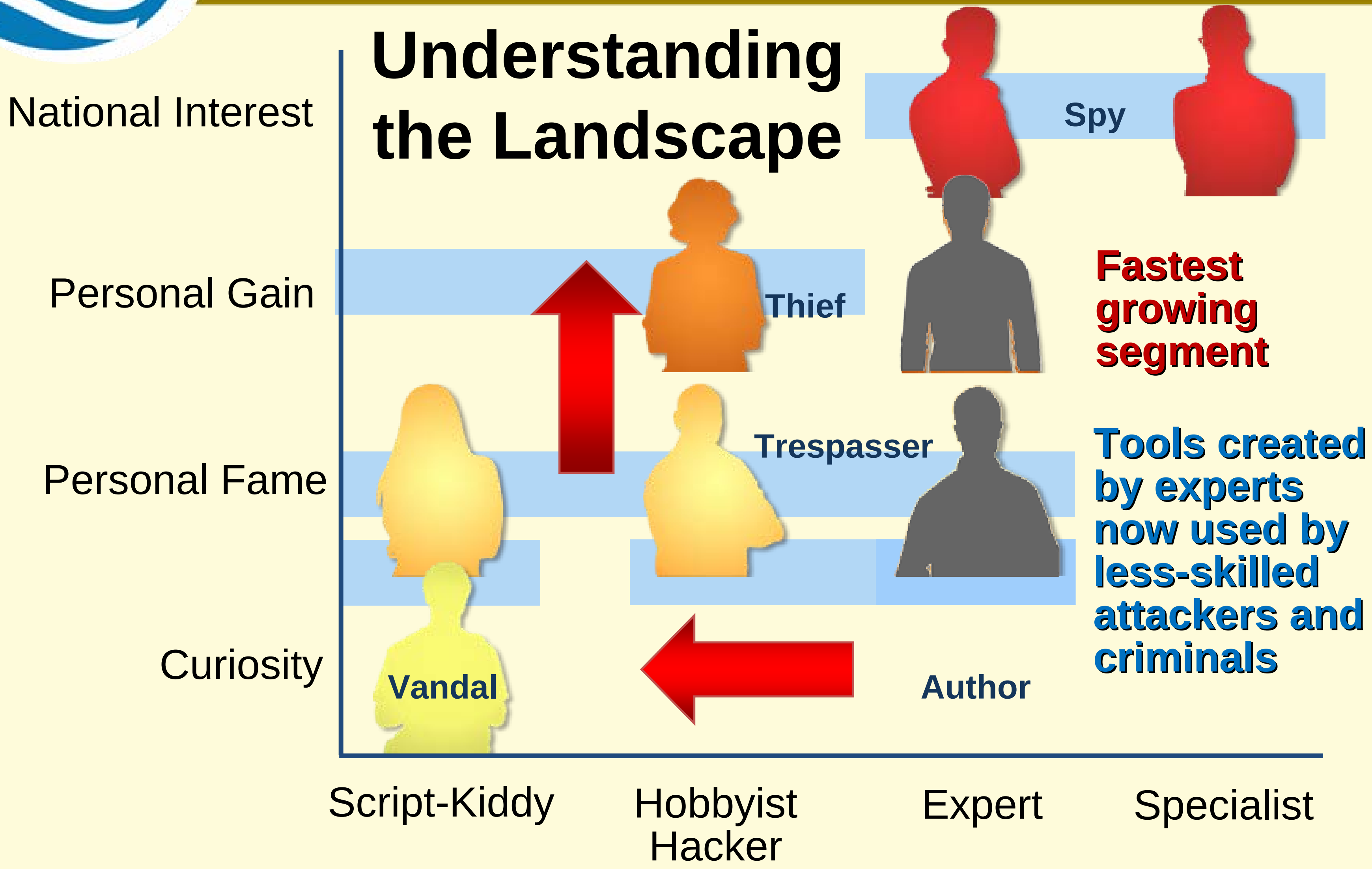
National Indian Gaming Commission

Information Technology Security: The Changing Threat Environment

Travis Waldo
IT Auditor
NIGC

Understanding the Landscape



Fastest growing segment

Tools created by experts now used by less-skilled attackers and criminals

How SAFE Are You?

