# Lecture 4

SECURITY ASSESSMENT

# Information Leakage



HOW PROTOCOLS CAN REVEAL INFORMATION TO ATTACKERS

# Information Leakage



- Protocols can reveal information
  - By design, some are meant to provide information
  - But they also reveal to Oscar the same or more information
- Information leaks can be used for
  - Social engineering attacks
  - Cracking passwords
  - Mapping network topologies
  - Determining open services provided by servers

No information is mundane!
All information can be misused

# How does Information Leak?



- Passive
  - Wire(less)tapping
    - Access to physical medium of communications
    - Possible active attacks - redirection to different physical medium
  - Tempest
    - Electronic emanations that can be captured by Oscar
- Active
  - Information services
    - Protocols specifically designed for providing information
  - Insecure protocols
    - Protocols in general that reveal information unintentionally
    - Protocols that can be abused to obtain information

# Locations for Wiretapping



- Internal
  - Wiring closets
  - Broadcast links (LANs)
  - Tempest
- External
  - Dial-out modems, **routers**, microwave links
- It is easier to tap into copper wiring and wireless than fiber
  - Increasingly becoming easy to tap into fiber as well
  - WLAN signals can be detected at great distances using a high gain antenna

# Tapping into external points



- Idea
  - Falsify route so that packets go through routers/hosts controlled by Oscar
- Methods
  - Use ICMP to send false redirect messages to routers
  - IP loose source route option
  - Bogus routing messages

## Using ICMP



- ICMP redirect messages can be used to create alternative routes to a destination
  - Oscar can use this to route traffic through machines that he controls
  - He can change, sniff, stop packets
- Prevention
  - ICMP redirect messages should be obeyed only by "hosts" NOT routers
  - They should be obeyed only if they are sent by a router on the same network as the host

## Using IP Loose Source Route Option



- The initiator of a connection can specify the route to the reply
  - This is an explicit path that the packet must take to reach the destination
  - The destination will use the inverse path as the return route whether or not it makes sense
- Oscar can spoof the source address and make packets go through his routers or hosts
  - The source perhaps never initiated the connection

# Bogus RIP or BGP Messages



- RIP = Routing Information Protocol
- Autonomous system (AS)
  - A collection of routers under the same administrative control and running the same routing protocol
  - RIP is used to exchange routing information in an AS
  - Routing tables are exchanged every 30 s using advertisements or RIP response messages
- In the older versions of RIP, it is easy to inject false routing messages
  - Oscar may have hijacked a router and make packets go through this router for his own benefit
- BGP = Border Gateway Protocol
  - Distributes routing information between ASs
  - Subject to similar attacks
  - More dangerous as it takes about 20 minutes for BGP information to propagate through the internet

# Protection Against Wiretapping



- Physical protection of wiring cabinets, hosts, routers, etc.
- OSPF and RIPv2 support some authentication
  - Most authentication schemes are weak
    - Simple password based authentication, most of them in cleartext
  - If a router has been compromised, it does not matter
- Check topology to see if an advertised route makes sense
  - Hard to implement
- ISPs use IS-IS protocol internally
  - IS = Intermediate System (from OSI model)
  - Since this protocol is not common, it provides some protection against malicious packets
- Use encryption

# TEMPEST



- Radiations and emanations from equipment can be captured
  - If they carry sensitive information, they can be compromised
  - Examples of leaky radiations:
    - Video monitors have the so-called van Eck radiation
    - Keyboard strokes
    - Reading and writing to disks
  - Crosstalk between cables carrying classified and unclassified information is also a tempest threat
- Encryption of messages cannot help in many cases here

# Security against Tempest threats



- Classification
  - Red – Cables and equipment that carry classified information
  - Black – Cables and equipment that carry unclassified information
- Need strict Red/Black separation
  - Physical areas must be separated
- Careful design of circuits and grounding
- Use of equipment that conforms to federal/military standards
  - e.g. MIL-STD-461B

## Information Services



- There are many information services that exist to help legitimate users
  - DNS
  - NIS
  - Finger, whois, LDAP and the web
- They *may* provide Oscar information about the network and users
  - Who is logged on
  - What accounts are inactive for a long time
  - What IP addresses are being used
  - What operating systems are running

## DNS Tools



- `nslookup` and `dig` are two common commands to lookup addresses and names
- `nslookup` creates its own command line
  - Several options for gathering information exist
- `dig` stands for Domain Internet Groper
  - Replacing `nslookup` as the tool to check for DNS
  - Helps you get the version number of the DNS software running on a name server

# nslookup

- Works on both Unix-like and Windows OSs
- Non-interactive and interactive modes
- Options to change nameserver, resolve a host name with a particular server, etc.
- Use `man nslookup` on Unix machine or nslookup and help on Windows machine for more details

Terminal — tcsh — 80x24

```
[Vani:~] prashant% nslookup paradox.sis.pitt.edu
Note:  nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead.  Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
Server:         205.171.3.65
Address:        205.171.3.65#53

Non-authoritative answer:
Name:   paradox.sis.pitt.edu
Address: 136.142.116.28
```

