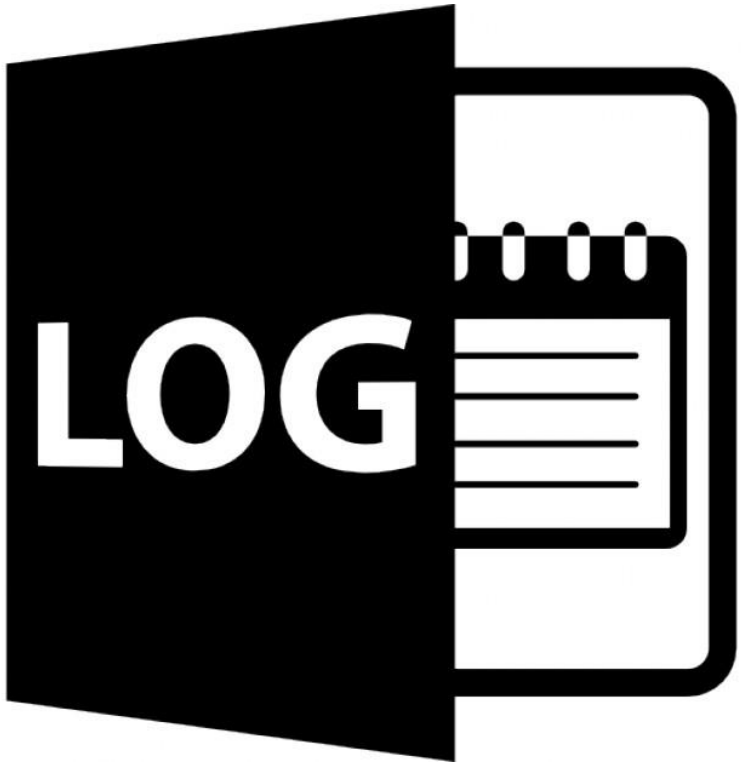
- Gerçek dünya gözlemlerine dayalı saldırganların taktikleri ve teknikleri hakkında küresel olarak erişilebilir bilgi tabanıdır.

Security Information & Event Management (SIEM)

- Bir kuruluşun uygulamaları, güvenlik cihazları ve bilgisayar sistemleri tarafından oluşturulan günlük(log) ve olay verilerinin tek bir çatı altında toplanması ve yönetilmesidir.
- Bu uygulamalara AlienVault OSSIM, Wazuh, OSSEC, Splunk, ELK örnekleri verilebilir.

Log

- Bilişim sistemlerinde gerçekleşen her bir olayın kayıt altına alınmasıdır.
- Logların düşük etkili sistemlerde 1-2 hafta, orta etkili sistemlerde 1-3 ay ve yüksek etkili sistemlerde ise 3-12 ay kadar kayıt altında tutulması sağlıklıdır.



Security Operation Center (SOC)

- Bir kuruluşu siber saldırılara karşı izlemek, analiz etmek ve korumaktan sorumlu ekiptir.