- In **June**, about **6.5 million** cryptographic hashes of LinkedIn **user passwords were stolen and posted online**.
- After the LinkedIn fiasco, **dating site eHarmony also confirmed a breach of 1.5 million** passwords that were hacked.
- **Hacker gang Swagger Security** strikes again, this time **breaching the networks of Warner Bros. and China Telecom**, releasing documents and publishing login credentials.
- The **University of Nebraska in Lincoln** acknowledged a data breach that exposed information of **more than 654,000 files of personal information on students and employees**, plus parents and university alumni.
- Hactivist group **Anonymous brought down** the websites of trade groups **U.S. Telecom Association and TechAmerica**, apparently for their protest of the cyber security bill proposed by Congress.
- At least **228,000 Social Security numbers** were exposed in a **March 30 breach** involving a **Medicaid server** at the Utah Department of Health
- Online retailer **Zappos disclosed hackers had broken into its network** and stolen information on **customers, including name, address, credit-card numbers and** cryptographically **scrambled passwords** stored in hash form.

How SAFE Are We?

In June, 2012:

•**6.5 million** cryptographic hashes of **LinkedIn** user passwords were stolen and posted online

•**eHarmony** confirmed a breach of **1.5 million** passwords that were hasked.

•Swagger Security breached **Warner Bros**. and **China Telecom**, releasing private documents and publishing login credentials

•The **University of Nebraska** acknowledged a data breach that exposed information of more than **654,000** files of personal information on students, employees, parents and university alumni.

•Hactivist group Anonymous brought down the websites of trade groups **U.S. Telecom Association** and **TechAmerica** in protest of the cyber security bill proposed by Congress.

Recently:

•***At least* 228,000** Social Security numbers were exposed in a March 30 breach involving a Medicaid server at the **Utah Department of Health**

•**Zappos.com** admitted that hackers had broken into its network and stolen information on customers, including name, address, credit-card numbers and cryptographically scrambled passwords stored in hash form.

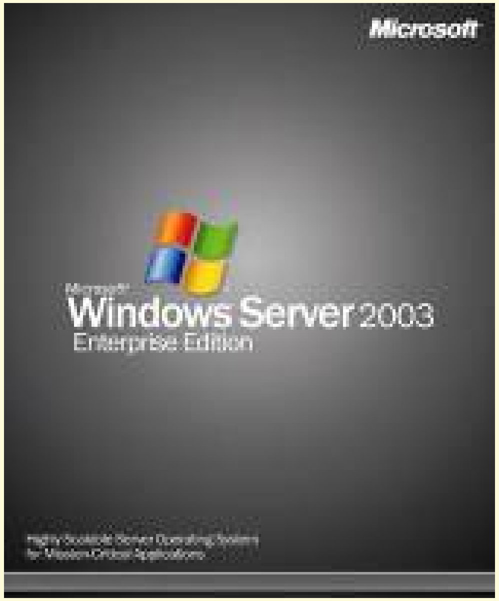
Honey Pot Projects

- Six computers attached to Internet
  - Different versions of Windows, Linux and Mac OS
- Over the course of one week
  - Machines were scanned 46,255 times
  - 4,892 direct attacks
- No up-to-date and patched operating systems succumbed to a single attack
- All non-updated systems were compromised
  - Windows XP with no patches
  - Infested in 18 minutes by Blaster and Sasser
  - Within one hour it became a "bot"

Source: StillSecure,
see http://www.denverpost.com/Stories/0,1413,36~33~2735094,00.html

Legacy and Environment

- **The security kernel of Windows NT was written-**
  - Before there was a World Wide Web
  - Before TCP/IP was the default communications protocol
- **The security kernel of Windows Server 2003 was written-**
  - Before buffer overflow tool kits were generally available
  - Before Web Services were widely deployed



Critical Threats

- 1. Social Engineering (phishing)
- 2. Spyware
- 3. Wireless Network Attacks
- 4. Rootkit
- 5. SQL Injection

Critical Threats

- ❑ **1. Social Engineering (phishing)**
- ❑ **2. Spyware**
- ❑ 3. Wireless Network Attacks
- ❑ 4. Rootkit
- ❑ 5. SQL Injection

Social Engineering

The art of convincing people to reveal confidential information.

Phases in a Social Engineering Attack

- **Research Target Company**
  Dumpster diving, websites, employees, tour company, etc.

