

Enumeration

A. Enumeration Pen Testing

- **Step 1: Find the network range**

Whois Lookup gibi araçları kullanarak ağ aralığını bulun. Ağ aralığını bulmak, hedef ağdaki önemli sunucuları numaralandırmaya yardımcı olur.

- **Step 2: Calculate the subnet mask**

Alt Ağ Maskesi Hesap Makinesi gibi araçları kullanarak IP aralığı için gereken alt ağ maskesini hesaplayın. Hesaplanan alt ağ maskesi, ana bilgisayarları ve açık bağlantı noktalarını keşfetmeyi içeren daha fazla numaralandırma için ping tarama ve bağlantı noktası tarama araçlarının çoğuna bir giriş işlevi görebilir.

- **Step 3: Undergo host discovery**

Nmap gibi araçları kullanarak Internet'e bağlı önemli sunucuları bulun. Internet'e bağlı sunucuları bulmak için Nmap sözdizimini kullanın: nmap - sP. Ağ aralığı yerine, ilk adımda elde edilen ağ aralığı değerini girin.

- **Step 4: Perform port scanning**

Açık portları bulun ve gerekmediklerinde kapatın. Açık portlar, bir saldırganın hedefin güvenlik çevresine girmesi için giriş kapısıdır. Bu nedenle, düğümlerdeki açık bağlantı noktalarını kontrol etmek için bağlantı noktası tarama gerçekleştirin. Kalemler testçileri ve güvenlik denetçileri, bağlantı noktası taraması yapmak için Nmap gibi araçları kullanır.

- **Step 5: Perform NetBIOS enumeration**

TCP / IP üzerinden ağ aygıtlarını tanımlamak ve bir etki alanına ait bilgisayarların listesini, tek tek ana bilgisayarlardaki paylaşımının listesini ve ilkeleri ve parolaları almak için NetBIOS numaralandırması gerçekleştirin. Hyena, Nsauditor Network Security Auditor ve NetScanTools Pro gibi araçlar NetBIOS numaralandırmasını gerçekleştirebilir.

- **Step 6: Perform SNMP enumeration**

Ağdaki SNMP sunucusunu sorgulayarak SNMP numaralandırması gerçekleştirin. SNMP sunucusu kullanıcı hesapları ve aygıtları hakkında bilgi verebilir. OpUtils Ağ İzleme Araç Seti ve Mühendisin Araç Seti gibi araçlar SNMP numaralandırması gerçekleştirebilir.

- **Step 7: Perform LDAP enumeration**

LDAP hizmetini sorgulayarak LDAP numaralandırması gerçekleştirin. LDAP hizmetinin numaralandırılması geçerli kullanıcı adları, departman ayrıntıları ve adres bilgileri sağlar. Saldırgan bu bilgileri sosyal mühendislik ve diğer saldırı türlerini gerçekleştirmek için kullanabilir. SoftTerra LDAP Yöneticisi gibi araçlar LDAP numaralandırması gerçekleştirebilir.

- **Step 8: Perform NTP enumeration**

NTP sunucusuna bağlı ana bilgisayar, istemci IP adresi, istemci sistemlerinde çalışan işletim sistemi vb. Bilgileri ayıklamak için NTP numaralandırması gerçekleştirin. Ntptrace, ntpdc ve ntpq gibi komutlar bu bilgiyi alabilir.

- **Step 9: Perform SMTP enumeration**

SMTP sunucusundaki geçerli kullanıcıları belirlemek için SMTP numaralandırması gerçekleştirir. NetScanTools Pro gibi araçlar bu bilgi için SMTP sunucusunu sorgulayabilir.

- **Step 10: Perform DNS enumeration**

Tüm DNS sunucularını ve kayıtlarını bulmak için DNS numaralandırması gerçekleştirir. DNS sunucuları sistem adları, kullanıcı adları, IP adresleri vb. Bilgiler sağlar. Windows nslookup yardımcı programı bu bilgileri ayıplayabilir.

