Internet Attacks

1

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

2

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

3

Types of Attacks *(cont)*

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

4

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

5

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

6

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

7

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

8

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

9

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

10

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)

11

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

12

Exploits *(cont)*

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

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

13

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

14

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

15

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

16

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

17

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

18

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”

19

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

20

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

21

Web Pages we’d like to see:

Click Here
to
Infect Your Machine

22

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

23

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

24

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

25

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”)

26

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)

27

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

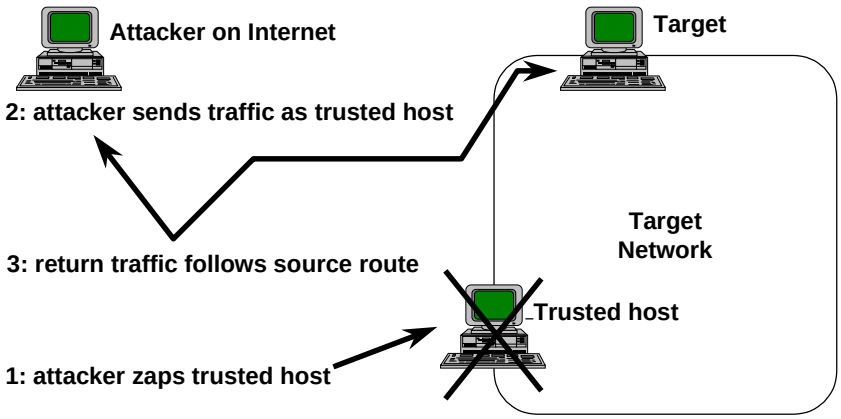