- **Select Victim**
  Identify a frustrated employee

- **Develop Relationship**
  Build some type of personal relationship with the selected employee

- **Exploit**
  Collect sensitive personal information (kids' names, birthdays), financial information or current company technologies

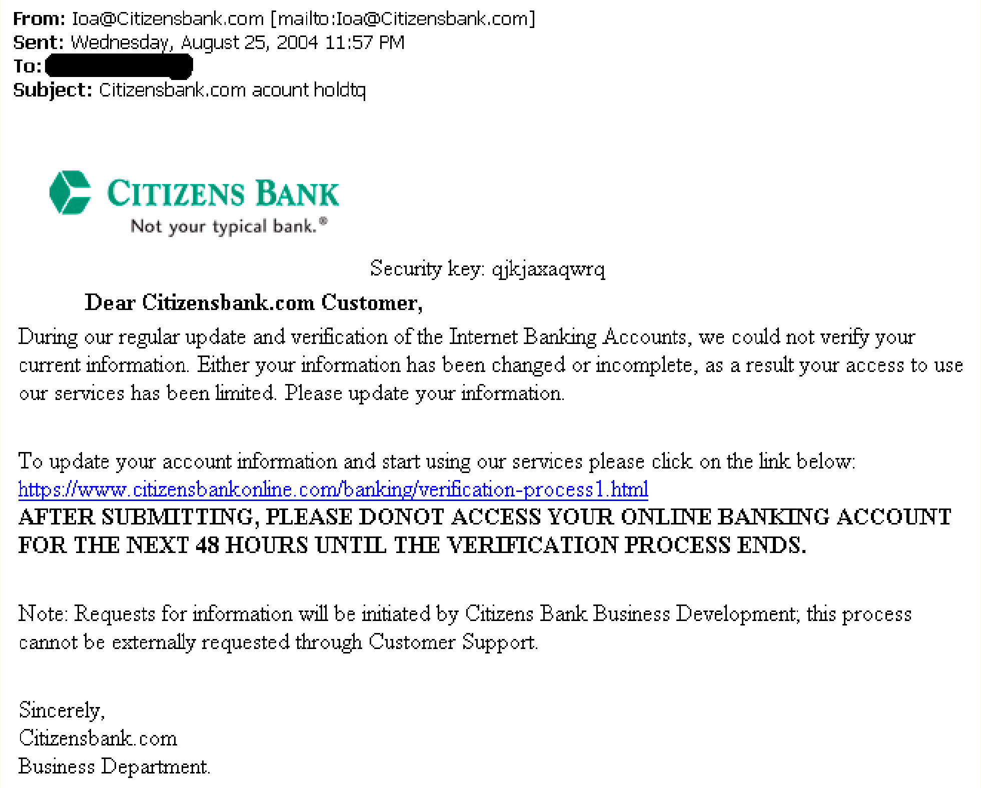
Social Engineering

Examples

Phishing

➢Designed to fraudulently obtain private information

➢Generally, does not involve personal contact, usually legitimate looking E-mail, websites, or other electronic means are involved in phishing attacks



From: Ioa@Citizensbank.com [mailto:Ioa@Citizensbank.com]
Sent: Wednesday, August 25, 2004 11:57 PM
To: [redacted]
Subject: Citizensbank.com acount holdtq

CITIZENS BANK
Not your typical bank.®

Security key: qjkjaxaqwrq

Dear Citizensbank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
https://www.citizensbankonline.com/banking/verification-process1.html
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citizens Bank Business Development; this process cannot be externally requested through Customer Support.

Sincerely,
Citizensbank.com
Business Department.

Social Engineering

Examples

Dumpster Diving
Trashing

Large amounts of information can be collected through company trash, such as:

company phone books - organizational charts – memos - company policy manuals

calendars of meetings - events and vacations - system manuals

printouts of sensitive data or login names and passwords - printouts of source code

disks and tapes - company letterhead and memo forms - outdated hardware

Social Engineering

Examples

On-Line Social Engineering

- ➢The Internet is fertile ground for social engineers looking to harvest passwords

- ➢Many users often repeat the use of one simple password on every account: Yahoo, Travelocity, Gap.com, etc.