- **Step 10: Perform IPsec, VoIP, VPN and Linux enumeration**

Şifreleme ve karma algoritma, kimlik doğrulama türü, anahtar dağıtım algoritması, SA LifeDuration, vb. Hakkında bilgi ayıqlamak için IPsec numaralandırma işlemini gerçekleştirir. İke-scan ve Nmap gibi araçlar bu bilgileri ayıplayabilir. VoIP ağ geçidi / sunucuları, IP-PBX sistemleri, istemci yazılımı (yazılım telefonları) / VoIP telefonları Kullanıcı aracı IP adresleri ve kullanıcı uzantıları vb. Hakkında bilgi almak için VoIP numaralandırması gerçekleştirir. Bu bilgileri toplamak için Svmap ve Metasploit gibi bir araç kullanın. RPC hizmet bağlantı noktalarındaki savunmasız hizmetleri tanımlamak için RPC numaralandırması gerçekleştirir. Bu bilgileri çıkarmak için Nmap ve NetScan Tools Pro gibi araçlar kullanın. Sistem kullanıcıları hakkında bilgi almak için Unix / Linux kullanıcı numaralandırması gerçekleştirir. Peksen, rwho ve parmak gibi komutlar bu bilgiyi alabilir.

- **Step 11: Document all the findings**

Son adım sayım kalemi testi sırasında elde edilen tüm bulguları belgelemektir. Sonuçları analiz edin ve müşterinin güvenliğini artırmak için karşı önlemler önerin.

B. NetBIOS Enumeration

1. **Nbtstat** : TCP / IP üzerinden NetBIOS (NetBT) protokol istatistiklerini, hem yerel hem de uzak bilgisayarlar için NetBIOS ad tablolarını ve NetBIOS ad önbelleğini görüntüler

Nbtstat Syntax: nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]

C. Enumerating User Accounts

PsExec, istemci yazılımlarını manuel olarak yüklemeye gerek kalmadan konsol uygulamaları için tam etkileşim ile tamamlanan, diğer sistemlerde işlemleri gerçekleştirilebilen hafif bir telnet deşifirmidir. PsExec'in en gücü kullanımı, uzak sistemlerde etkileşimi komut istemleri ve başka türlü uzak sistemler hakkında bilgi gösterme yeteneği olmayan Ipconfig gibi uzaktan etkinleştirme araçlarını başlatmaktadır.

Syntax: psexec [\computer[,computer2[,...] | @file]] [-u user] [-p psswd] [-n s] [-r servicename] [-h] [-l] [-s|-e] [-x] [-I [session]] [-c [-f|-v]] [-w directory] [-d] [-<priority>] [-a n,n,...] cmd [arguments]

- PsFile

PsFile, uzaktan açılan bir sistemdeki dosyaların listesini gösteren bir komut satırı yardımcı programıdır ve açılan dosyaları ada veya dosya tanımlayıcısına göre kapatabilir. PsFile'in varsayılan davranışı, uzak sistemler tarafından açılan yerel sistemdeki dosyaları listelemektir. Bir komutun ardından ":" yazılması, komutun sözdizimiyle ilgili bilgileri görüntüler.

Syntax: psfile [\RemoteComputer [-u Username [-p Password]]] [[Id | Path] [-c]]

- PsGetSid

PsGetSid, SID'leri görünen adlarına veya tam tersine çevirir. Yerleşik hesaplar, etki alanı hesapları ve yerel hesaplar üzerinde çalışır. Ayrıca kullanıcı hesaplarının SID'lerini görüntüler ve bir SID'yi onu temsil eden ada çevirir. SID'leri uzaktan sorgulamak için ağ üzerinde çalışır.

Syntax: psgetsid [\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]

- PsKill

PsKill, uzak sistemlerde işlemleri öldürebilen ve yerel bilgisayardaki işlemleri sonlandıracan bir kill yardımcı programıdır. PsKill'i bir işlem kimliğiyle çalıştırırmak, o kimliğin işlemi yerel bilgisayarda öldürmeyeleştirir. Bir işlem adı belirtirse, PsKill bu adı sahip tüm işlemleri öldürür. Uzak bir işlemi sonlandırmak için PsKill'i kullanmak için hedef bilgisayara bir istemci yüklemenize gerek yoktur.