Command Prompt

```
C:\Documents and Settings\prashant>nslookup
Default Server:  acheron.sis.pitt.edu
Address:  136.142.116.73

> paradox.sis.pitt.edu lethe.sis.pitt.edu
Server:  lethe.sis.pitt.edu
Address:  136.142.116.11

Name:    paradox.sis.pitt.edu
Address:  136.142.116.28

> set type=mx
> sis.pitt.edu
Server:  acheron.sis.pitt.edu
Address:  136.142.116.73

sis.pitt.edu    MX preference = 10, mail exchanger = mail.sis.pitt.edu
sis.pitt.edu    nameserver = acheron.sis.pitt.edu
sis.pitt.edu    nameserver = phlegethon.exp.sis.pitt.edu
sis.pitt.edu    nameserver = lethe.sis.pitt.edu
sis.pitt.edu    nameserver = icarus.sis.pitt.edu
mail.sis.pitt.edu       internet address = 136.142.116.22
lethe.sis.pitt.edu      internet address = 136.142.116.11
icarus.sis.pitt.edu     internet address = 136.142.116.2
acheron.sis.pitt.edu    internet address = 136.142.116.73
phlegethon.exp.sis.pitt.edu     internet address = 136.142.118.4
> exit

C:\Documents and Settings\prashant>
```



# dig

- `dig` is used primarily on unix-like systems
- It can provide a lot of information based on the options selected
- Used for troubleshooting purposes as well
- Use `man dig` on Unix machine for more details

Terminal — tcsh — 78x33

```
[Vani:~] prashant% dig @136.142.116.73 mx sis.pitt.edu

; <<>> DiG 9.2.2 <<>> @136.142.116.73 mx sis.pitt.edu
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 674
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; QUESTION SECTION:
;sis.pitt.edu.                  IN      MX

;; ANSWER SECTION:
sis.pitt.edu.           86400   IN      MX      10 mail.sis.pitt.edu.

;; AUTHORITY SECTION:
sis.pitt.edu.           86400   IN      NS      lethe.sis.pitt.edu.
sis.pitt.edu.           86400   IN      NS      icarus.sis.pitt.edu.
sis.pitt.edu.           86400   IN      NS      acheron.sis.pitt.edu.
sis.pitt.edu.           86400   IN      NS      phlegethon.exp.sis.pitt.edu.

;; ADDITIONAL SECTION:
mail.sis.pitt.edu.      86400   IN      A       136.142.116.22
lethe.sis.pitt.edu.     86400   IN      A       136.142.116.11
icarus.sis.pitt.edu.    86400   IN      A       136.142.116.2
acheron.sis.pitt.edu.   86400   IN      A       136.142.116.73
phlegethon.exp.sis.pitt.edu. 86400 IN   A       136.142.118.4

;; Query time: 94 msec
;; SERVER: 136.142.116.73#53(136.142.116.73)
;; WHEN: Mon May 24 13:19:55 2004
;; MSG SIZE  rcvd: 223

[Vani:~] prashant%
```

# DNS Zone Transfer Attacks



- Primarily used for information and reconnaissance by Oscar
  - DNS information is meant to be available globally
  - Using `ls -d` with nslookup will list all records for the domain
  - Sometimes the host information is also included (OS, version, architecture etc.)
- Typically, this option is disabled by most administrators except for the secondary name server
  - Typically use name/address based authentication :-(

# Other Information Services



- LDAP
  - Lightweight Directory Access Protocol
  - Supplies public key certificates, address books, calendars, etc.
- The Web
  - Some old implementations allow you to list all files in a user's directory
    - Several sources of information – rhosts, dead.letter, etc.
- Finger and whois

# Other Protocols that Leak Information (I) - RPC



- RPC = Remote procedure call
  - Client can make subroutine calls to a server *transparently*
  - Network programming complexities are masked by the RPC layer
  - Available on many platforms including Windows (MSRPC)
    - COM+ makes use of MSRPC
- RPC servers do not use fixed port numbers
  - Rely on *rpcbind* to map the service to the port number
  - rpcbind is also called *portmapper*
- The command *rpcinfo* can reveal what services are available at what port numbers using what protocols

# NIS



- NIS = Network Information Service
  - The name says it all ☺
  - Formerly called Yellow Pages
  - An RPC based application
- Distributes a variety of information from a central database to clients/other servers
  - Examples: Password files, public and private key databases, etc.
  - There are access control mechanisms in place to prevent unauthorized access
  - Oscar could still sniff a password file that is being legitimately transferred over the network

# Protocols that Leak Information (II) - HTTP



- HTTP sessions provide valuable information
  - GET command with a URL and
    - User agent – specifies browser and OS (and so what bugs you have on your system)
    - Referer – the page where you clicked the link
    - Accept – data formats that you accept (images, pdfs, etc.)
    - Cookie – information previously set by the same server
      - Cookies are used to maintain state information
    - Browser dependent information – depends on the browser
  - Response
    - Similar to GET message