- ➢Once the hacker has one password, he or she can probably get into multiple accounts

- ➢Large amounts of personal data on the social sites as well

Social Engineering

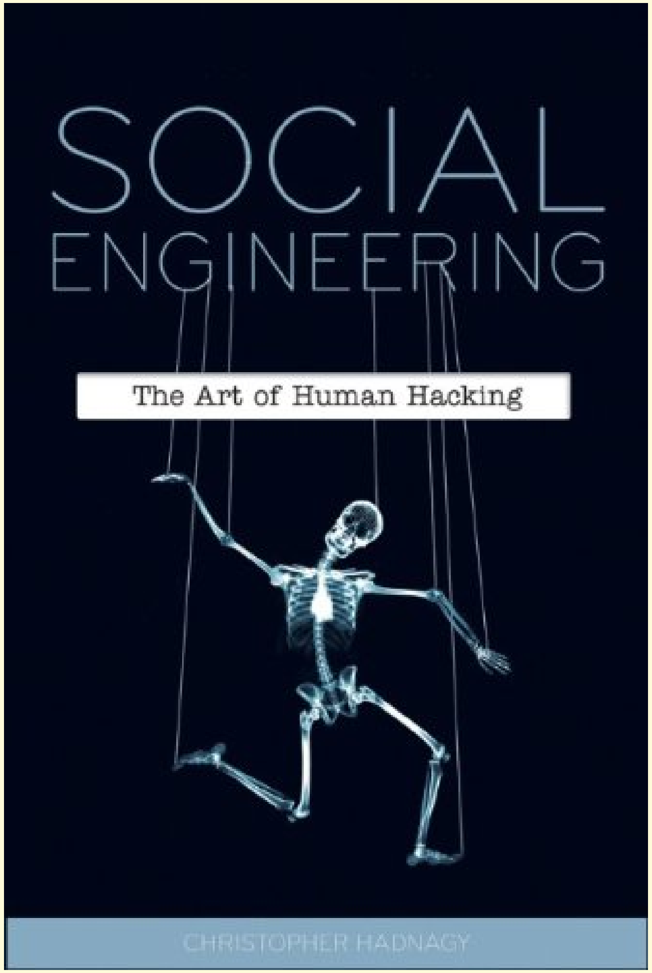
Examples

Persuasion

Hackers employ social engineering from a psychological point-of-view

Basic methods include:

- impersonation
- conformity
- diffusion of responsibility
- plain old friendliness

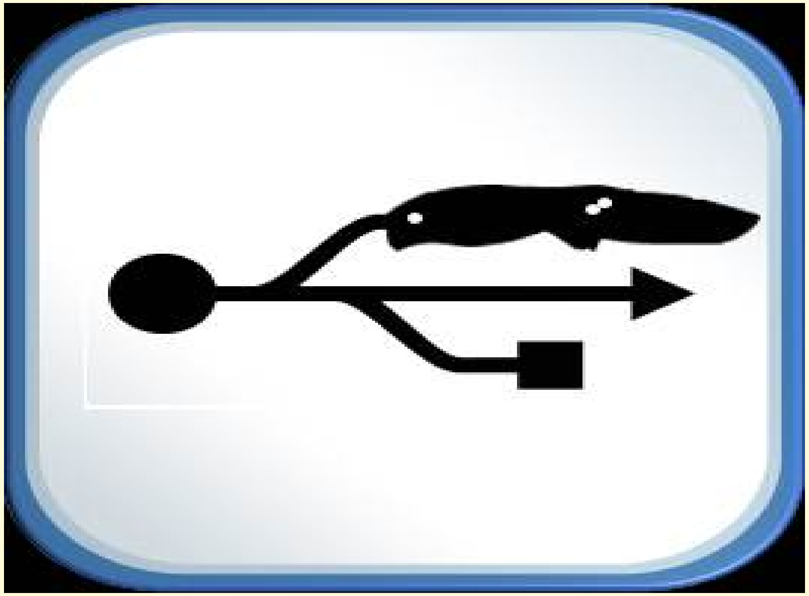


Social Engineering

Examples

Switchblade

This method uses the **Windows AutoRun** feature to run a program that silently infects the computer and steals data by running as a background task.



Critical Threats

✓ 1. Social Engineering (phishing)

✓ 2. Spyware

□ **3. Wireless Network Attacks**

□ 4. Rootkit

□ 5. SQL Injection

Wireless Network Attacks

Packet Sniffing

Def: The act of capturing packets of data flowing across a computer network. The software or device used to do this is called a packet sniffer. Packet sniffing is to computer networks what wiretapping is to a telephone network.