Syntax: pkill [-] [-t] [\computer [-u username] [-p password]] <process name | process id>

- PsInfo

PsInfo, yükleme türü, çekirdek oluşturma, kayıtlı kuruluşu ve sahip, işlemci sayısı ve türleri, fiziksel bellek miktarı, yükleme de dahil olmak üzere yerel veya uzak eski Windows NT / 2000 sistemleri hakkında önemli bilgileri toplayan bir komut satırı aracıdır. ve bir deneme sürümü ise son kullanma tarihidir. Varsayılan olarak, PsInfo yerel sistem için bilgileri gösterir. Uzak sisteminde bilgi almak için bir uzak bilgisayar adı belirtin.

Syntax: psinfo [[\computer[,computer[,...] | @file] [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]

- PsList

PsList, işlem CPU ve bellek bilgileri veya iş parçacığı istatistikleri hakkında bilgi görüntüleyen bir komut satırı aracıdır. Kaynak killlerindeki (pstat ve pmon) araçlar farklı veri türlerini gösterir, ancak yalnızca araçların çalıştığı sistemdeki işlemlerle ilgili bilgileri görüntüler.

- PsLoggedOn

PsLoggedOn, hem yerel olarak oturum açan kullanıcıları hem de yerel bilgisayar veya uzak bilgisayar için kaynaklar aracılığıyla oturum açan kullanıcıları görüntüleyen bir uygulamadır. Bilgisayar yerine bir kullanıcı adı belirttiğinde, PsLoggedOn ağ mahallesindeki bilgisayarlarda arama yapar ve kullanıcının oturum açmış olup olmadığını gösterir. PsLoggedOn'un yerel olarak oturum açmış bir kullanıcı tanımı, Kayıt Defterine yüklenmiş bir profili olan bir tanımdır, bu nedenle PsLoggedOn, HKEY_USERS anahtarının altındaki anahtarları tarayarak kimin oturum açtığını belirler. Adı veya kullanıcı SID'si (güvenlik Tanımlayıcısı) olan her anahtar için PsLoggedOn karşılık gelen kullanıcı adını arar ve görüntüler. Bir bilgisayarda kaynak paylaşımıları aracılığıyla kimlerin oturum açtığını belirlemek için PsLoggedOn, NetSessionEnum API'sini kullanır.

Syntax: psloggedon [-] [-1] [-x] [\computername | username]

- PsLogList

Elogdump yardımcı programı, Olay Günlüğünün içeriğini yerel veya uzak bir bilgisayara döker. PsLogList, kullanıcının güvenlik kimlik bilgilerinin Olay Günlüğüne erişime izin vermediği durumlarda uzak sistemlerde oturum açılabilmesi dışında, PsLogList'in olay günlüğünün bulunduğu bilgisayardan mesaj dizeleri alması dışında bir elogdump klonudur. PsLogList'in varsayılan davranışı, Olay Günlüğü kayıtlarının görsel olarak biçimlendirilmesiyle birlikte yerel bilgisayarda Sistem Olay Günlüğü içeriğini görüntülemektir.

```
Syntax: psloglist [- ] [\computer[,computer[,...]] | @file [-u username [-p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w] [-c][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...]] | -e ID[,ID[,...]]] [-o event source[,event source][,...]] [-q event source[,event source][,...]] [-l event log file] <eventlog>
```

- PsPasswd

PsPasswd, yerel veya uzak sistemlerde bir hesap parolasını değiştirerek yöneticilerin, yönetici parolasında toplu bir değişiklik yapmak için yönetikleri bilgisayarlara karşı PsPasswd çalıştırın toplu dosyalar oluşturmalarına olanak tanır. PsPasswd, Windows parola sıfırlama API'larını kullanır, bu nedenle ağ üzerinden paroları net olarak göndermez.

```
Syntax: pspasswd [[\computer[,computer[,...]] | @file [-u user [-p psswd]]] Username [NewPassword]
```

