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

ENUMERATİON:

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

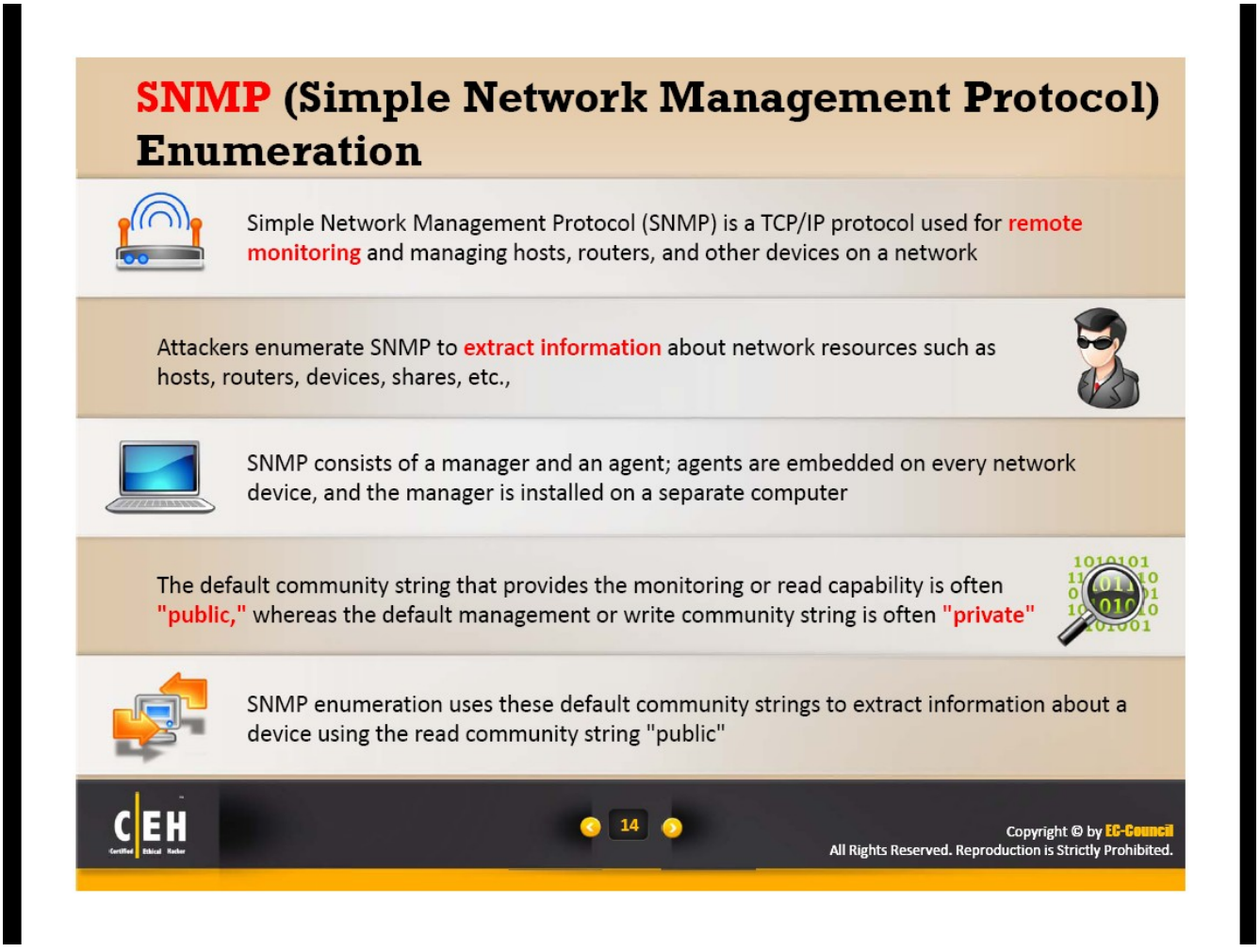
Saldırganlar ağ kaynakları ve paylaşımlarını kullanıcı ve gruplarını listeleyebilirler.

SNMP Üzerinden bilgi toplama:

SNMP Bilgi toplama araçları

Snmpenum
Snmpwalk
Nessus snmp pluginleri
Solarwinds snmp araçları
Cain & Abel SNMP

Simple Network Management Protocol:



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 değişiklik ve iletişimi sağlayan uygulama.

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

MIB (Management Information Base) Nedir?