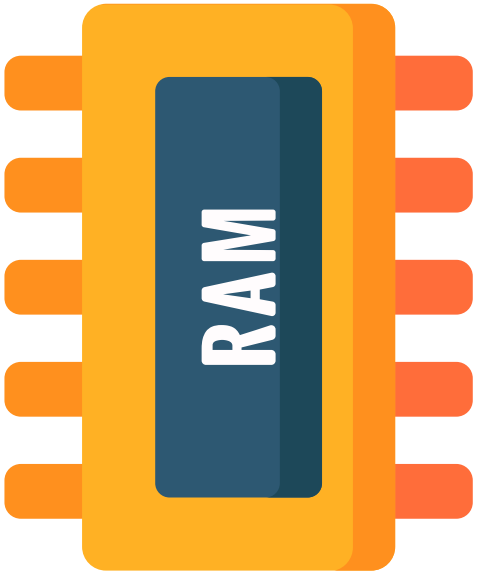
PurpleBox

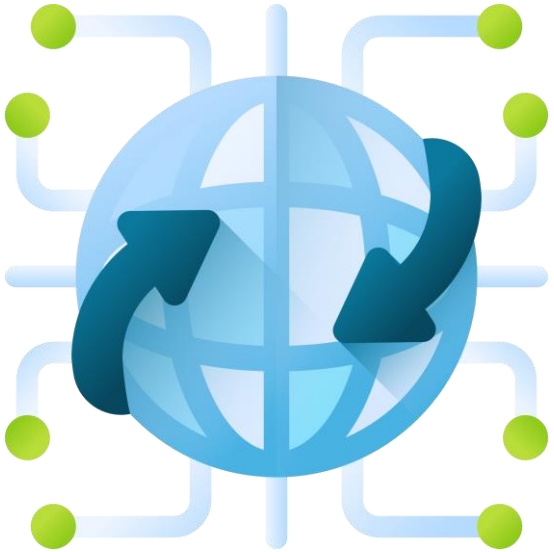
Windows Forensic 101

www.prplbx.com

Bize Neler Lazım?

- Log Kayıtları
- RAM Dökümü
- Ağ Trafik Kayıtları





Windows Logları

Windows logları üç başlık altında karşımıza çıkmaktadır:

- Uygulama Logları
- Sistem Logları
- Güvenlik Logları

Windows, her log için bir ID değeri tanımlamıştır. Örneğin:

Event ID 1102: Güvenlik loğlarının silindiğini belirtir.

Windows Logları

Interactive

- Klavye/Konsol

Network

- Ağ Üzerinden SMB vb.

Batch

- Zamanlanmış Görev

Service

- Servis/Uygulamaya Giriş

Unlock

- Normal Kullanıcı Girişi, Kilit Açma vb.

Network Cleartext

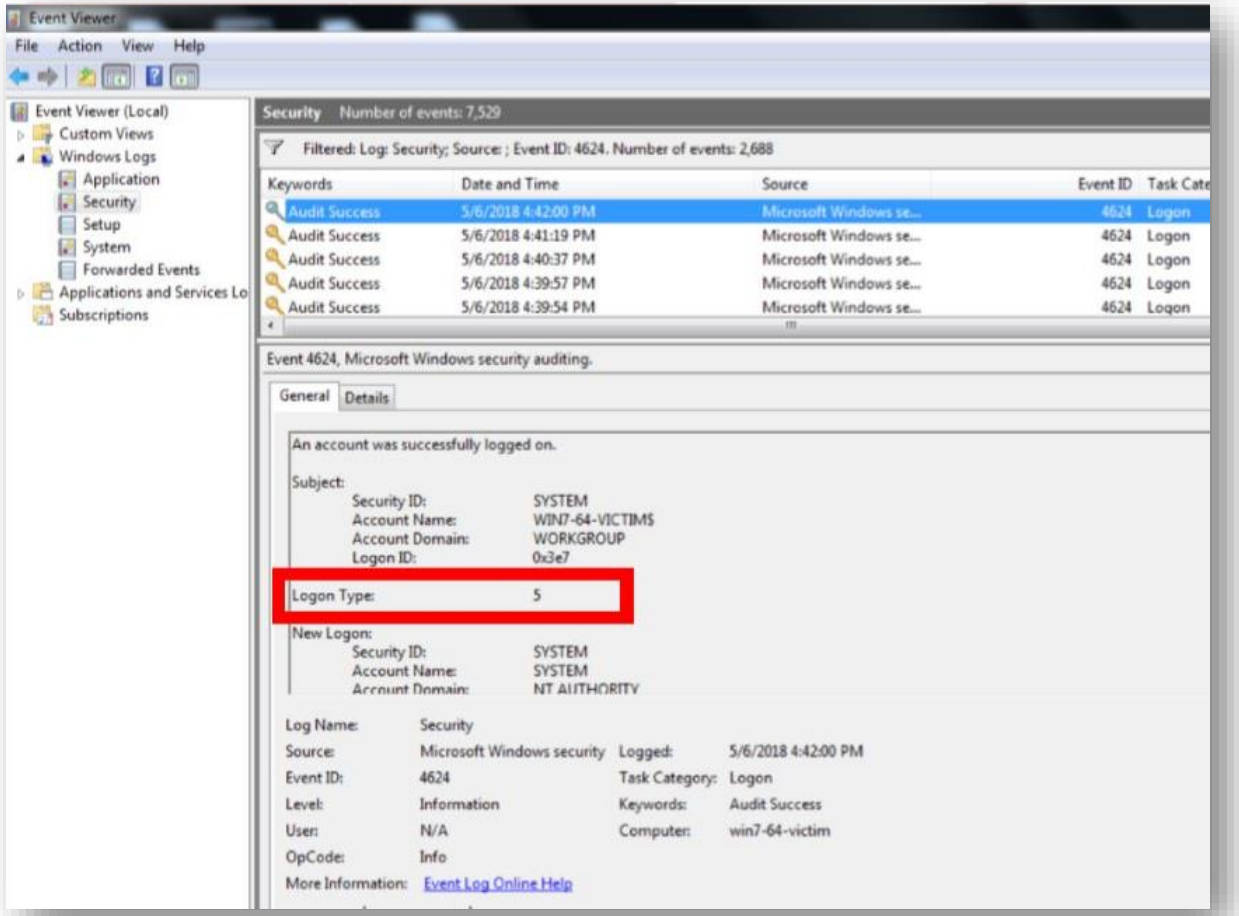
- Ağ üzerinden açık metin parola kullanılarak yapılan girişler