- PsShutdown

PsShutdown yerel veya uzak bilgisayıri kapatabilir veya yeniden başlatabilir. İstemci yazılımının elle yüklenmesini gerektirmez.

```
Syntax: psshutdown [[\computer[,computer[,...]] | @file [-u user [-p psswd]]] -s|-x|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]
```

Enumerating Shared Resources Using Net View

Net View, bilgisayar veya ağ kaynaklarının listesini görüntüleyen bir komut satırı yardımcı programıdır. Belirtilen çalışma grubundaki bilgisayarların veya belirtilen bilgisayarda bulunan paylaşılan kaynakların bir listesini görüntüler.

Usage: net view \\<computername> Or net view /workgroup:

- Burada x, kaynaklarını görüntülemek istediğiniz belirli bir bilgisayarın adıdır
- y, paylaşılan kaynaklarını görüntülemek istediğiniz çalışma grubunun adıdır

Enumerating Shared Resources Using Net View

Net View, bilgisayar veya ağ kaynaklarının listesini görüntüleyen bir komut satırı yardımcı programıdır. Belirtilen çalışma grubundaki bilgisayarların veya belirtilen bilgisayarda bulunan paylaşılan kaynakların bir listesini görüntüler.

Usage: net view \\<computername> Or net view /workgroup:

- Burada x, kaynaklarını görüntülemek istediğiniz belirli bir bilgisayarın adıdır
- y, paylaşılan kaynaklarını görüntülemek istediğiniz çalışma grubunun adıdır

D. NTP Enumeration

NTP Enumeration Commands

NTP numaralandırma komutları, NTP sunucusunu değerli bilgiler için sorgulamak üzere ntpdate, ntptrace, ntpdc ve ntpq'yi içerir.

- ntpdate
 - Bu komut, bir dizi zaman kaynağından zaman örneği sayısını toplar.

```
Syntax: ntpdate [-bBdoqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [servername/IP_address]
```

- ntptrace
 - Bu komut, NTP sunucusunun nereden zaman alacağını belirler ve NTP sunucuları zincirini ana zaman kaynağına kadar takip eder.

```
Syntax: ntptrace [-vdn] [-r retries] [-t timeout] [servername/IP_address]
```

- ntpdc

- Bu komut, ntpd arka plan programını geçerli durumu hakkında sorular ve bu durumda değişiklik ister.

Syntax: `ntpdc [-ilnps] [-c command] [hostname/IP_address]`

- **ntpq**

- Bu komut NTP arka plan programı ntpd işlemlerini izler ve performansı belirler.

Syntax: `ntpq [-inp] [-c command] [host/IP_address]`

E. Other Enumeration

IPsec Enumeration

IPsec, ağ geçidinden ağ geçidine (LAN'dan LAN'a) ve ana makineden ağ geçidine (uzaktan erişim) kurumsal VPN çözümleri için en yaygın olarak uygulanan teknolojidir. IPsec, VPN üç noktaları arasındaki iletişimini sağlamak için ESP (Kapsülleme Güvenliği Yükü), AH (Kimlik Doğrulama Başlığı) ve IKE (Internet Anahtar Değişimi) gibi çeşitli bileşenleri kullanarak veri güvenliği sağlar. Çoğu IPsec tabanlı VPN, bir VPN ortamında Güvenlik İlişkileri (SA) ve şifreleme anahtarları oluşturmak, müzakereler etmek, değiştirmek ve silmek için IKE'nin bir parçası olan ISAKMP'yi (Internet Güvenlik Birliği Anahtar Yönetim Protokolü) kullanır.

