Internet Attacks

Types of attacks

• Social engineering
  – Fooling the victim for fun and profit
• Impersonation
  – Stealing access rights of authorized users
• Exploits
  – Exploiting a hole in software or operating systems
Types of attacks (cont)

- Transitive trust
  - Exploiting host-host or network-network trust
- Data driven
  - Trojans, trapdoors, viruses
- Infrastructure
  - Taking advantage of protocol or infrastructure features or bugs

Types of Attacks (cont)

- Denial of service
  - Preventing system from being used
- Magic
  - New things nobody has seen yet
Social engineering

- Example #1:
  - Email sent to users from “root” to users on large academic network
  - “please change your password to ‘fooble’”
  - Attacker then logs in as user from over network
  - System bugs exploited to gain complete run of system

Social engineering

- Example #2:
  - Attacker calls switchboard and impersonates employee “this is Dr. XXX trying to reach the data center.”
  - Calls data center “this is Dr. XXX -- my modem is not working, has the modem pool ## changed?”
  - Gets modem pool phone ## and name of system manager from data center operator
Social engineering (cont)

– Calls computer room, “this is <system manager> - I’ve accidentally locked myself out of the Sun, can you do the following on the console for me?...”
– Dials in and logs in

Social engineering

• Very hard to protect against
• How to protect against it:
  – Educate staff
  – Have well-known mechanisms for problem reporting and handling
  – Identify transactions that must be done in person
Impersonation

• Example #1:
  – User telnets into network from terminal room at a trade show
  – Attacker with network sniffer (tcpdump, nitsniff, etc) at trade show or network captures complete login session
  – Attacker later logs into system with user-id and stolen password

Impersonation

• Example #2:
  – College students place RS-232 tap on serial lines between modem closet and computer room
  – Late-night monitoring set up at cross-wired terminal
  – System manager logs in and sets privilege
  – Attacker later logs into system with stolen passwords
Impersonation

- “two factor” authentication: something you have + something you know
- It is hard to steal a physical token over a network or a telephone!
- Applications may encrypt data to protect traffic (e.g.: encrypted TELNET sessions)

Exploits

- Example #1:
  - Sendmail process runs with system privileges
  - Mail to invalid user-id triggers “bounce” message return-to-sender
  - Attacker sends a message to invalid recipient that appears to have come from a program invocation
Exploits (cont)

– Mailer dutifully “bounces” message to program and executes attackers commands with privileges

To: fishlips@target.com
From: “| /bin/sed ‘1,/^$/d’ | sh”

Exploits

• Badly written software is the norm
• Most software has security added as an afterthought (once it’s too late to design it right)
• Too many programs run with excessive privileges
• Few programs take advantage of system’s underlying security features
Transitive trust

• Example #1:
  – Entire network set up with ".rhosts files" so that users can log in from “trusted” hosts w/o giving a password
  – One user has a ".rhosts" file that trusts a host on a different network
  – Attacker compromises remote network

Transitive trust (cont)

  – Attacker scans all user command history files for invocations of the “rlogin” command and discovers the user who habitually accesses remote network
  – Attacker compromises user’s account and now has foothold in an entirely new network
  – Attacker island-hops from network to network
Transitive trust

• Example #2:
  – Network of workstations share files via NFS
  – Attacker compromises a client workstation’s administrator account
  – Attacker can create privileged executables on file systems exported from server

Transitive trust (cont)

– Attacker creates privileged executable on server then logs in as normal user
– Attacker executes privileged program and gains privilege on file server
Transitive trust

- Current software suites do not have adequate mechanisms for trust delegation and containment
- System admins must carefully map out trust relationships between hosts on networks
- Consider “internal firewalls”

Data driven attacks

- Example #1:
  - Attacker mails victim user a PostScript file with file operations in it
  - Victim displays it on workstation with a PostScript interpreter
  - PostScript interpreter executes file operations which add attacker’s host to user’s “.rhosts” file
  - Attacker logs into user’s account
Data driven attacks

- Example #2:
  - Attacker on IRC (Internet Relay Chat) tells “newbie” users to obtain a utility program that will help them use system better
  - Users download program and run it
  - Program deletes all user’s files and emails a copy of password file to attacker

Web Pages we’d like to see:

Click Here to Infect Your Machine
Data driven attacks

- Firewall can help screen out some
- Restricting services can help reduce potential for attack
- Educate users about not just executing anything they are given

Infrastructure attacks

- Example #1: (“DNS Spoofing”)
  - Attacker compromises a system that is name server for a network
  - Victim has a host called “foo.victimdomain.com” in their “.rhosts” file
  - Attacker sets up a name mapping from the address of one of his systems to “foo.victimdomain.com”
  - Attacker uses rlogin to gain access
DNS spoofing

- When building a system do not rely on DNS for making security critical decisions
- Programs like tcp_wrappers do “double reverse lookup” which makes it harder to mount attack
- Most firewalls use DNS information only for routing mail and user services