New Credentials

- Abc Kullanıcısı ile Çalıştır

Remote Interactive

- Remote, RDP etc.



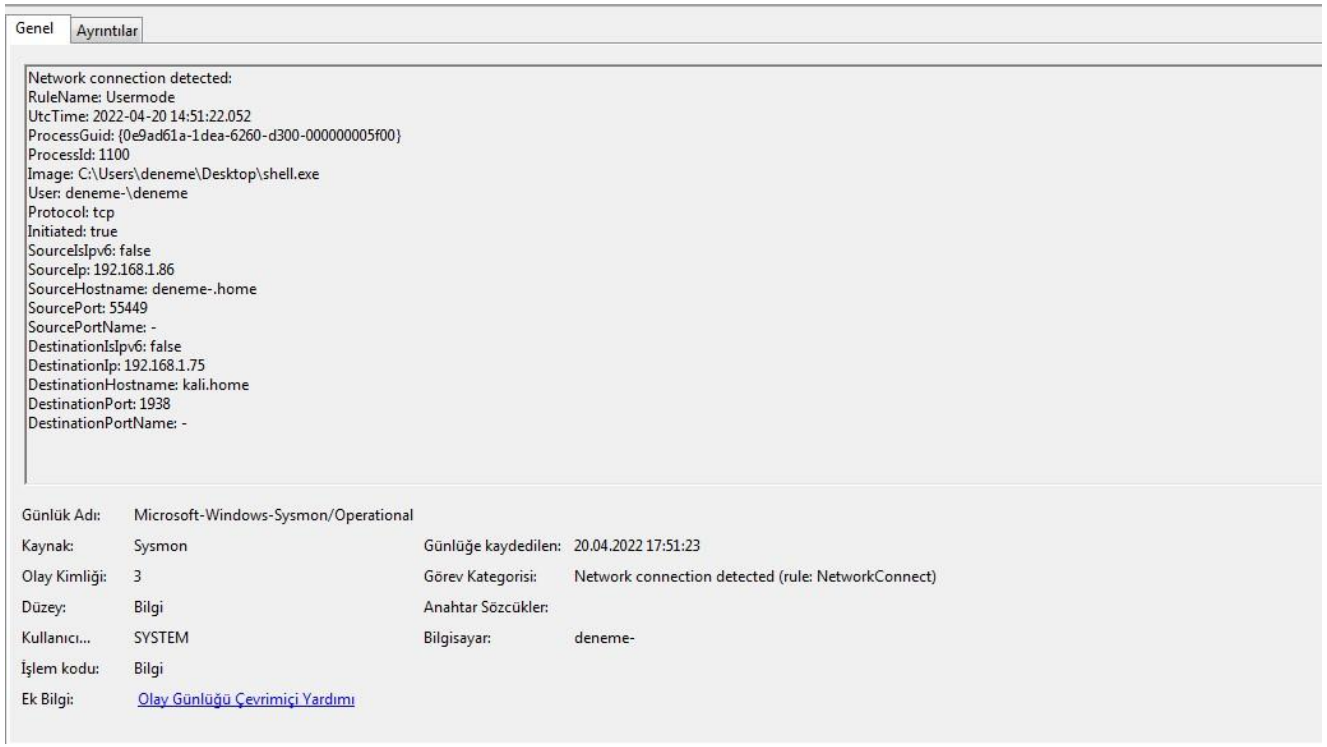
Önemli Windows Logları

- 4624 – Başarılı Oturum Açma
- 4625 – Başarısız Oturum Açma
- 4720 – Yeni Hesap Oluşturulma
- 4722 – Kullanıcı Hesabının Etkinleştirilmesi
- 4728 – Kullanıcı Grubuna Dahil Edilmesi (Örneğin Domain Admins)
- 4768 – Kerberos Kimlik Doğrulama Bileti (TGT) istendi
- 4769 – Kerberos Servis Bileti Talep Edildi
- 4770 – Kerberos Servis Bileti Yenilendi
- 1102 – Güvenlik Logları Silindi

Bilgisayarın kapatıldığını gösteren logu göremeyiz.
Sizce sebebi ne olabilir?

Sysmon Nedir?

Microsoft tarafından geliştirilen SysInternals ailesinin bir bireyidir. Bu araç ile sistemde oluşan hareketleri ve olayları kayıt altına alabiliriz. Bir Agent olarak düşünebiliriz. Anti virüslerden farkı, sistemi derinlemesine izlemesi ve yapılan her işlemi kayıt altına alması diyebiliriz.

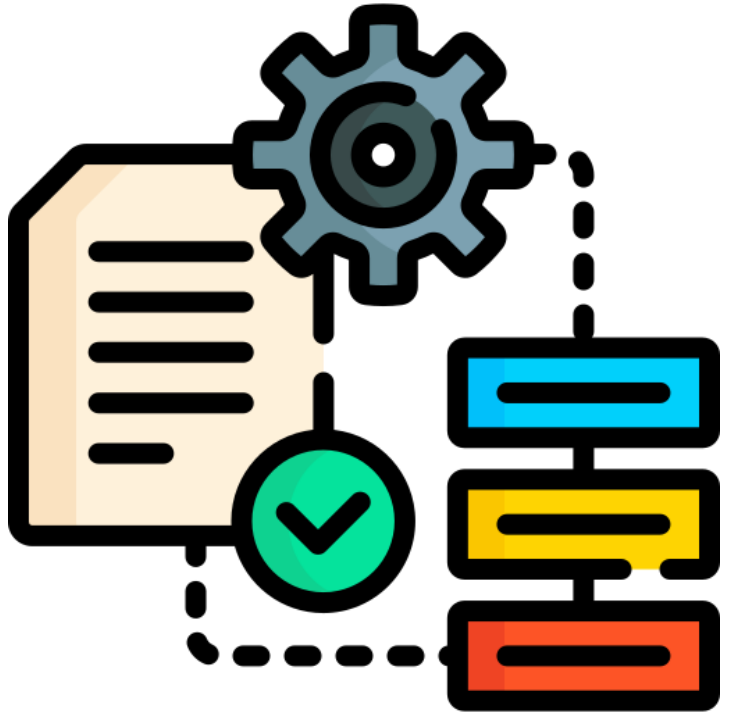


Windows İşlemler (Windows Process)

Arka planda çalışan küçük programlardır. Her program da kendi içinde işlem üretebilmektedir.

Windows üzerinde işlemlere örnek vermek gerekirse:

Lsass.exe, smss.exe, csrss.exe winlogon.exe vb. verilebilir.