Saldirgın, bir VPN ağ geçidinin varlığı ile ilgili bilgileri edinmek için Nmap vb. Araçlarla UDP bağlantı noktası 500'de ISAKMP için basit bir doğrudan tarama yapabilir. 500 numaralı bağlantı noktasıından isakmp durumunu kontrol etmek üzere Nmap taraması gerçekleştirmek için aşağıdaki komutu girebilirisiniz:

nmap -sU -p 500 <target-IP>

Saldirgınlar, şifreleme ve karma algoritma, kimlik doğrulama türü, anahtar dağıtım algoritması, SA LifeDuration vb. Gibi hassas bilgileri numaralandırmak için ike-tarama gibi parmak izi araçlarını kullanarak daha fazla araştırma yapabilirler. Bu tür taramada, ISAKMP başlığına sahip özel hazırlanmış IKE paketleri gönderilir hedef ağ geçidine ve yanıtlar kaydedilir. Benzer tarama aracıyla ilk IPsec VPN keşfi aşağıda ele alınmıştır:

ike-scan -M <target-gateway-IP>

RPC Enumeration

```
# nmap -sR <target IP/network>
# nmap -T4 -A <target IP/network>
```

Ayrıca, hedef ağın RPC bilgilerini yakalamak için NetScanTools Pro gibi araçları da kullanabilirsiniz

Unix/Linux User Enumeration

Bir numaralandırma yürütme için önemli admınlardan biri Unix / Linux kullanıcı numaralandırması yapmaktadır. Unix / Linux kullanıcı numaralandırması, kullanıcı adı, ana bilgisayar adı, her oturumun başlangıç tarihi ve saatı gibi ayıntılarla birlikte kullanıcıların listesini sağlar. UNIX / Linux kullanıcı numaralandırmasını gerçekleştirmek için aşağıdaki komut satır yardımcı programlarını kullanabilirsiniz:

- **rusers**

rusers, uzak makinelerde veya yerel ağdaki makinelerde oturum açan kullanıcıların bir listesini görüntüler. Kime benzer çıktılar görüntüler, ancak yerel ağdaki ana bilgisayarlar / sistemler için.

Syntax: `/usr/bin/rusers [-a] [-l] [-u] [-h] [-i] [Host ...]`

Where,

- **-a:** Gives a report for a machine even if no users are logged in
- **-h:** Sorts alphabetically by host name
- **-l:** Gives a longer listing similar to the who command
- **-u:** Sorts by number of users
- **-i:** Sorts by idle time

- **rwho**

rwho, yerel ağdaki ana bilgisayarlarında oturum açan kullanıcıların bir listesini görüntüler. Rwho arka plan programını çalıştıran yerel ağdaki tüm makineler için her oturumun kullanıcı adı, ana bilgisayar adı ve başlangıç tarihi ve saatı hakkında bilgi içeren kime benzer çıktılar üretir.

Sözdizimi: `rwho [-a]`

-a: Tüm kullanıcıları içerir. Bu bayrak olmadan, oturumları bir saat veya daha uzun süre kullanılmayan kullanıcılar rapora dahil edilmez.

