

HAZIRLAYAN
BEDRİ SERTKAYA
bedri@bedrisertkaya.com
Sistem Uzmanı
CEH EĞİTMENİ

ENUMERATION:

Enumaretion ağda yer alan sistemlerden kullanıcı adları, bilgisayarlar, paylaşımlar, ağ kaynakları(yazıcılar vb.) elde etme işidir.

TCP Servislerini dinlemek için:

```
netstat -ant|grep LISTEN
```

UDP servislerini dinlemek için:

```
netstat -anu| grep i- UDP
```

TCPDUMP

Sık kullanılan parametreleri:

-i: ağ arabirimi
-nn: isim çözme

tcp port = port numarası

host = host seçimi
-w=kaydet

Web trafiğini izlemek için:

```
tcpdump -nn -i eth0 tcp port 80
```

ip adresine gelen giden trafiği görmek için:

```
tcpdump -nn -i eth0 host 8.8.8.8
```

Gelen giden smtp trafiği:

```
tcpdump -nn -i et
```

Saldırganlar ağ kaynakları ve paylaşımlarını kullanıcı ve gruplarını listeleyebilirler.

SNMP Üzerinden bilgi toplama:

SNMP Bilgi toplama araçları

Snmpenum

Snmpwalk

Nessus snmp pluginleri

Solarwinds snmp araçları

Cain & Abel SNMP

Simple Network Management Protocol:

SNMP (Simple Network Management Protocol) Enumeration



Simple Network Management Protocol (SNMP) is a TCP/IP protocol used for **remote monitoring** and managing hosts, routers, and other devices on a network

Attackers enumerate SNMP to **extract information** about network resources such as hosts, routers, devices, shares, etc.,



SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer

The default community string that provides the monitoring or read capability is often **"public,"** whereas the default management or write community string is often **"private"**



SNMP enumeration uses these default community strings to extract information about a device using the read community string "public"



Simple Network Management Protocol ağa bilgisayarlar ve ağa bağlı diğer cihazların uzaktan denetimini ve yönetimini sağlayan protokoldür.

Saldırganlar SNMP enumeration yaparak ağ kaynakları ve paylaşımlar hakkında bilgi sahibi olabilirler.

SNMP yönetici ve agent olmak üzere iki bileşenden meydana gelmektedir..Agentlar yönetici ile cihaz arasındaki deęişiklik ve iletişimi saęlayan uygulama.

Yönetici uygulama ise agent'dan aldığı bilgileri kullanıcıya aktaran bileşen.

MIB (Management Information Base) Nedir?

MIB SNMP tarafından yönetilecek bütün aę nesnelerinin sanal veritabanıdır. MIB veritabanı hiyerarşik bir yapıdadır.Her yönetilen nesne içinde MIB Object Identifiers(OID) tarafından benzersiz şekilde atanır.

OID yetki girişleri, stringleri kapsar.

SNMP protokolü MIB veritabanını OID benzersiz numaralarını human-readable hale getirmek için kullanır.

Snmperenum ile Bilgi Toplama:

Bu iş için snmperenum ve angry ip scanner araçları kullanılabilir.

SMTP Enumeration: Aşağıda yer alan resimde eposta sunucusunda yönetimsel bazlı sömürü yapılmaya çalışılmıştır.

SMTP Enumeration

Attackers can directly interact with SMTP via the telnet prompt:

```
C:\ Command Prompt
telnet 192.168.0.1 25
220 uk03.cak.uk ESMTP Sendmail 8.9.3; Wed, 9 Nov 2005 15:29:50 GMT
EXPN ROOT
250 <root@uk03.nu.cak.uk>
250 <smith.j@uk03.nu.cak.uk>
EXPN BIN
250 <bin@uk03.nu.cak.uk>
VRFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VRFY ORACLE
550 ORACLE... User unknown
QUIT
```

Netbios Enumaretion:

Biz bu iş için Superscan aracını kullandık.

Netbios Enumeration

Attackers use the NetBios enumeration to obtain:

1. List of computers that belong to a domain
2. List of shares on the individual hosts on the network
3. Policies and passwords



Port	Service
TCP 53	DNS zone transfer
TCP 135	Microsoft RPC Endpoint Mapper
TCP 137	NetBIOS Name Service (NBNS)
UDP 139	NetBIOS Session Service (SMB over NetBIOS)
TCP 445	SMB over TCP (Direct Host)
UDP 161	Simple Network Management protocol (SNMP)
TCP/UDP 389	Lightweight Directory Access Protocol (LDAP)
TCP/UDP 3368	Global Catalog Service

CEH Certified Ethical Hacker

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

NETBIOS Windows işletim sisteminde ip isim çözümleme yapılmasını sağlayan bir windows apisidir. (Application Programming Interface).NETBIOS sömürülerek yerel ağdaki bilgisayarlar listelenebilir.Şifreler elde edilebilir.

Network Time Protocol Enumeration:

Network time protocol ağa bağlı bilgisayarların zamanını konfigüre etmeyi sağlayan protokoldür.

Linux NTP enumeration araçları:

ntpdate:
güncel zamanı ayarlar

ntpq:NTP'ye bağlı eş sunucuları gösterebilmektedir.

Örnek:ntpq komutu girildikten sonra
peers yazıldığında gerekli listelemeyi yapar.

ntptrace:NTP'nin zamanı nereden aldığını kontrol eder ve gösterir.
Ntpdc sunucularını listeler:

Örnek:

```
greyday@ubuntugrey:~$ ntpdc -c monlist
```

```
remote address      port local address  count m ver rstr avgint lstart
```

```
=====
```

```
ts1.aco.net         123 192.168.2.2      53 4 4 1d0 79 1
fetchmail.mediainvent. 123 192.168.2.2      54 4 4 1d0 78 3
europium.canonical.com 123 192.168.2.2      52 4 4 1d0 81 85
asteria.debian.or.at 123 192.168.2.2      53 4 4 1d0 79 94
ntp.cnh.at          123 192.168.2.2      53 4 4 1d0 79 103
```

Linux Enumaretion:

Program:<https://github.com/rebootuser/LinEnum>