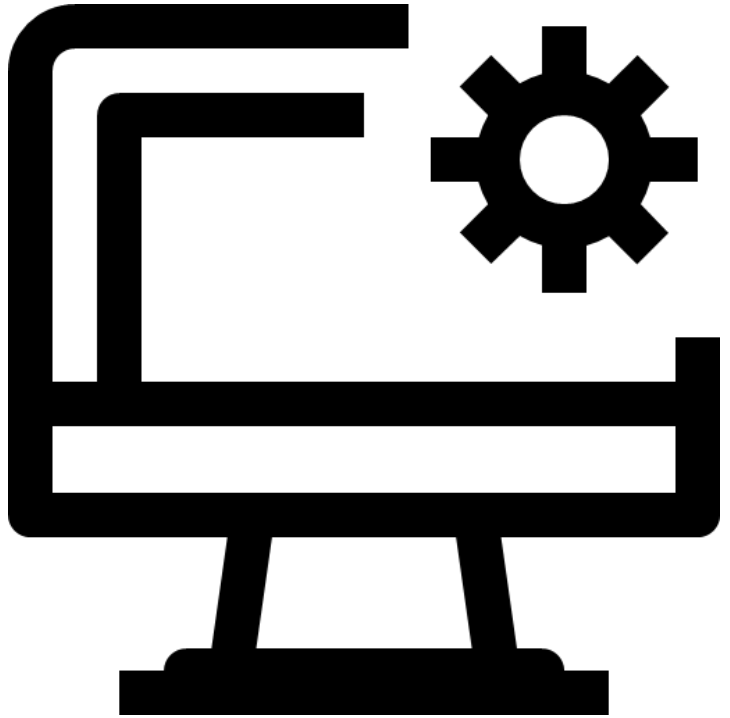


Windows İşlemler (Windows Process)

Smss.exe: Yeni oturumların oluşturulmasından sorumludur. İşlem listesinde bir tane gözükmektedir.

Csrss.exe: Windows API'ler ile iletişimi sağlar ve işlemlerin kapatılmasını sağlar. Parent işlemi ise smss.exe'dir. İşlem listesinde iki tane gözükmektedir.

Winlogon.exe: Kullanıcıların logon ve logoff işlemlerinden sorumludur. Parent işlemi smss.exe'dir. LogonUI.exe kullanıcı adı ve parolayı lsass.exe'ye gönderir. Lsass.exe ise AD ve lokal SAM dosyaları üzerinden kullanıcı doğrulaması yapar.

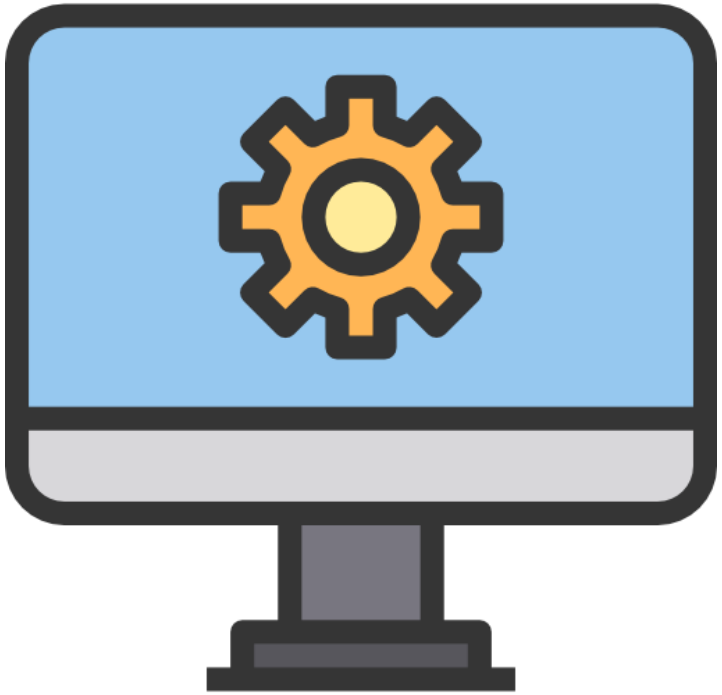


Windows İşlemler (Windows Process)

Winnit.exe: Services.exe, lsass.exe ve lsm.exe gibi işlemlerin başlatılmasından sorumludur. Parent işlemi smss.exe'dir. İşlem listesinde bir tane gözükmektedir.