28

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

29

Source Routing



30

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

31

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

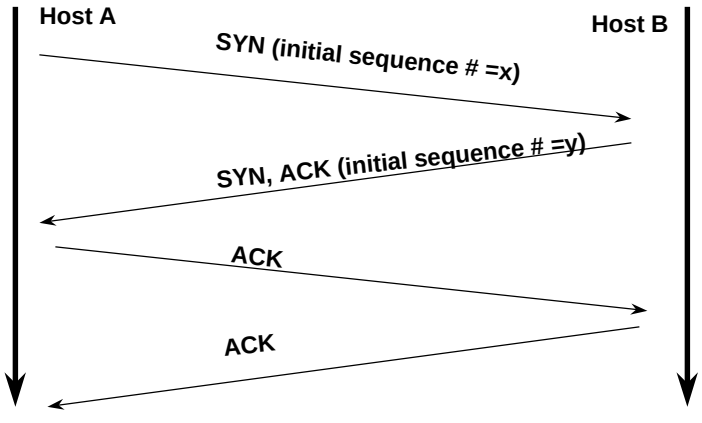
32

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

33

Sample TCP Session



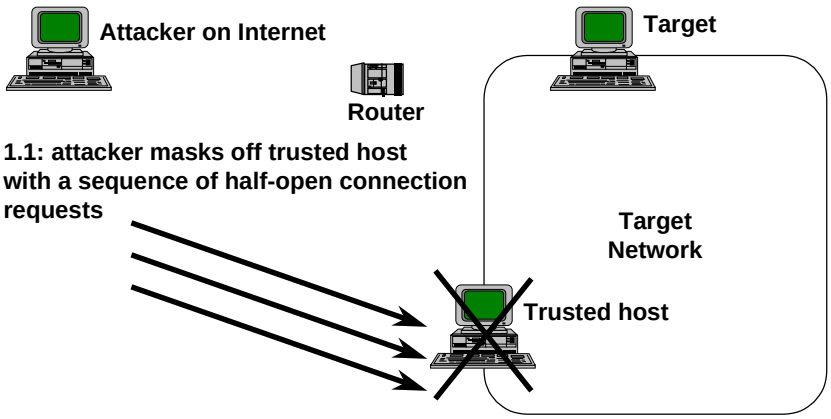
34

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

35

Sequence guessing: phase #1



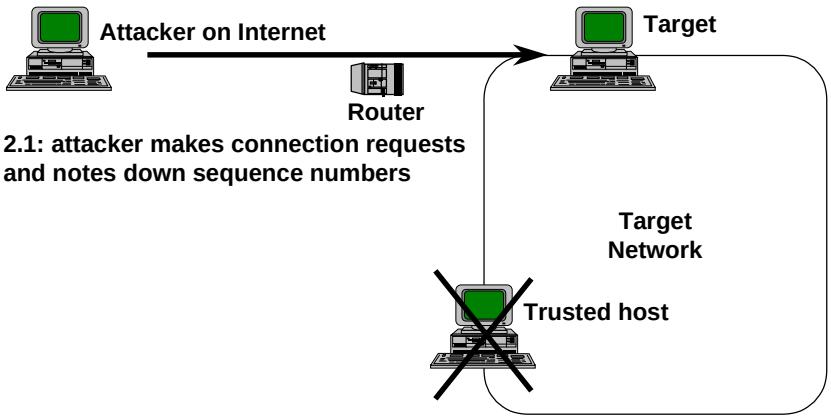
36

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

37

Sequence guessing: phase #2



38

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

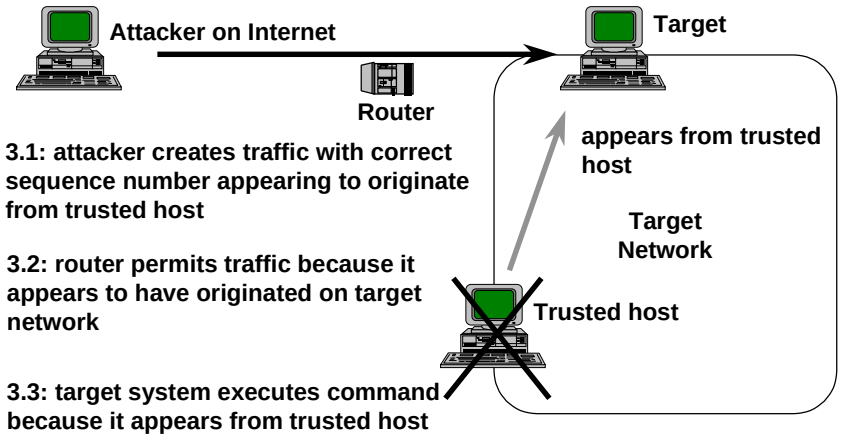
39

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

40

Sequence guessing: phase #3



41

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”

42

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!

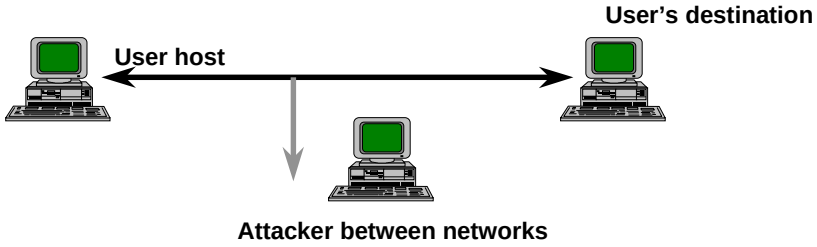
43

TCP splicing

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

44

TCP splicing: phase #1



1.1: user logs into destination across network

1.2: attacker observes login and records packet sequence numbers

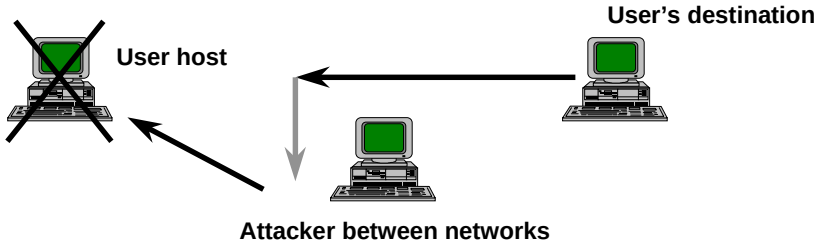
45

TCP splicing

- Phase #2:
  - Attacker jams user's machine
  - User's machine closes connection unilaterally
  - User sees his login disconnected

46

TCP splicing: phase #2



2.1: attacker jams user's machine

2.2: user sees login session hang or die

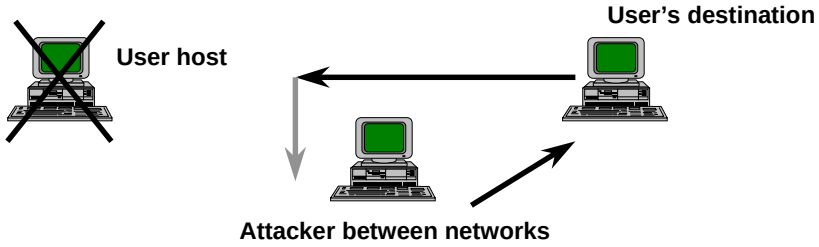
47

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

48

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

49

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

50

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!