Cracking Passwords

Active Online Attack: LLMNR/NBT-NS Poisoning

LLMNR (Bağlı Yerel Çok Noktaya Yayın Adı Çözümlemesi) ve NBT-NS (NetBIOS Ad Hizmeti), aynı bağlantıda bulunan ana bilgisayarlar için ad çözümlemesi gerçekleştirmek için kullanılan Windows işletim sistemlerinin iki ana öğesidir. Bu hizmetler Windows işletim sistemlerinde varsayılan olarak etkindir. DNS sunucusu ad sorgularını çözme girişiminde başarısız olursa, ana bilgisayar kimliği doğrulanmamış bir UDP yayını gerçekleştirerek tüm ana bilgisayarlara aradığı bir adı olup olmadığını sorar. Bağlanmaya çalışan ana bilgisayarın kimliği doğrulanmamış ve yayın işlemini izlemesi nedeniyle, saldırganın LLMNR (UDP bağlantı noktası 5355) ve NBT-NS (UDP bağlantı noktası 137) yayınılarını pasif olarak dinlemesi ve yanıt vermesi kolaylaşır hedef ana bilgisayar gibi davranışarak Bir ana bilgisayarla bağlantıyı kabul ettikten sonra, saldırgan bir kimlik doğrulama işlemi gerçekleştirmek için isteği sahte bir sunucuya (örneğin TCP: 137) yönlendirmek için Responder.py veya Metasploit gibi araçları kullanabilir. Kimlik doğrulama işlemi sırasında saldırgan, kendini doğrulamaya çalışan ana bilgisayardan alınan sahte sunucuya bir NTLMv2 karmaşı gönderir. Bu karma bir diskte saklanır ve hashcat veya John the ripper gibi çevrimdişi karma kırma araçları kullanılarak kırılabilir. Bir kez kırıldığında, bu kimlik bilgileri meşru ana bilgisayar sisteme erişmek için oturum açmak için kullanılabilir.

Steps involved in LLMNR/NBT-NS poisoning:

1. Kullanıcı, \\ DtaServr olarak yanlışlıkla yazdığı veri paylaşım sistemine bağlanmak için bir istek gönderir.
2. \\ DataServer, kullanıcıya \\ DtaServr adlı ana bilgisayarı bilmediğini söyleyerek yanıt verir.
3. Kullanıcı daha sonra ağıdaki herhangi birinin ana bilgisayar adını bilip bilmediğini öğrenmek için LLMNR / NBT-NS yayını gerçekleştirir \\ DtaServr.
4. Saldırgan kullanıcıya \\ DataServer olduğunu söyleyerek yanıt verir ve kullanıcı NTLMv2 karmaşasını kabul eder ve kullanıcıya bir hataya yanıt verir.

LLMNR/NBT-NS Poisoning Tools

- Responder

Bir LLMNR, NBT-NS ve MDNS zehirleyicisini yanıtlayın. Belirli NBT-NS (NetBIOS Ad Hizmeti) sorgularına ad soneklerine göre yanıt verir. Varsayılan olarak, araç yalnızca SMB için olan Dosya Sunucusu Hizmeti isteğine yanıt verir.

Features:

- Built-in SMB Auth server, MSSQL Auth server, HTTP and HTTPS Auth server, HTTPS Auth server, LDAP Auth server
- Built-in FTP, POP3, IMAP, SMTP Auth servers
- ICMP Redirect
- Rogue DHCP

Some of the LLMNR/NBT-NS spoofing tools are listed below:

- Metasploit

System Hacking

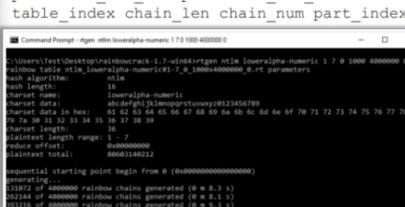
Cracking Passwords

Tools to Create Rainbow Tables: rtgen and Winrtgen

rtgen

- The rtgen program needs **several parameters** to generate a rainbow table. Syntax for the command line is:

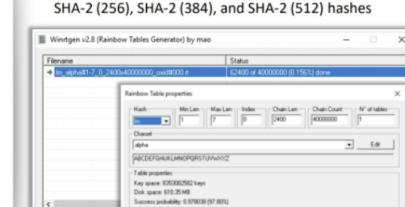
```
Syntax: rtgen hash_algorithm charset
plaintext_len_min plaintext_len_max
table_index chain_len chain_num part_index
```



<http://project-rainbowcrack.com>

Winrtgen

- Winrtgen is a graphical **rainbow table generator** that supports LM, FastLM, NTLM, LMCHELL, HalfLMCHALL, NTLMCHELL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384), and SHA-2 (512) hashes