Lsm.exe: Smss.exe ile beraber çalışmaktadır ve oturumların oluşturulması veya değiştirilmesinden sorumludur. Windows 7'den sonra lsm.dll olarak karşımıza çıkmaktadır. Parent işlemi wininit.exe'dir.

Services.exe: Servislerin ve sürücülerin (Device Driver) hafızaya yüklenmesini sağlar. Sisteme başarılı bir şekilde login olunduktan sonra HKLM/System/Select/LastKnow anahtarının yedeğini alır. Bu anahtar Lastknow Good olarak bilinen bilgisayar Recovery modunda açıldığında sistemin kusursuz çalıştığı zamanındaki haline getiren anahtardır.



Windows İşlemler (Windows Process)

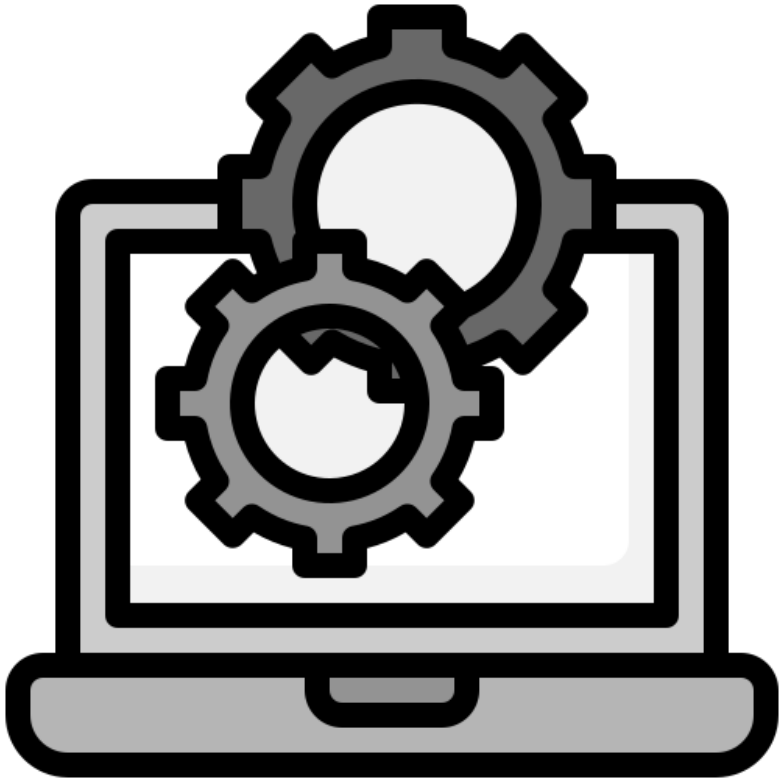
Lsass.exe: Token üretiminden, güvenlik ilkelerinin oluşturulmasından ve kullanıcı doğrulama işlemlerinden sorumludur. Parent işlemi Winnit.exe'dir. İşlem listesinde bir tane gözükmektedir.

Svchost.exe: DLL dosyaları üzerinden başlatılan işlemlerin yürütülmesini sağlar. DLL dosyaları çalıştırılabilir olmadığı için svchost.exe çağrılarak servisler ayağa kaldırılır. Tüm servisler serviceDLL register değerine sahiptirler. Bu register değerleri ile svchost.exe hangi DLL dosyalarını kullanacağını bilir. Parent işlemi services.exe'dir.

Taskhost.exe: Svchost.exe gibi DLL tabanlı servislerin çalıştırılması için kullanılır. Windows 8'de taskhostex.exe, Windows 10'da ise taskhostw.exe olarak karşımıza çıkar. Parent işlemi services.exe'dir.

