SERVICE SCAN

AND

NETWORK ENUMERATION

BARBAGALLO VALERIO
DA LOZZO GIORDANO
MELLINI GIAMPIERO

Roma Tre

Sicurezza dei sistemi informatici e delle reti

Basics

- **Host Discovery:**
  - determine the accessible hosts on a network
  - ICMP ping, SYN Ping, ACK Ping, UDP Ping, IP Protocol Ping and ARP Ping

- **Port Scanning:**
  - search a network host for open ports
  - TCP scanning and UDP scanning

  - **Service scan**
    - identifies the services running on a list of open ports
    - sending some probe data to the port and monitoring the response
  - **TCP/IP stack fingerprinting** (a.k.a. **OS fingerprinting**)
    - the process of determining the operating system used by a remote target
    - TCP/IP flag settings are specific to various operating systems

Tools

Some powerful tools for "host discovery and port scanning":

- **Netcat** (TCP/IP swiss army knife)
  - offers basic functionalities for **TCP and UDP scanning**
  - needs zero I/O mode (option -z)
- **Hping**
  - able to send custom TCP/IP packets and to display target replies
  - used to exploit the idle scan scanning technique
- **Nessus**
  - begins by doing a port scan with one of its internal portscanners (or it can also use Nmap) to determine which ports are open on the target
  - then tries various exploits on the open ports
- **Nmap**
  - an open source tool for network exploration and security auditing
  - designed to rapidly scan large networks

  …

Nmap (Network Mapper)

Port Division

- open, closed, filtered, unfiltered, open|filtered and closed|filtered

Scanning techniques

-sS (TCP SYN scan)

-sT (TCP connect() scan)

-sU (UDP scans)

-sN; -sF; -sX (TCP Null, FIN, and Xmas scans)

-sA (TCP ACK scan)

-sW (TCP Window scan)

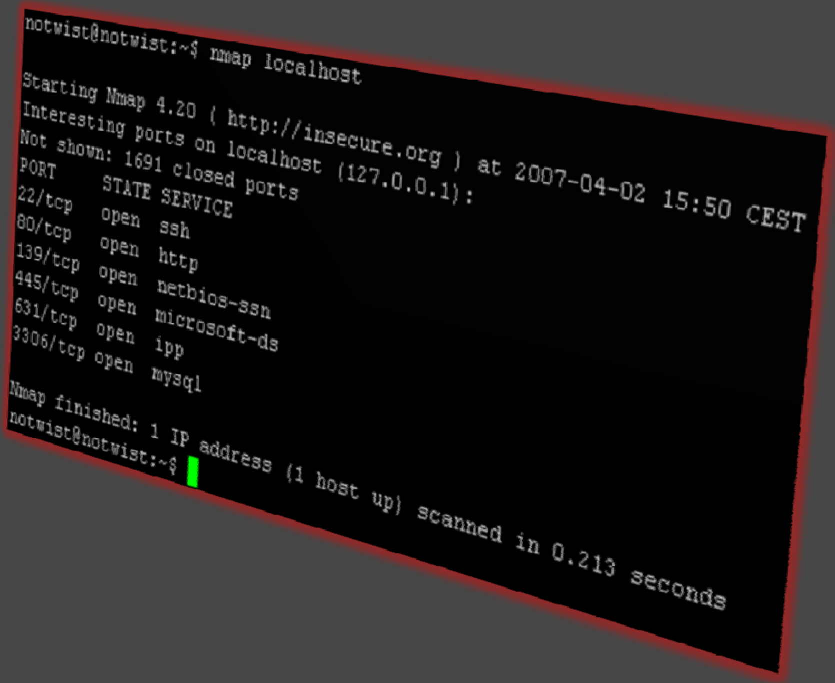
-sM (TCP Maimon scan)

--scanflags (Custom TCP scan)

-sI <zombie host[:probeport]> (Idlescan)

-sO (IP protocol scan)

-b <ftp relay host> (FTP bounce scan)



```
notwist@notwist:~$ nmap localhost

Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
631/tcp  open  ipp
3306/tcp open  mysql

Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
notwist@notwist:~$
```

Nmap - Idlescan (Zombie Scan)

First Stage:

1. IPID Probe:		Attacker	→	Zombie	SYN/ACK
		Zombie	→	Attacker	RST (IPID 31337)

Second Stage:

2. Attack:		Attacker	→	Target	Spoofed SYN from the Zombie
	open port	Target	→	Zombie	SYN/ACK
if		Zombie	→	Target	RST (increments its IPID)
	closed port	Target	→	Zombie	RST

Third Stage:

3. IPID Probe:		Attacker	→	Zombie	SYN/ACK
		Zombie	→	Attacker	RST (IPID 31338) -> IPID INCREMENTED

- takes advantage of the “predictable IPID flaw”
- sends spoofed packets to a computer
- nmap -P0 -p <port> -sI <zombie IP:Port> <target IP>

```
Starting Nmap 4.01 (guardian.telservice.net)
Int. ports on guardian.telservice.net(205.21
(The ports scanned but not shown are in state
Port      State    Service        Version
22/tcpopen   ssh            SSH 3.9p1(prot
25/tcpopen   smtp           Postfix smtpd
53/tcpopen   domain
```

```
Last login:19:01:41 on console
Welcome to CRI!
SECOM Interagency Contract Network 6674
Mark-Coleran:~ mcoleran$ show tag 443 -
loading....
```

```
et Mask
et Routing
et Mirrors
nonymous Pr

94.6.1.219
96.23.147.34    196.40.43.34      200.21.225.82    200.21
00.52.4.82      200.61.6.50       202.103.6.178    202.10
02.105.130.19   202.105.230.226   202.106.139.88   202.108.122.38
02.110.220.14   202.9.136.40      202.99.225.45

coleran$ Nmap GUI
```

```
loading....
Chain 14, UMIT Recover from SMTP- smtp.guardian.co.uk
File 23
From:   adrian.spanna@guardian.co.uk
Subject: flight details conf ASAP
Date: 17:53:21 BDT
To:   simon.ross@guardian.co.uk
Return-Path: <adrian.spanna@guardian.co.uk>
Delivery-Date: 17:48:55 +0100
Received: from mail.guardian.co.uk ([195.72.171.30]) by mail.guardian.net.uk with esmtp (Exim 4.52)
id 1DsNwF-00023o-Bb for simon.ross@guardian.co.uk; 17:48:55 +0100
Envelope-To: simon.ross@guardian.co.uk
Message-Id: <6407D046A0F712458139A7E11326731112D55A@guardian.co.uk> Mime-Version: 1.0 !

Ross, Simon mr

Flight-(MSC)-2538 Fri 17 Nov 2006                   Flight-(MSC)-2539 Fri 17 Nov 2006

Outbound                                            Return
Flight 2538              Non-stop                   Flight 2539              Non-stop
Status:                  Confirmed (HK)             Status:                  Confirmed (HK)
Class of Service:        Euro (M)                   Class of Service:        Euro (M)
Depart:    06:00 AM      Arrive:    08:00 AM        Depart:    12:00 PM      Arrive:    1:05 PM
Fri 17 Nov 2006          Fri 17 Nov 2006            Fri 17 Nov 2006          Fri 17 Nov 2006

Heathrow Arpt (LTR)      Citta Di Torino Arpt (TRN) Citta Di Torino Arpt(TRN) Heathrow Arpt (LTR)
London                   Turin                      Turin                    London
Terminal N               Terminal C                 Terminal C               Terminal N


Eticket ref no:          2897XH
Travel services ref no:  UK938934
```

Thank you for your attention!