

# YMH321 Bilgi Sistemleri ve Güvenliđi

## Güvenlik Araçları

**Bölüm - 9**

**Prof. Dr. Resul DAŞ**  
Fırat Üniversitesi  
Yazılım Mühendisliđi Bölümü

# Konu Başlıkları

---

- Güvenlik Araçları
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

# Güvenlik Araçları

---

- Savunmadan çok “saldırı”ya yönelik araçlar.
- Amaç, saldırganlardan önce sistemdeki açıkları ortaya çıkarıp gereken önlemleri almak.

# Nmap

---

- “Network Mapper”
- Ağ araştırması ve güvenlik denetlemesi yapan açık kaynaklı ücretsiz bir yazılım.
- Geniş ölçekli ağları taramak için tasarlanmıştır.
- Alışılmışın dışında IP paketleri göndererek tarama yapar.

# Nmap

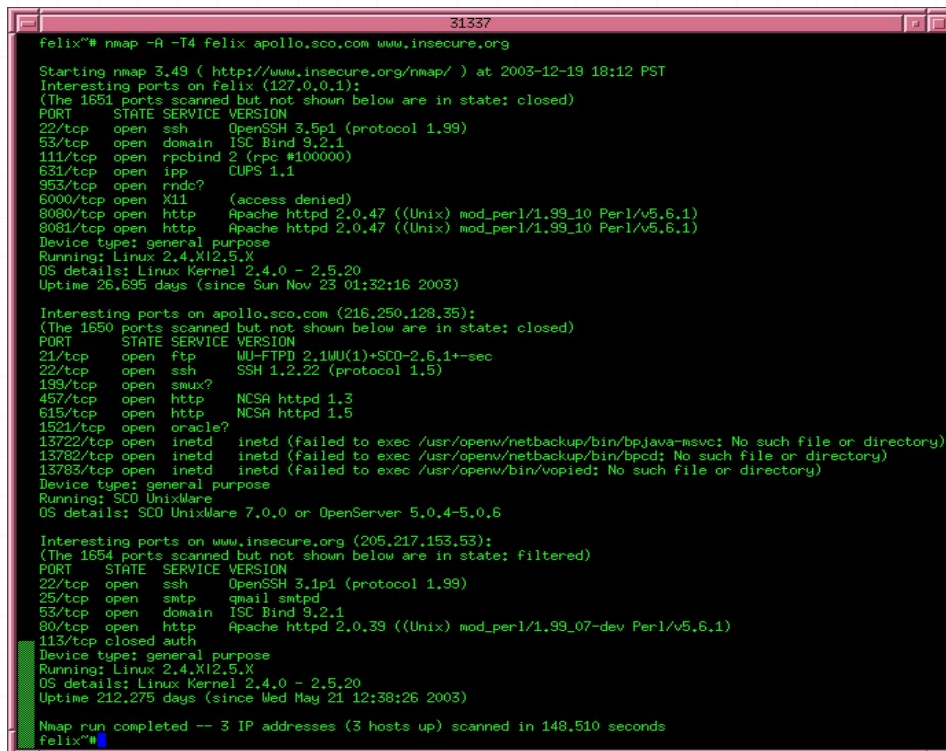
- Ağdaki canlı bilgisayarlar
- Çalışan servisler (Uygulama adı ve versiyonu)
- Koşulan işletim sistemi
- Varsa kullanılan güvenlik duvarı





# Nmap Görselleri

- [www.insecure.org/nmap](http://www.insecure.org/nmap)