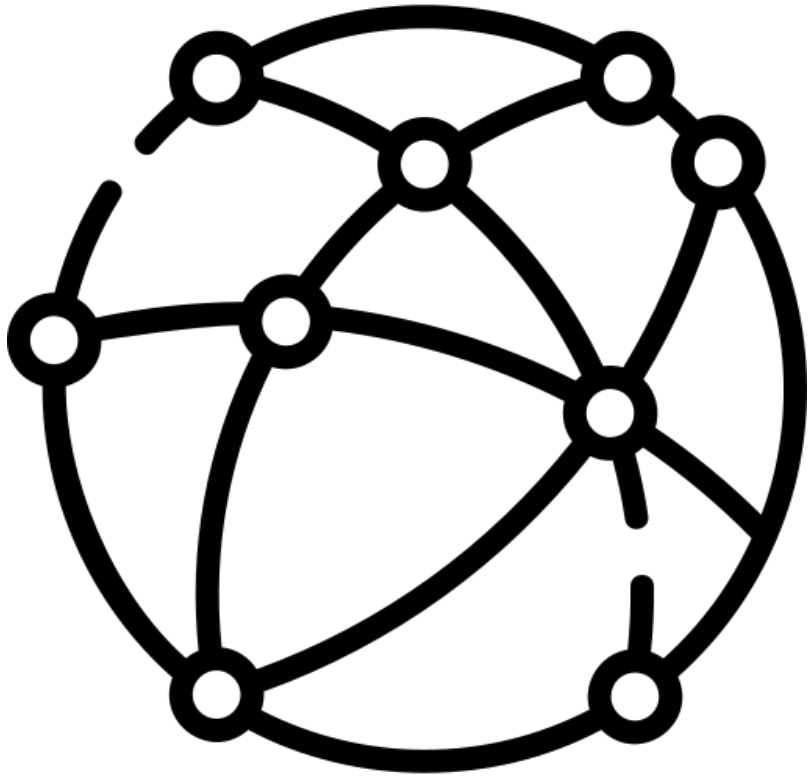
Windows İşlemler (Windows Process)

Explorer.exe: Masaüstü üzerindeki dosya erişimi, dosya ve dizinler arasında gezinme, dosyalara erişme gibi işlemlerden sorumludur. Her kullanıcı için bir tane çalışır.



Ağ Trafik Analizi Nasıl Yapılır?

- Ağ trafik analizi Wireshark veya alternatif araçlar ile gerçekleştirilebilir. Biz analizlerimizi Wireshark üzerinden gerçekleştireceğiz.
- Wireshark, ağ içerisinde gelen/giden paketleri yakalayan ve bunu bir interface üzerinden görüntülememizi sağlayan açık kaynak kodlu araçtır.
- CAP, PCAP veya PCAPNG gibi uzantıları kullanmaktadır.



Wireshark ile Filtreleme Yapmak

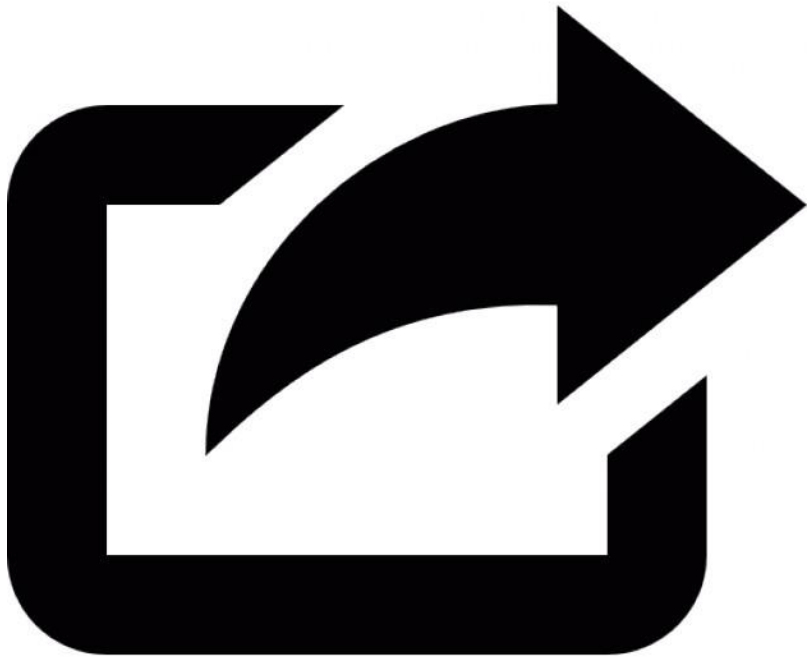
- ip.addr == 192.168.1.224
- ip.src == 10.43.54.65 or ip.dst == 10.43.54.65
- tcp.port == 443
- data.len > 63 and icmp
- tcp contains SSH-2.0