# Protocols that Leak Information (III)



- SMTP
  - Simple Mail Transfer Protocol
  - Main protocol for sending e-mail messages
  - Can be used to get valuable information
    - Convert mail aliases to real login names – find out who the sysadmin is
- Instant messaging
  - When a buddy logged in; when he logged out; when he logged in again
  - Can provide valuable information about the real/cyber activities of a person
- SNMP
  - Used in network management
  - MIBs can reveal a lot of information
  - More about SNMP in later classes
- X11 servers
  - Can be used to capture keystrokes of other users
  - Should be forced to operate only on local machines

# More serious information leaks/holes



- Anonymous FTP and TFTP (trivial FTP)
  - Should be restricted to a couple of directories
  - Otherwise, Oscar can navigate to areas and get files and information he should not
- Microsoft's SMB (Server Message Block) protocol
  - Transported on a variety of protocols
  - Ports 135-139, 445
  - Net Send
- Since these protocols can potentially reveal file contents they are more dangerous
  - A particular example is the password file
  - They can also be used to place backdoors and bugs

# Abusing Protocols to get Information



TCP AND ICMP

# Port Scanning



- Scans of open ports are a common way for Oscar to find out what services are available for exploits
- Many scans are blatant - Oscar does not hide his attempts to scan hosts/systems
- ACK Scan
  - Oscar sends TCP segments with the ACK field set to ports on hosts that he thinks are open
  - If a port is open, the service responds with a RST because there is no connection
  - Oscar knows that the port is open
- If the ACK bit is set, some packet filters allow the packet into the network because it may be part of an active connection

# ICMP for Mapping Targets



- Oscar cannot launch many attacks randomly as they may result in unforeseen consequences like quick detection or total failure
  - Reconnaissance is extremely important - we have seen ways of doing this with say DNS zone transfers
- Ringzero was a Trojan program that scanned ports 80, 8080 and 3128 (http, http-proxy and squid proxy) randomly
  - For a long time no one knew that these scans were due to Ringzero
- A common method of mapping a network is to use ping (ICMP echo request)
  - Many networks now block ping from outside, but ACK scans and others have replaced it

# Mapping Techniques



- Brute force
  - Ping entire range of IP addresses suspected to exist in a network
  - Produces a lot of signatures detectable by IDS systems
- Technique 1
  - Broadcast the ICMP message! - Directed Broadcast
  - Uses the a.b.c.0 or a.b.c.255 addresses
- Technique 2
  - Broadcast to a subnet that Oscar suspects may exist
  - Example: a.b.c.63 will broadcast to a 64 node subnet
- Technique 3
  - ICMP requests can be made to hosts to determine the subnet masks in a variety of ways

# Penetration Test

- The test to find out security vulnerabilities by hacking the security system ourselves
  - By our own people or hiring third party
- The test for checking the policy compliance
  - To make sure the organization's policy has been regulated
- To test the current status of your security system whether it is still strong enough
  - The dynamic change of the networks and devices can cause new vulnerabilities
- The test to be conducted by "Ethical Hacker"

# Standards for Pen Test

- TIGER (http://www.tigerscheme.org)
  - founded in 2007, on the principle that a commercial certification scheme run on independent lines
- OWASP (*https://www.owasp.org*)
  - Open Web Application Security Project (OWASP) is an Open Source community project developing software tools and knowledge based documentation that helps people secure web applications and web services
- Payment Card Industry (PCI) (*https://www.pcisecuritystandards.org*)
  - established in December 2004, and apply to all Members, merchants, and service providers that store, process or transmit cardholder data
- ISACA *https://www.isaca.org*
  - Was established in 1967 and has become a pace-setting global organization for information governance, control, security and audit professionals
- OSSTMM *http://www.osstmm.org*
  - The aim of The Open Source Security Testing Methodology Manual (OSSTMM) is to set forth a standard for Internet security testing.
  - It is intended to form a comprehensive baseline for testing that, if followed, ensures a thorough and comprehensive penetration test has been undertaken

# What Should You Test?

- Off-the-shelf products like servers, smart phones, firewalls and routers etc.
- Bespoke software development like web sites, mobile applications and games etc.
- Telephone equipment like exchanges, smart phones, VOIP and fax servers etc.
- Wireless systems like WIFI networks, RFID tokens, and contactless cash etc.
- Physical protection like CCTV, door entry systems and mechanical locks etc.

# Steps for Pentest

- Reconnaissance
  - Whois
  - Internet Search
  - DNS Record Retrieval
  - Social Engineering
  - Dumpster Diving
  - Website Copying
- Exploitation
  - Discovery & Probing
- Reinforcement
  - Password Cracking
  - Vulnerability Scanning
- Making a final report
  - Give suggestion based on organization's policy