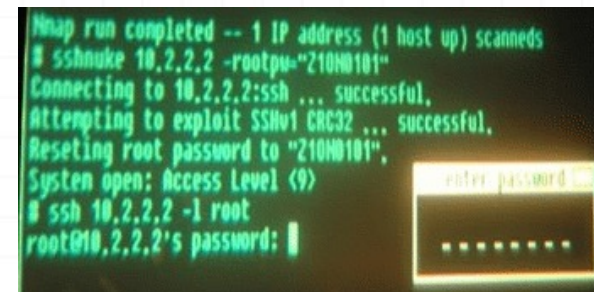
```
felix@~$ nmap -A -T4 felix apollo.sco.com www.insecure.org

Starting Nmap 3.49 ( http://www.insecure.org/nmap/ ) at 2003-12-19 18:12 PST
Interesting ports on felix (127.0.0.1):
(The 1651 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.5p1 (protocol 1.99)
53/tcp    open  domain   ISC Bind 9.2.1
111/tcp   open  rpcbind  2 (rpc #100000)
631/tcp   open  ipp       CUPS 1.1
953/tcp   open  rmds?
6000/tcp  open  X11       (access denied)
8080/tcp  open  http      Apache httpd 2.0.47 ((Unix) mod_perl/1.99_10 Perl/v5.6.1)
8081/tcp  open  http      Apache httpd 2.0.47 ((Unix) mod_perl/1.99_10 Perl/v5.6.1)
Device type: general purpose
Running: Linux 2.4.X12.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 26.695 days (since Sun Nov 23 01:32:16 2003)

Interesting ports on apollo.sco.com (216.250.128.35):
(The 1650 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       MU-FTPD 2.1MU(1)+SCO-2.6.1+-sec
22/tcp    open  ssh      SSH 1.2.22 (protocol 1.5)
199/tcp   open  smux?
457/tcp   open  http      NCSA httpd 1.3
615/tcp   open  http      NCSA httpd 1.5
1521/tcp  open  oracle?
13722/tcp open  inetd    inetd (failed to exec /usr/openw/netbackup/bin/bpjava-msvc; No such file or directory)
13782/tcp open  inetd    inetd (failed to exec /usr/openw/netbackup/bin/bpod; No such file or directory)
13783/tcp open  inetd    inetd (failed to exec /usr/openw/bin/vopied; No such file or directory)
Device type: general purpose
Running: SCO UnixWare
OS details: SCO UnixWare 7.0.0 or OpenServer 5.0.4-5.0.6

Interesting ports on www.insecure.org (205.217.153.53):
(The 1654 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp      qmail smtpd
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http      Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X12.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212,275 days (since Wed May 21 12:38:26 2003)

Nmap run completed -- 3 IP addresses (3 hosts up) scanned in 148.510 seconds
felix@~$
```



```
Nmap run completed -- 1 IP address (1 host up) scanned
# sshnuke 10.2.2.2 -rootpw="210HW101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Resetting root password to "210HW101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password: [REDACTED]
```



# Nessus



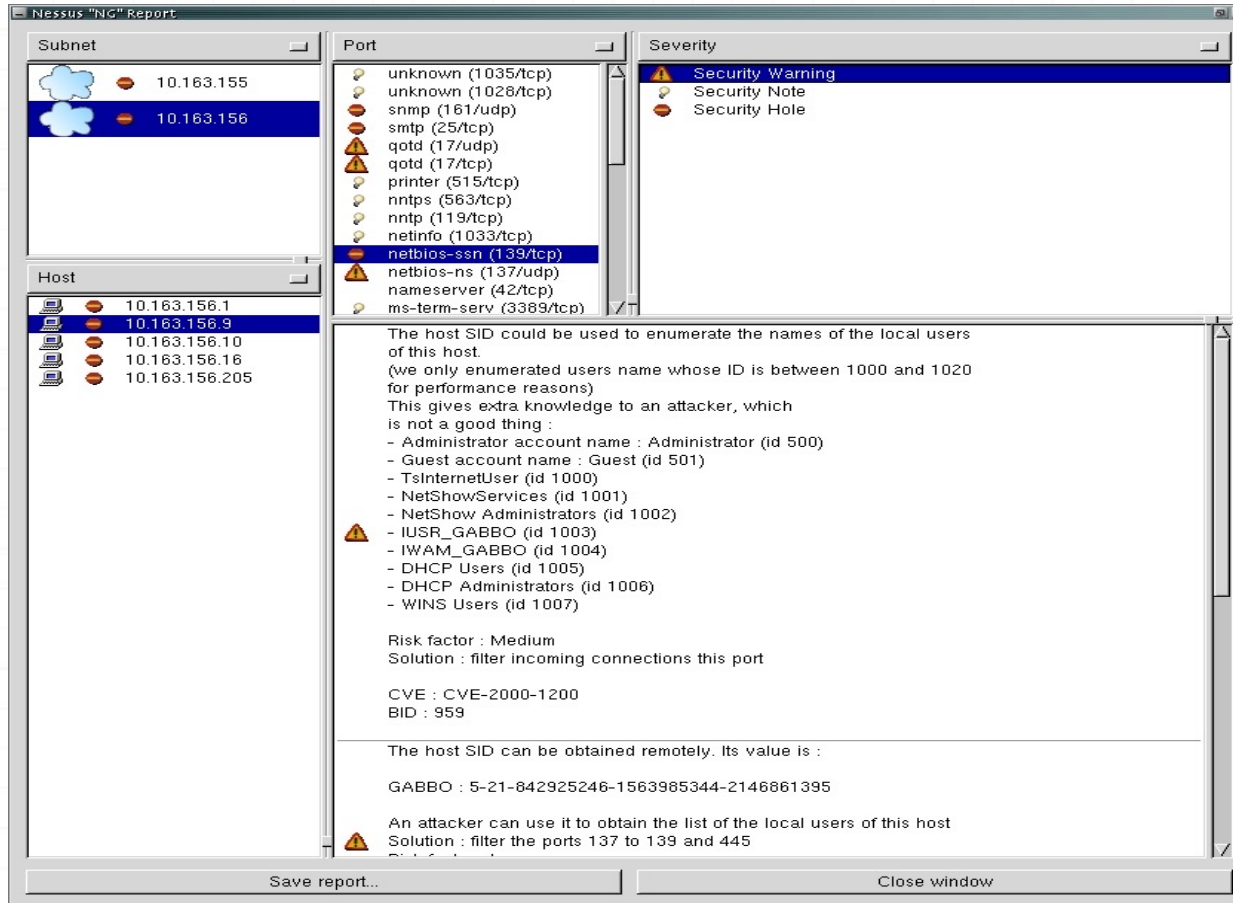
- Güçlü, güncel ve ücretsiz bir uzaktan güvenlik taraması aracı.
- Diğerlerinden en büyük farkı bilinen kurallara bağlı olmaması. (Örnek: web sunucusu 1234 numaralı portta çalışsa bile nessus onu bulup güvenlik taraması yapabiliyor.)