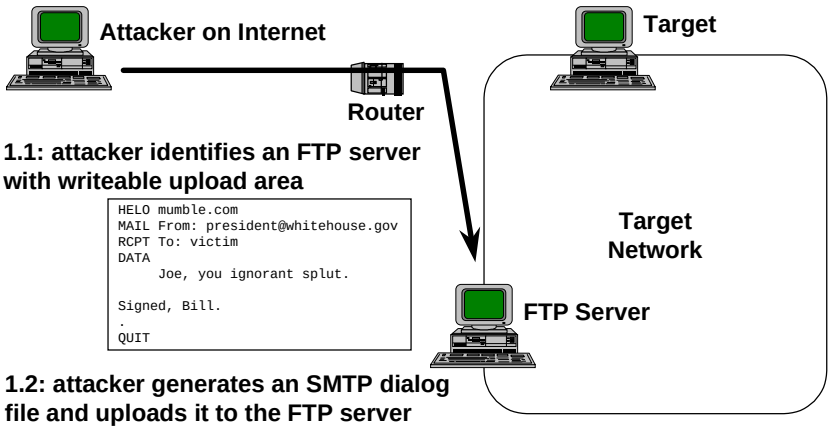
51

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

52

FTP Bouncing: phase #1



1.1: attacker identifies an FTP server with writeable upload area

```
HELO 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

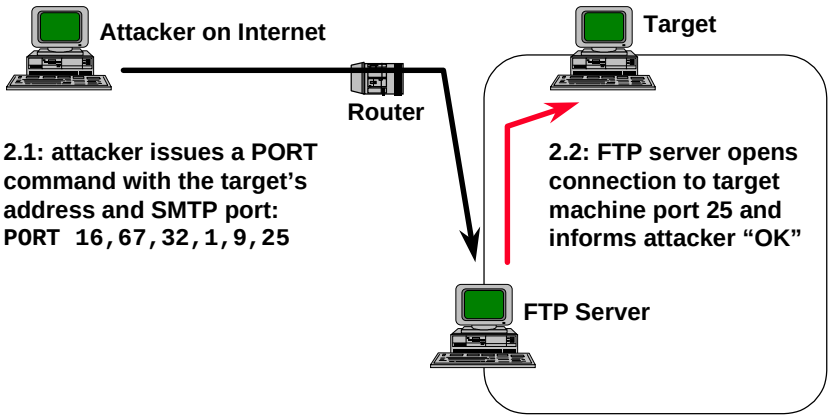
53

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"

54

FTP Bouncing: phase #2



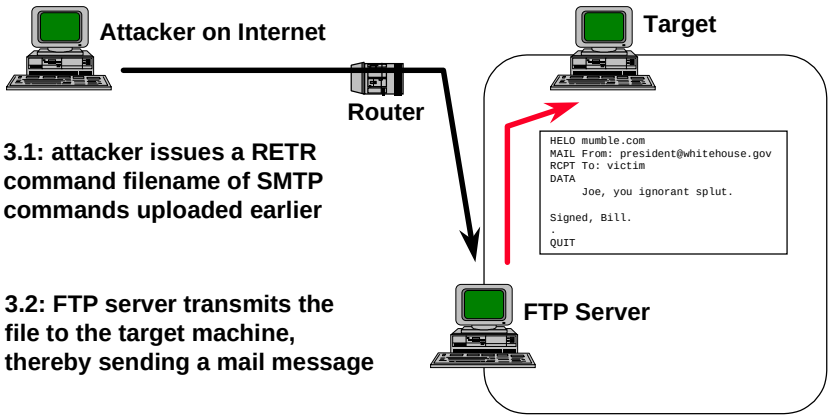
55

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

56

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

57

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!

58

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

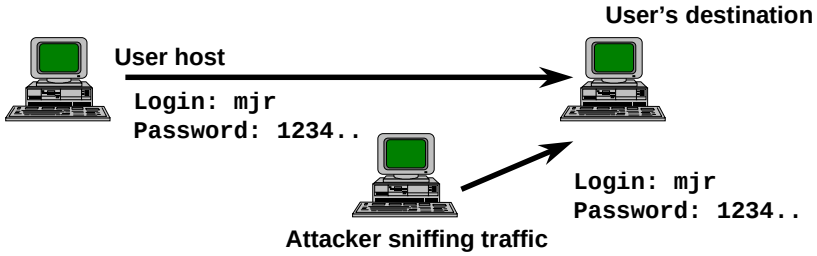
59

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

60

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

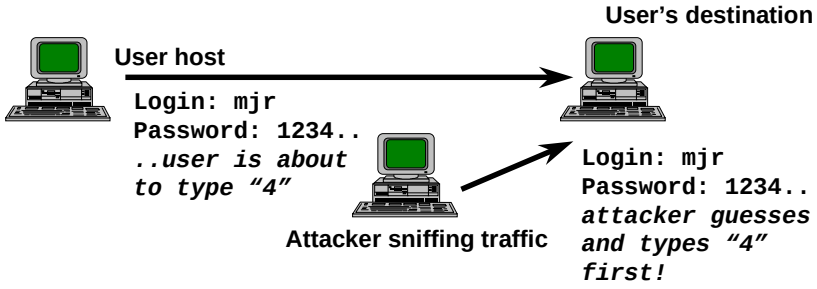
61

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

62