Daha fazlası için:

Wiki.wireshark.org

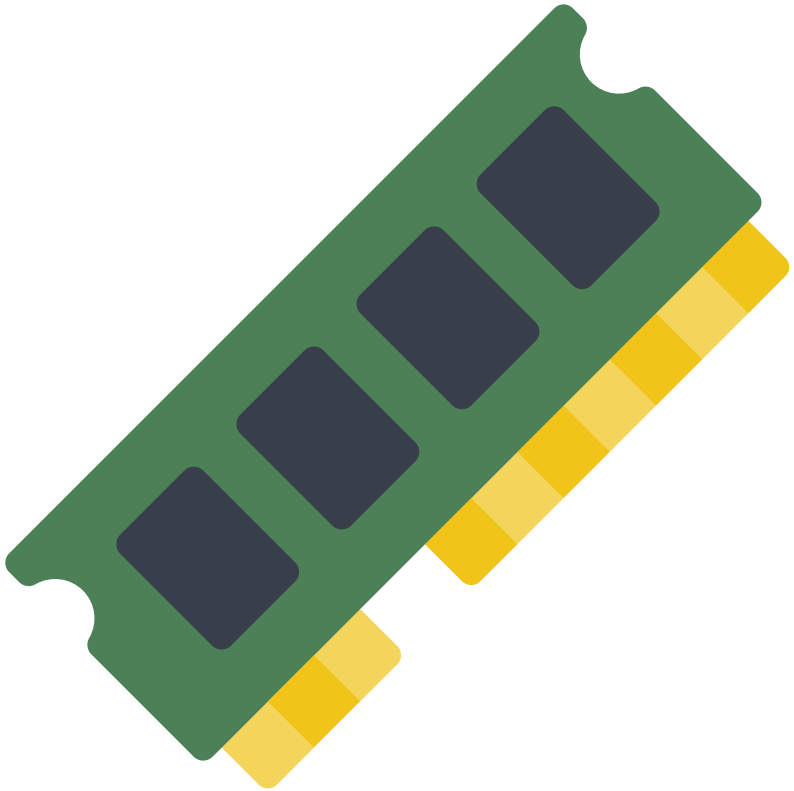
Ağ Trafiğinden Dosya Çıkarmak

- Bir ağ trafiğinden dosya çıkarmak istersek Wireshark veya Network Miner gibi araçlar kullanılabilir.



RAM İmajı Nasıl Alınır & Nasıl İncelenir?

- Windows sistemlerde RAM imajı RAP Capturer, Dumplt veya Memoryze gibi araçlarla alınabilir.
- İnceleme için Volatility (Vol) aracı kullanılabilir.



Peki Neler Arıyoruz?

- Yatay veya dikey hareket. Sağı solu kurcalayan bir sistem var mı?
- Dışarıyla konuşmaması gereken bir sunucu dışarıyla konuşuyor mu?
- Kullanılmaması gereken protokol veya process var mı?
- Sadece IP adresi ile yapılan bağlantlar. DNS cache kaydı yoksa hayatına alan adı olmadan başlamıştır. (Bağlantı sadece IP adresi olarak kurulmuştur)

Saldırgan Ne Yapmak Zorunda?

- Dosya yüklemek
- Süreç çalıştırmak
- Registry üzerinde değişiklik

Saldırganlar En Çok Hangi Komutları Çalıştırır?

Sıralama	Çalıştırılan Windows Komutu
1	tasklist
2	ver
3	ipconfig
4	systeminfo
5	net time
6	netstat
7	whoami
8	net start
9	qprocess
10	query

Demo

Thank you!
Any Questions?

PurpleBox

www.prplbx.com