# Nessus

- Platform: Unix ve benzeri sistemler +  
Windows
- Çok çeşitli raporlama yetisi (HTML, XML, LaTeX, and ASCII)
- Uyumlu ek (plug-in) yazılımları ve GTK arayüzü ile kullanışlı
- [www.nessus.org](http://www.nessus.org)



# Nessus Görseli



# Ethereal



- Unix ve windows üzerinde çalışabilen bir protokol analizi aracı.
- Canlı bir ağ üzerindeki verileri incelemek veya disk üzerine kaydetme amacıyla kullanılır.
- Her paket için ayrıntılı bilgi gösterebilen interaktif bir arayüzü vardır.

# Ethereal

- Metin tabanlı versiyonu tethereal.
- Ücretsiz.



```
brunching.com  TCP    1028 > www [ACK] Seq
brunching.com  HTTP    GET / HTTP/1.0
.1.85
.1.85  — Contents of TCP stream
brunch  GET / HTTP/1.0
.1.85  Connection: Keep-Alive
brunch  User-Agent: Mozilla/4.75 [en] (X11;
.1.85  Host: www.brunching.com
.1.85  Accept: image/gif, image/x-xbitmap,
.1.85  Accept-Encoding: gzip
brunch  Accept-Language: en
```

[www.ethereal.com](http://www.ethereal.com)

# Snort



- Gerçek zamanlı trafik analizi ve paket kayıtlaması yapabilen ücretsiz bir ağ saldırı belirleme sistemi.
- Protokol analizi, içerik araştırması ve eşlemesi yapabilir.
- Tampon taşıma, gizli port taramaları, CGI saldırıları, SMB yoklamaları, işletim sistemi belirleme saldırıları gibi birçok saldırı veya yoklamayı belirleyebilir.

# Snort

---

- Esnek bir kural yazma dili
- Modüler uyumlu ek yazılım mimarisi.
- Gerçek zamanlı alarm mekanizması.  
(syslog, windows eventlog, winpopup, vb.)
- Arayüz yazılımı ACID.

[www.snort.org](http://www.snort.org)



# tcpdump

- Ağ inceleme ve veri yakalama amaçlı klasik bir sniffer.
- Metin tabanlı
- Ağ hareketlerini incelemeye kullanılır.
- Verilen deyimleri eşleyerek belirli bir ağ arayüzündeki paket başlıklarını gösterebilir.
- Nmap tcpdump altyapısını kullanır.
- [www.tcpdump.org](http://www.tcpdump.org)

# DSniff



- Güçlü bir ağ denetleme ve giriş testi (penetration test) amcına yönelik araçlar takımı.
- dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf ve webspay araçları ağ üzerinde pasif bir şekilde kayda değer veri araştırmasında kullanılı. (şifre, e-posta, vb.)

# DSniff

- arpspoof, dnsspoof ve macof normalde saldırganın ulaşamayacağı (2. katman) ağ bilgilerine ulaşmasını kolaylaştırır.
- sshmitm ve webmitm ssh ve https oturumlarında monkey-in-the-middle saldırılarında kullanılır.