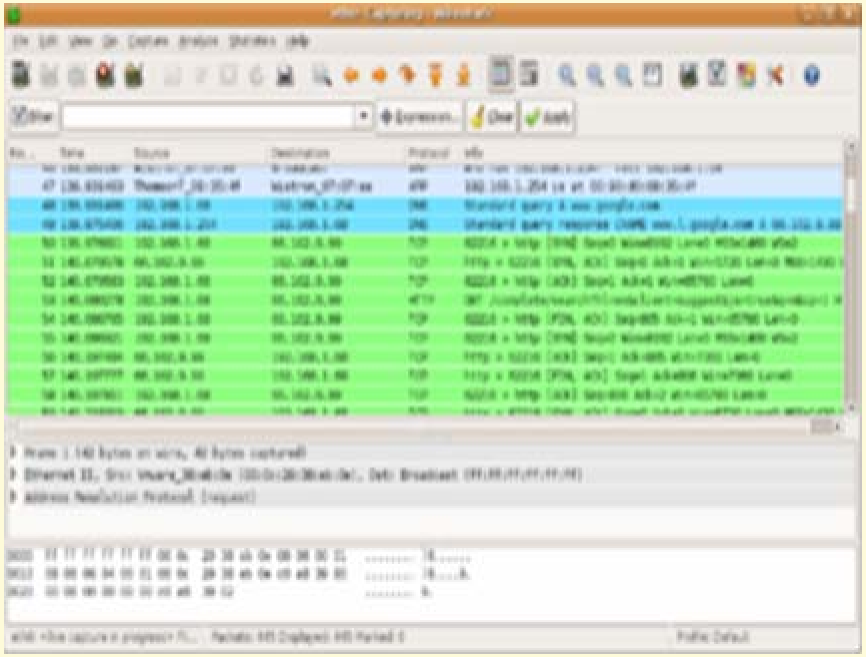
❖**Types of attacks**:

- DHCP Attacks
- ARP Poisoning
- Spoofing
- DNS Poisoning
- Password Capture

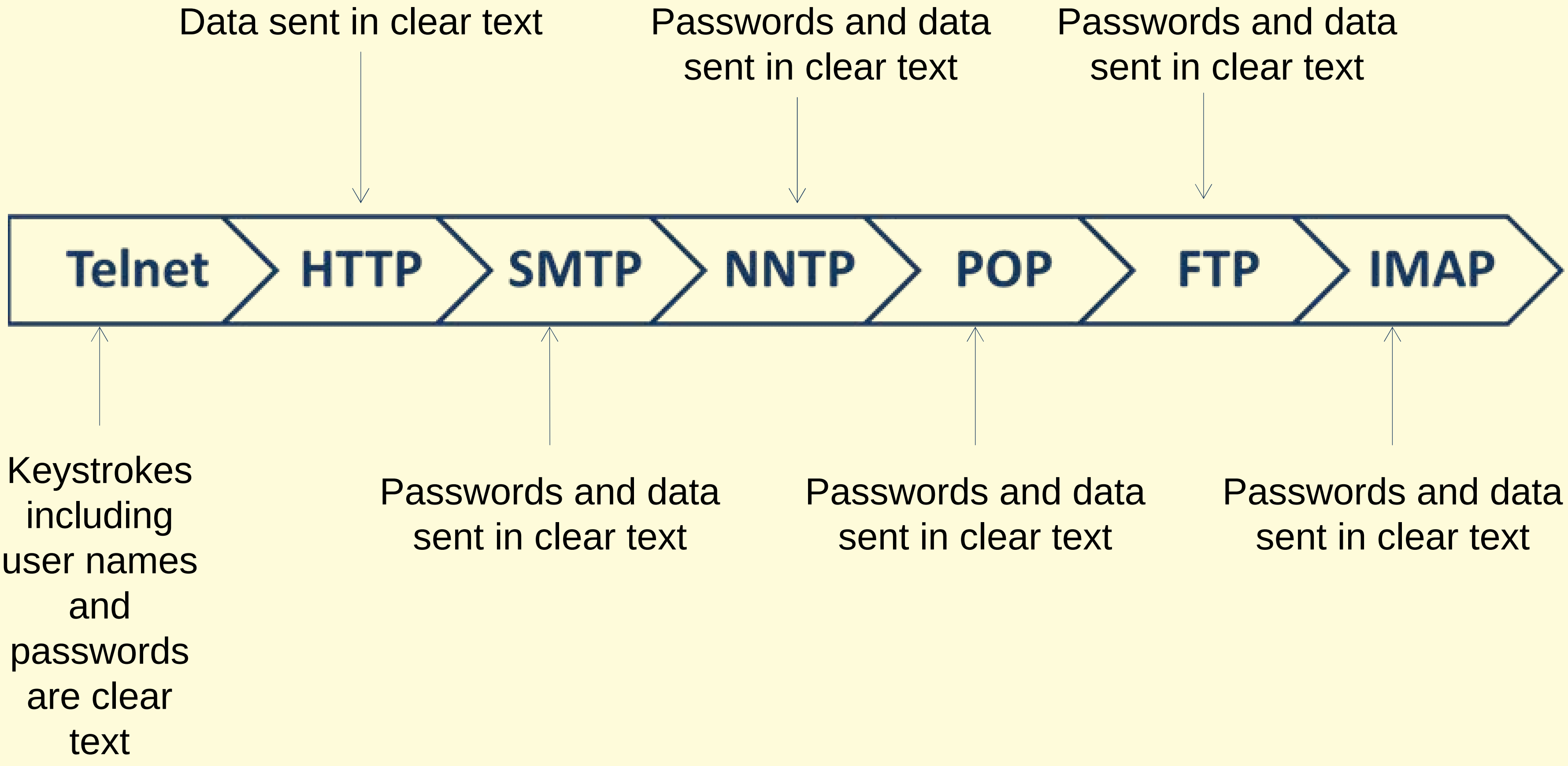
Network Hacking Tools

Packet Analyzers

- Network troubleshooting
- Analysis
- Software development
- Communications protocol development
- Education
- Graphical front-end
- Information sorting & filtering options
- Sees all traffic
- Puts network interface into promiscuous mode



Protocols Vulnerable to Sniffing



Telnet → HTTP → SMTP → NNTP → POP → FTP → IMAP

Telnet: Keystrokes including user names and passwords are clear text

HTTP: Data sent in clear text

SMTP: Passwords and data sent in clear text

NNTP: Passwords and data sent in clear text

POP: Passwords and data sent in clear text

FTP: Passwords and data sent in clear text

IMAP: Passwords and data sent in clear text

How do we defend against Sniffing?

- **Restrict** physical access to the network media to ensure that packet sniffer cannot be installed.
- Use **encryption** to protect confidential information.
- **Permanently** add the MAC address of the gateway to the ARP cache.
- Use **static IP address and static APR tables** to **prevent attackers** from adding the spoofed ARP entries for the machines in the network.
- **Turn off** network identification broadcasts and if possible, restrict the network to authorized users.
- Use **IPv6** instead of IPv4 protocol.
- Use **encrypted** sessions such as:
  - SSH instead of Telnet
  - Secure Copy (SCP) instead of FTP
  - SSL for e-mail connection, etc.

Critical Threats

- ✓ 1. Social Engineering (phishing)
- ✓ 2. Spyware
- ✓ 3. Wireless Network Attacks
- □ **4. Rootkit**
- □ 5. SQL Injection