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!

63

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

64

Denial of service attacks

- Example #1:
  - Attacker ICMP bombs router off the network

  or
  - Attacker ICMP bombs router at service provider off the network

65

Denial of service attacks

- Example #2:
  - Attacker floods network link with garbage packets

  or
  - Attacker floods mail hub with junk mail

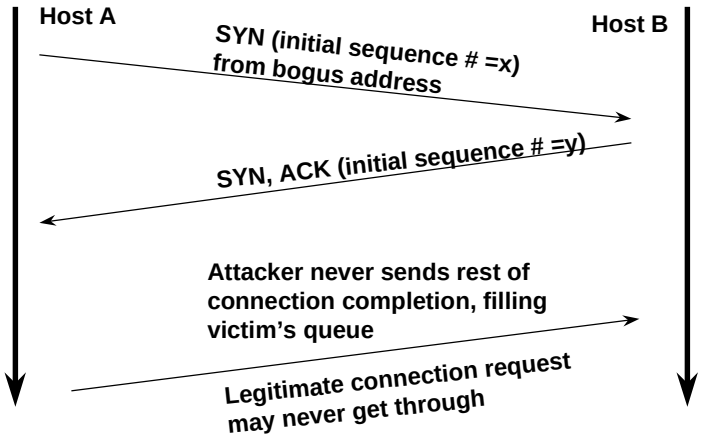
66

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

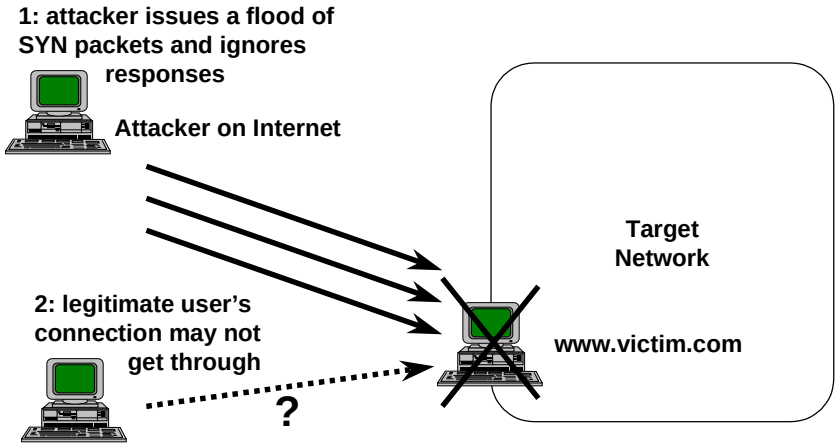
67

SYN flooding a TCP Session



68

Syn Flooding



69

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

70

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

71

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

72

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

73

Summary

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

74