<http://www.oxid.it>

System Hacking

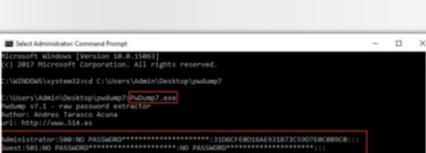
Cracking Passwords

Tools to Extract the Password Hashes

C|EH Certified Ethical Hacker

pwdump7

- pwdump7 extracts LM and NTLM password hashes of local user accounts from the **Security Account Manager** (SAM) database

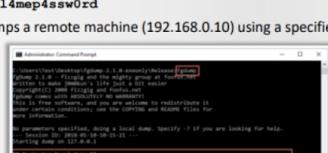


fgdump

- fgdump works like pwdump but also extracts **cached credentials** and allows **remote network execution**

```
fgdump.exe -h 192.168.0.10 -u AnAdministrativeUser -p 14mep4ssw0rd
```

Dumps a remote machine (192.168.0.10) using a specified user



Note: These tools must be run with administrator privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Password Cracking Cheat Sheet : <https://book.hacktricks.xyz/brute-force>

Steganography

Mysecret.txt dosyasını, stego dosyası stego.jpg oluşturarak kapak resmimize (cover.jpg) gömmek için şu komutu verin:

```
steghide embed -pf mysecret.txt -cf cover.jpg -sf stego.jpg
```

Sırrımızı çıkarmak için şu komutu kullanıyoruz:

steghide extract -sf stego.jpg

<https://pequalsnp-team.github.io/cheatsheet/steganography-101>

<https://0xrick.github.io/lists/stego/>

<https://zweilosec.gitbook.io/hackers-rest/os-agnostic/steganography>

Covering Tracks

A. Clearing Logs

Clear_Event_Viewer_Logs.bat, hedef sistemin günlüklerini silmek için kullanılabilen bir yardımcı programdır.

- **Steps to clear logs using Clear_Event_Viewer_Logs.bat utility**
 1. Download the **Clear_Event_Viewer_Logs.bat** utility from the <https://www.tenforums.com>
 2. Unblock the .bat file
 3. Right click or press and hold on the .bat file, and click/tap on **Run as administrator**.
 4. If prompted by **UAC**, click/tap on **Yes**.
 5. A command prompt will now open to clear the event logs. The command prompt will automatically close when finished.
- **Steps to clear logs using clearlogs.exe utility**
 1. Download the **clearlogs.exe** utiliy from <http://www.ntsecurity.nu>
 2. Run clearlogs.exe from the command prompt, and clear the security, system, and application logs using the following options
 - **C:\clearlogs.exe -app**(for clearing application logs)
 - **C:\clearlogs.exe -sec**(for clearing application logs)
 - **C:\clearlogs.exe -sys**(for clearing application logs)
- **Steps to clear logs using meterpreter shell**

If the system is exploited with the Metasploit, the attacker uses a **meterpreter shell** to wipe out all the logs from a Windows system:

 1. Launch **meterpretershell prompt** of the Metasploit Framework.
 2. Type **clearrev** command in meterpreter shell prompt and press **Enter**. The logs of the target system will start being wiped out.

Manually Clearing Event Logs

For Windows

- Navigate to Start → Control Panel → System and Security → Administrative Tools → double click Event Viewer
 - Delete the all the log entries logged while compromising of the system

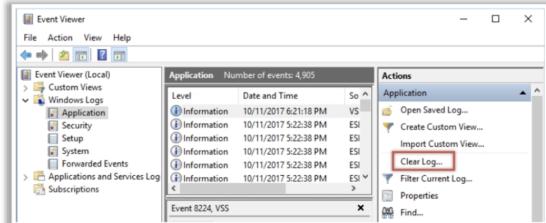


FIGURE 6.8: Clearing Event logs for Windows

For Linux

- Navigates to `/var/log` directory on the Linux system
 - Open plain text file containing log messages with text editor `/var/log/messages`
 - Delete the all the log entries logged while compromising of the system