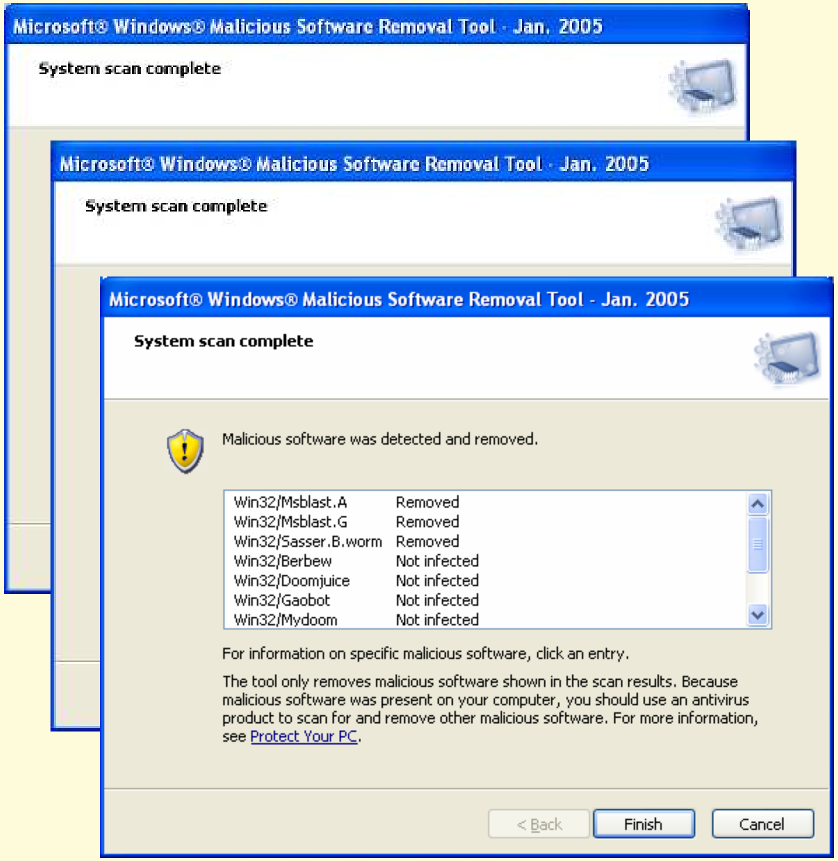
What are Rootkits?

- A **Rootkit** is a stealthy type of software, often **malicious**, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued **privileged access** to a computer system.

- Installation can be automated, or an attacker can install it once they've obtained root or Administrator access by -
  - Cracking the system
  - Privilege escalation
  - Social engineering

How do we defend against Malicious Software?

- Install antivirus software
- Install a firewall
- Update the operating system regularly to the latest patches and service packs
- Install antimalware software



Microsoft® Windows® Malicious Software Removal Tool - Jan. 2005

System scan complete

Microsoft® Windows® Malicious Software Removal Tool - Jan. 2005

System scan complete

Microsoft® Windows® Malicious Software Removal Tool - Jan. 2005

System scan complete

Malicious software was detected and removed.

Win32/Msblast.A	Removed
Win32/Msblast.G	Removed
Win32/Sasser.B.worm	Removed
Win32/Berbew	Not infected
Win32/Doomjuice	Not infected
Win32/Gaobot	Not infected
Win32/Mydoom	Not infected

For information on specific malicious software, click an entry.

The tool only removes malicious software shown in the scan results. Because malicious software was present on your computer, you should use an antivirus product to scan for and remove other malicious software. For more information, see Protect Your PC.

Critical Threats

- ✓ 1. Social Engineering (phishing)
- ✓ 2. Spyware
- ✓ 3. Wireless Network Attacks
- ✓ 4. Rootkit
- □ **5. SQL Injection**

What is a SQL Injection?

- *Def*.: a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a Web application for execution by a backend database.
- SQL Injection is the **most common website vulnerability**
- **Most programmers are still not aware of this threat**

SQL Injection Attacks on the Rise

A few recent examples:

- November 2010: the **British Royal Navy** website was compromised
- December 2010: CitySights New York tour company had **100,000 bank card numbers** stolen
- March 2011: **TripAdvisor** (an Expedia company) had part of its membership list stolen
- March 2011: **Oracle's MySQL website was compromised** via a SQL injection attack with user accounts and passwords being accessed

Risks of SQL Injection Attacks

- **Authentication Bypass-** the attacker logs onto an application without providing valid username and password and gains admin privileges.
- **Information Disclosure-** the attacker obtains sensitive information that is stored in the database e.g. player account information.
- **Compromised Data Integrity-** deface webpage, insert malicious content, or alter the contents of a database.
- **Compromised Availability of Data-** delete the database information, delete logs, or audit information contained in a database.
- **Remote Code Execution-** compromise the host operating system.

How to Defend Against SQL Attacks

- **Run** database service account with minimal rights
- **Disable** commands like xp_cmdshell
- **Suppress** all error messages
- Use **custom error** messages
- Use low privileged account for DB connection
- **Filter** all client data
- **Use only stored procedures** to validate user input
- **Use SQL Injection Detection tools**

QUESTIONS???