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

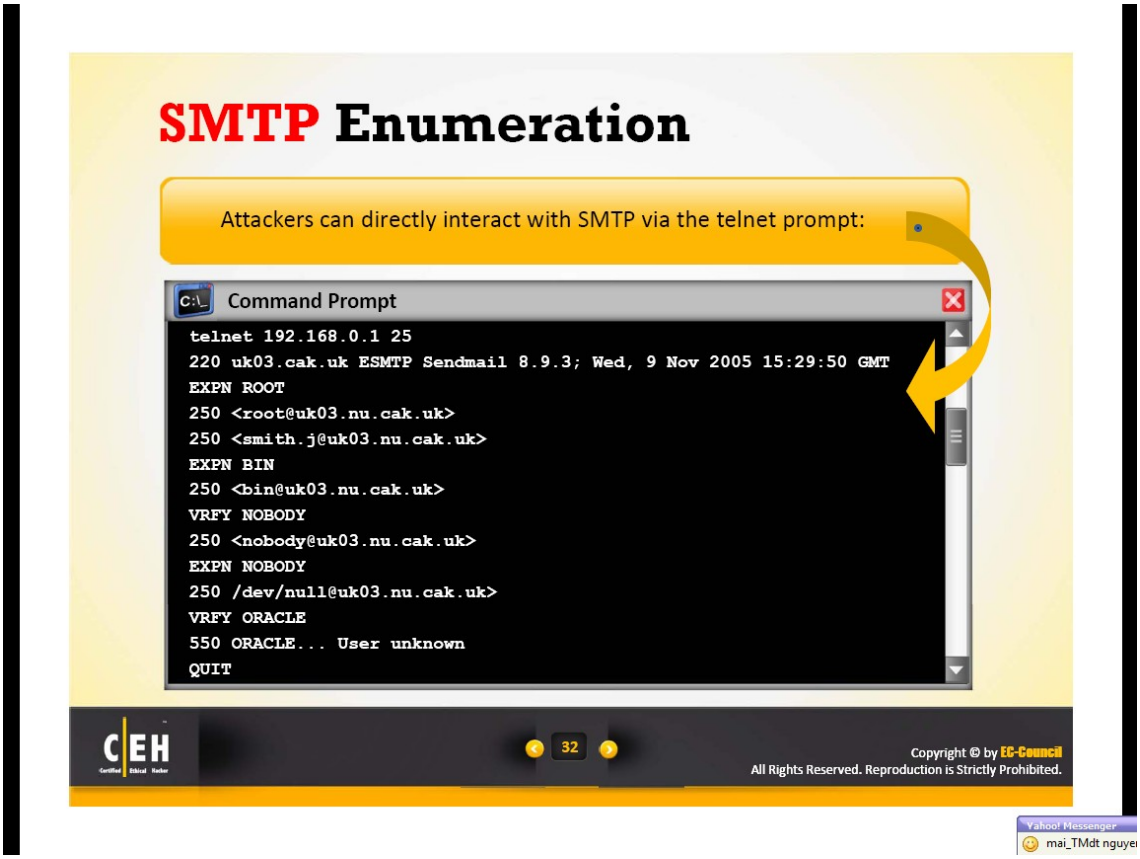
OID yetki girişleri, stringleri kapsar.

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

Snmpenum ile Bilgi Toplama:

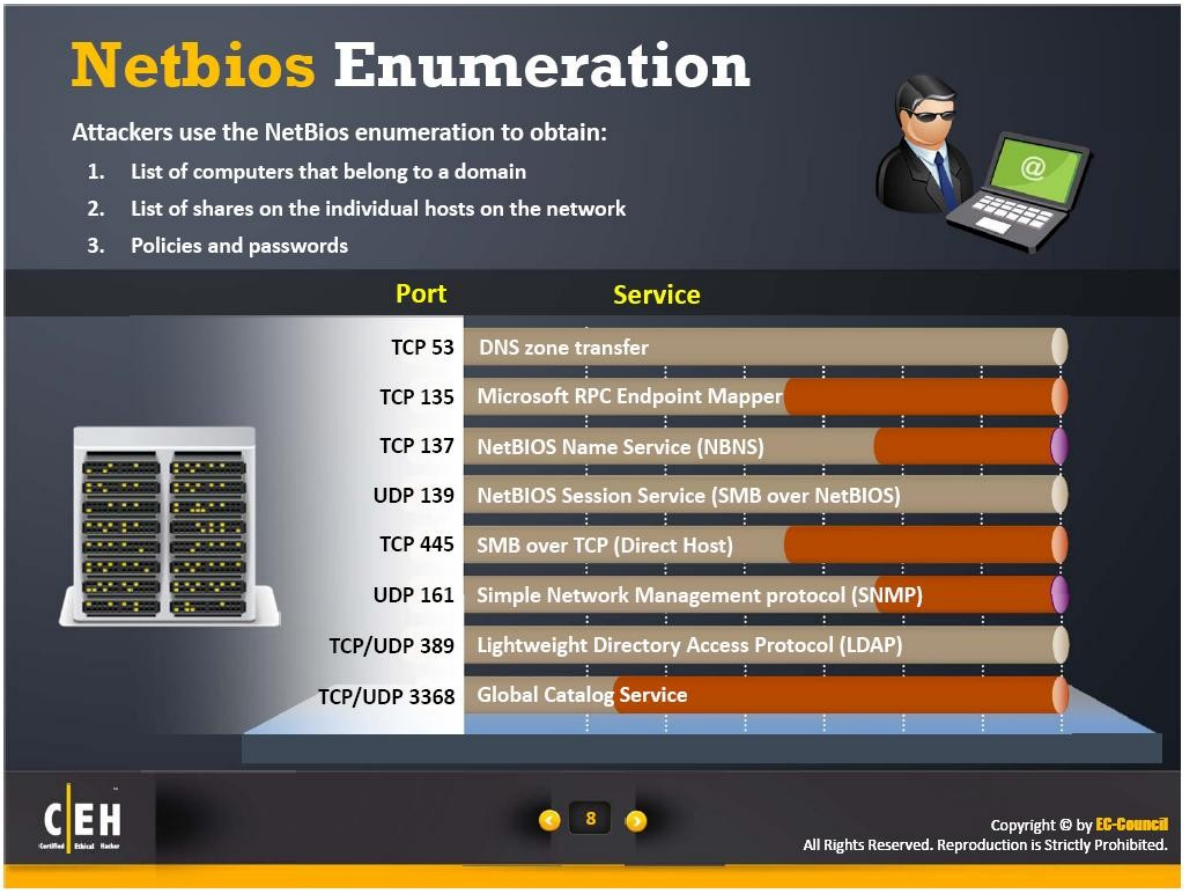
Bu iş için snmpenum ve angry ip scanner araçları kullanılabilir.

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



Netbios Enumaretion:

Biz bu iş için Superscan aracını kullandık.



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 bilgisayaların 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  lstint
===============================================================================
======
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