Infrastructure attacks

- Example #2: (“ICMP bombing”)
  - ICMP (Internet Control Message Protocol) is used by routers to notify a host when a destination is unreachable
  - Attacker can “knock a machine off the air” by sending ICMP to target system telling it that a destination is not available
  - Tools for this are widely available (e.g.: “nuke” “icmpbomb”)
ICMP bombing

- Most firewalls block ICMP into and out of network
- Firewalls that are a single point of connectivity correctly interpret ICMP without letting it through
- Unfortunately ICMP is also used to legitimate purposes (e.g., “ping” - ICMP echo request)

Infrastructure attacks

- Example #3: (“Source Routing”)
  - IP protocol specifies that source-routed traffic should return on the reverse route from which it came
  - Attacker selects a trusted host within the target network and knocks it off the air using ICMP bombing
  - Attacker sets address of his system to that of the trusted host
Infrastructure attacks (cont)

- Attacker uses rlogin or TELNET with source routed packets
- Target host sees packets coming from trusted machine and may permit better access

Source Routing

1: attacker zaps trusted host
2: attacker sends traffic as trusted host
3: return traffic follows source route
Source Routing

- Defeat source routing with firewalls that block and log source routed packets
- Many routers can block source routed packets
- Tools like tcp_wrappers detect source-routed traffic and trigger alarms

Infrastructure attacks

- Example #4: (“TCP sequence guessing” or “the Mitnick Attack”)
  - TCP connections rely on an increasing sequence number to correctly order traffic over connection
  - When connection is created, a new semi-random sequence number is used
Infrastructure attacks (cont)

- If an attacker knows the sequence numbers of a connection stream he can generate correct-looking packets even though the response packets do not reach him.
- In order for attack to work response packets must not reach the correct destination.

Sample TCP Session

```
Host A          Host B
SYN (initial sequence # =x)  
SYN, ACK (initial sequence # =y)  
ACK  
ACK
```
TCP Sequence guessing

• Phase #1:
  – Victim is behind a router-based firewall that allows through all traffic originating from victim network
  – Router firewall also permits incoming traffic on SMTP service port to target network
  – Attacker “gags” trusted host by initiating a number of partial TCP connection requests

Sequence guessing: phase #1

1.1: attacker masks off trusted host with a sequence of half-open connection requests
TCP sequence guessing

- Phase #2:
  - Attacker generates a number of connection attempts against target system’s SMTP port from an outside machine
  - Attacker notes down sequence numbers of the connections as they are created

Sequence guessing: phase #2

2.1: attacker makes connection requests and notes down sequence numbers
TCP sequence guessing

• Phase #3:
  – Attacker computes sequence numbers that will be assigned to next connection
  – Attacker generates packets from outside machine with source address of inside trusted machine
  – Generated packets have correct sequence numbers for client side of dialog

TCP sequence guessing (cont)

  – Target machine thinks it has received an “rsh” command from trusted inside machine and executes it, adding a line to the password file
Sequence guessing: phase #3

3.1: attacker creates traffic with correct sequence number appearing to originate from trusted host
3.2: router permits traffic because it appears to have originated on target network
3.3: target system executes command because it appears from trusted host

TCP sequence guessing

- Most dual-homed firewalls immune to sequencing since they block all traffic to inside network
  - Impossible to “jam” nodes on inside
- Correctly configured routers can prevent sequence guessing
  - Router should not let “in” traffic claiming to come from “inside”
Infrastructure attacks

- Example #5: (“TCP splicing”)
  - Attacker between networks watches for a legitimate connection
  - Waits until after user has logged in
  - “Steals” connection and becomes user
- Negates protections provided by authentication tokens!

TCP splicing

- Phase #1:
  - Attacker between networks identifies a connection to steal
  - Monitors connection until user has logged in
  - Starts recording packet sequence numbers
TCP splicing: phase #1

1.1: user logs into destination across network
1.2: attacker observes login and records packet sequence numbers

TCP splicing

- Phase #2:
  - Attacker jams user’s machine
  - User’s machine closes connection unilaterally
  - User sees his login disconnected
TCP splicing: phase #2

2.1: attacker jams user’s machine

2.2: user sees login session hang or die

TCP splicing

• Phase #3:
  – Attacker resumes sending packets with correct sequence numbers
  – Remote system does not realize anything has happened and keeps communicating with attacker
TCP splicing: phase #3

3.1: attacker generates correctly sequenced packets appearing to come from user’s machine
3.2: user’s destination keeps sending return packets to user’s machine which does not see them because it is jammed
3.3: attacker keeps monitoring traffic on stolen session

TCP splicing

- Application level encryption is effective solution since attacker cannot generate traffic that will decrypt to meaningful data

This attack has not been widely seen - yet
Infrastructure attacks

- Example #6: ("FTP bouncing")
  - Attacker locates a trusted system that is running an FTP server with upload capability
  - Uploads a file of commands or data
  - "Bounces" the download to a different system for delivery
- This may work through some firewalls!