<http://naughty.monkey.org/~dugsong/dsniff/>

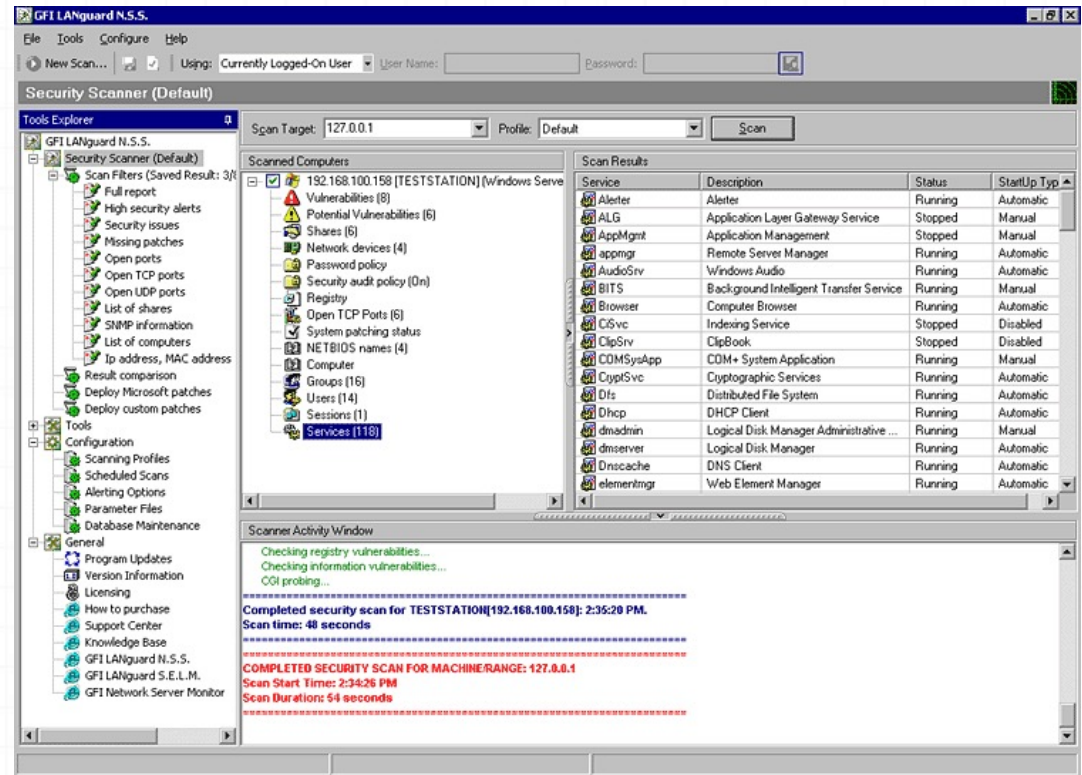
# GFI LANguard

---

- Sistemdeki güvenlik hasar risk analizini otomatik olarak yapan bir araç.
- Windows üzerinde çalışır.
- Ağ taraması yapar.
- Her makinenin servis paket durumunu, yamanmamış güvenlik açıklarını, açık paylaşım alanlarını ve portlarını, çalışan uygulamalarını, vb. birçok bilgiyi raporlar.

# GFI LANguard

- Ücretli bir yazılımdır.  
(Windows tabanlı!)
- Deneme sürümü  
mevcut.
- [www.gfi.com](http://www.gfi.com)





# Ettercap

- Anahtarlamalı yerel ağlar için kullanılan bir sniffer, araya girme ve kayıt yapma aracıdır.
- Şifreli olanlar da dahil birçok protokol için aktif ve pasif inceleme özelliği vardır.
- Kurulmuş bağlantılara veri enjeksiyonu yapma ve filtreleme özellikleri vardır.
- Ağ geometrisini çıkarma ve işletim sistemi tespitleri yapabilir.

# John the Ripper

---

- Çok hızlı bir şifre kırıcısı.
- Unix (11'i resmi olarak desteklenen birçok farklı mimarisinde), DOS, Win32, BeOS ve OpenVMS üzerinde çalışabilir.
- Geliştirilme amacı zayıf unix şifrelerini tespit etmek.
- Unix crypt(3) şifre özü, Kerberos AFS ve Windows NT/2000/XP LM özlerini kırabilir.
- Aynı zamanda sürekli güncellenen şifre veritabanı vardır.

# ISS Internet Scanner

---

- Uygulama düzeyinde ağa bağlı araçlar üzerinde hasar risk analizi yapabilen ücretli bir yazılım.
- Ağdaki güvenlik açıklarını yakalamada çok iyi fakat çok pahalı bir yazılım. (ucuz + iyi = nessus)

[www.iss.net](http://www.iss.net)

# tripwire

- Bütünlük analizi yapan araçların büyükbabası.
- Dosya ve dizinlerin bütünlüklerinin bozulup bolulmadığını inceler.
- Herhangi bir değişim sonrası sistem yöneticilerini uyarır.
- Açık kaynak kodlu versiyonu Linux için [www.tripwire.org](http://www.tripwire.org) da mevcut.
- Diğer sistemler için ücretli.

# Güvenlik Araçları

- Ana kaynak:  
[www.insecure.org](http://www.insecure.org)





# Sonuç

---

# Sorular

---