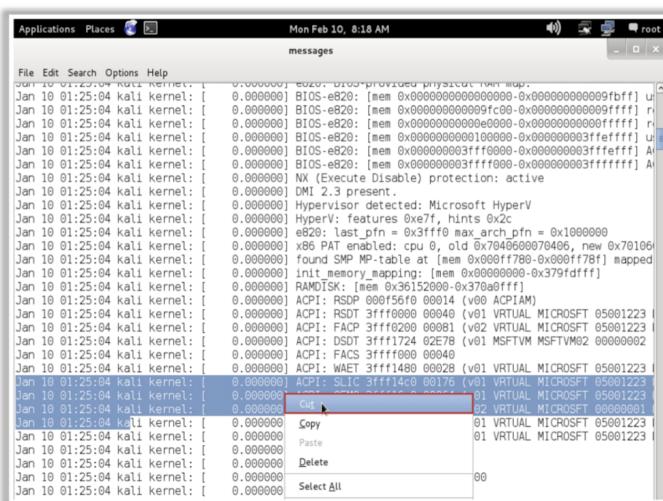


FIGURE 6.9: Clearing Event logs for Linux

Covering BASH Shell Tracks

BASH veya Bourne Again Shell, komut geçmişini bash geçmişi olarak adlandırılan bir dosyada saklayan utangaç uyumlu bir kabuktur. Daha fazla ~/.bash_history komutunu kullanarak kaydedilmiş komut geçmişini görüntüleyebilirsiniz. Bash_history dosyası, bir saldırının kökenini ve saldırgan tarafından bir sistemi tehlikeye atmak için kullanılan tam komutları izlemek için araştırmacılar tarafından kullanılabilceğinden, BASH'in bu özelliği bilgisayar korsanları için bir sorundur. Saldırganlar, kaydedilmiş komut geçmişinin parçalarını temizlemek için aşağıdaki komutları kullanır:

- The BASH is an **sh-compatible shell** which stores command history in a file called **bash_history**
 - You can view the saved command history using **more ~/.bash_history** command

Attackers use following commands to clear the saved command history tracks:

- └ command history tracks:
 - └ Disabling history
 - └ export HISTSIZE=0
 - └ Clearing the history
 - └ history -c (Clears the stored history)
 - └ history -w (Clears history of current shell)
 - └ Clearing the user's complete history
 - └ cat /dev/null > .bash_history && history -c && exit
 - └ Shredding the history
 - └ shred ~/.bash_history (Shreds the history file, making its content unreadable)
 - └ shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit (Shreds the history file and clear the evidence of the command)

Windows

- NTFS has a feature called as **Alternate Data Streams** that allows attackers to hide a file behind other normal files
- Given below are some steps in order to hide file using NTFS:
 - Open the command prompt with an elevated privilege
 - Type the command “`type C:\SecretFile.txt > C:\LegitFile.txt:SecretFile.txt`” (here, file is kept in C drive where SecretFile.txt file is hidden inside LegitFile.txt file)
 - To view the hidden file, type “`more < C:\SecretFile.txt`” (for this you need to know the hidden file name)

```
Administrator: Command Prompt
C:\>type C:\SecretFile.txt > C:\LegitFile.txt:SecretFile.txt
C:\>more < C:\SecretFile.txt
0hjdaJdn
Hidden Content
```

UNIX

- Files in UNIX can be hidden just by **appending a dot (.)** in front of a file name
- Attackers can use this feature to edit the **log files** to cover their tracks
- Attackers can use “`export HISTSIZE=0`” command to delete the command history and the specific command they used to hide log files

```
root@kali:~/Desktop/TEST# ls
CHANGELOG  dirtycow.c    README.md  sprayxml.py  TEST.py  Utilities
dirtycow   hello_world.txt  Responder-master test_1.txt  unicorn  wms
root@kali:~/Desktop/TEST# mv test_1.txt test_1.txt
root@kali:~/Desktop/TEST# ls
CHANGELOG  dirtycow.c    README.md  sprayxml.py  unicorn  wms
dirtycow   hello_world.txt  Responder-master TEST.py  Utilities
root@kali:~/Desktop/TEST#
```