FTP Bouncing

- Phase #1:
  - Attacker locates an FTP server behind a firewall
  - FTP server has a writeable upload area
  - Attacker generates (in this example) an SMTP dialog of a spoofed mail message
  - Attacker uploads the message
FTP Bouncing: phase #1

1.1: attacker identifies an FTP server with writable upload area

HELLO mumble.com
MAIL From: president@whitehouse.gov
RCPT To: victim
DATA
Joe, you ignorant splut.
Signed, Bill.
QUIT

1.2: attacker generates an SMTP dialog file and uploads it to the FTP server

FTP Bouncing

• Phase #2:
  – Attacker FTPs to the FTP server and sends a PORT command
    • PORT’s IP address is that of the victim system
    • PORT’s IP port is the SMTP port
  – FTP server opens connection to victim system and informs attacker “OK”
FTP Bouncing: phase #2

2.1: attacker issues a PORT command with the target’s address and SMTP port: PORT 16, 67, 32, 1, 9, 25

2.2: FTP server opens connection to target machine port 25 and informs attacker “OK”

FTP Bouncing

• Phase #3:
  – Attacker sends a RETR command specifying the data file containing the SMTP dialog
  – FTP server dutifully transmits the file to the previously opened port
    • Fake Email is sent
    • Email appears to originate on FTP server
    • FTP server logs may not reveal the attack
FTP Bouncing: phase #3

3.1: attacker issues a RETR command filename of SMTP commands uploaded earlier

3.2: FTP server transmits the file to the target machine, thereby sending a mail message

FTP Bouncing

• FTP bouncing makes address-based verification difficult
  – FTP servers may now provide launching points for attack
  – Many Windows/PC based FTP servers can easily be used to issue bounce attacks
• Implication: Externally reachable FTP servers **must** be carefully managed!
Infrastructure attacks

- Example #7: (“Racing Authentication”)
  - Authentication systems that rely on a unidirectional dialog may be spoofed by an attacker
  - Attack is based on typing faster than the victim and guessing the last digits/letters of passwords
- Defeats many tokens and one-time password schemes

Racing Authentication

- Phase #1:
  - Attacker is in a position to sniff user logging in with SecurID, S/Key or similar authentication token
  - Watches user input keystrokes one at a time, duplicating them in a duplicate login attempt
Racing Auth: phase #1

1.1: user starts to log in with SecurID

1.2: attacker “mirrors” user’s login attempt

1.3: user starts to enter SecurID keycode

Racing Authentication

• Phase #2:
  – Attacker waits until user is ready to enter the final digit of their SecurID code
  – Attacker takes a guess and picks a number and enters it first
  – Odds are 1 in 10 that a successful login will be granted to attacker
  – Normal user thinks he just made a typo
Racing Auth: phase #2

2.1: attacker waits until user enters second to last digit
2.2: attacker guesses last digit and enters it before user does

One time in 10 attacker gets in!

Racing Authentication

- Racing authentication does not work on challenge/response or signature based authentication systems
- Can also be prevented by authentication servers that do not allow a user to be in the process of logging in from more than one terminal simultaneously
Denial of service attacks

• Example #1:
  – Attacker ICMP bombs router off the network
  or
  – Attacker ICMP bombs router at service provider off the network

Denial of service attacks

• Example #2:
  – Attacker floods network link with garbage packets
  or
  – Attacker floods mail hub with junk mail
SYN Flooding

- Deny legitimate users service by jamming the target machine with half-open TCP sessions
  - Eventually connections may get through but it disrupts service and causes long timeouts
  - Many hacker tools for SYN flooding are now on the ‘net
Syn Flooding

1: attacker issues a flood of SYN packets and ignores responses

2: legitimate user’s connection may not get through

SYN Flooding

• Most responses to SYN flooding are quick and dirty fixes
  – Increase buffer and queue sizes
  – Generate automatic RST packets to clear jamming

• SYN flooding type attacks will always be technically feasible
Denial of service attacks

- Few things network administrator can do to protect against it
  - Attacker can always attack “upstream” of point of connection and interrupt service
- Internet protocols are designed to withstand single points of failure
  - Cannot handle active attackers on network that introduce multiple failures

Magic attacks

- We don’t know what these will look like
- They’re the attack that someone hasn’t thought of yet
- Attack will be utterly mysterious in origin and will surprise everyone
- Hopefully it will be easy to fix
What does the future hold?

- Host-based software will continue to be buggy and unreliable from a security standpoint
- Vendors will continue to add security as an afterthought rather than designing it in from the beginning
- Encryption will be more widely deployed in spite of government restrictions

Summary

- Attackers are performing active R&D to figure out how to break into networks
- Some attacks very technical
- Some attacks very low tech