

# Sig•Mat

Meeting 4

# Port Scanning Project

How was it?



# nmap

Open-source network  
scanner

→ The industry standard  
for network scanner /  
port scanning in  
security

```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE  SERVICE VERSION
22/tcp    open   ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open   smtp      Postfix smtpd
53/tcp    open   domain    ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open   http      Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE  SERVICE  VERSION
21/tcp    open   ftp       Serv-U ftpd 4.0
25/tcp    open   smtp      IMail NT-ESMTP 7.15 2015-2
80/tcp    open   http      Microsoft IIS webserver 5.0
110/tcp   open   pop3      IMail pop3d 7.15 931-1
135/tcp   open   mstask     Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open   msrpc      Microsoft Windows RPC
5800/tcp  open   vnc-http   Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

# Firewalls

→ a network security system that monitors and controls incoming and outgoing network traffic

→ based on predetermined security rules

→ barrier between a trusted network and an untrusted network

# Firewalls



**LIVE DEMO TIME**