

# TCP/IP Security Attacks

Raj Jain  
Washington University in Saint Louis  
Saint Louis, MO 63130  
[Jain@cse.wustl.edu](mailto:Jain@cse.wustl.edu)

These slides are available on-line at:

<http://www.cse.wustl.edu/~jain/cse571-09/>



1. TCP Segment Format, Connection Setup, Disconnect
2. IP: Address Spoofing, Covert Channel, Fragment Attacks, ARP, DNS
3. TCP Flags: Syn Flood, Ping of Death, Smurf, Fin
4. UDP Flood Attack
5. Connection Hijacking
6. Application: E-Mail, Web spoofing

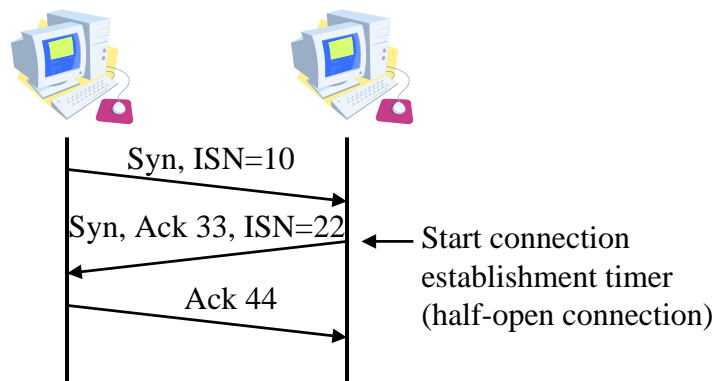
## TCP Segment Format

Source Port					Destination Port				
Sequence Number									
Ack Number									
Data Offset	Res	Urg	Ack	Push	Reset	Syn	Fin	Window	
Checksum					Urgent Pointer				
Options							Padding		
Data									

- ❑ Urgent: Deliver immediately at destination
- ❑ Push: Leave source immediately
- ❑ First data byte is ISN+1. Ack is next byte expected.  
Expecting Ack to Ack+window-1 next.

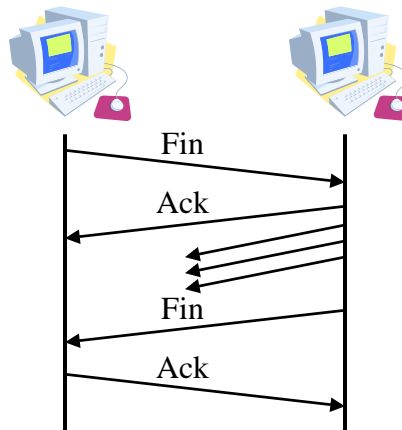
## TCP Connection Setup

- ❑ Three way handshake



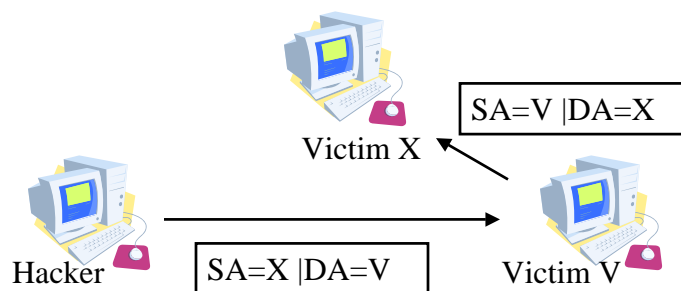
## TCP Disconnection

- Fin  $\Rightarrow$  No more data. Connection can be closed.
- Four-way handshake



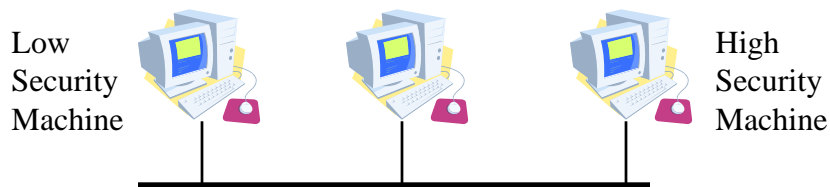
## IP Address Spoofing

- Send requests to server with someone X's IP address. The response is received at X and discarded. Both X and server can be kept busy  $\Rightarrow$  DoS attack



## Covert Channel

- ❑ **Loki** - a client server application,
  - Uses ICMP echo to send covert commands
  - <http://xforce.iss.net/xforce/xfdb/1452>
- ❑ **Timing Channel** - CPU load indicates a 0 or 1  
(Two processes on the same machine)
- ❑ **Storage Channel** - Print queue length large = 1, small=0



## IP Fragment Attacks

- ❑ Fragments can overlap
- ❑ Final packets can be too large

## TCP Flags

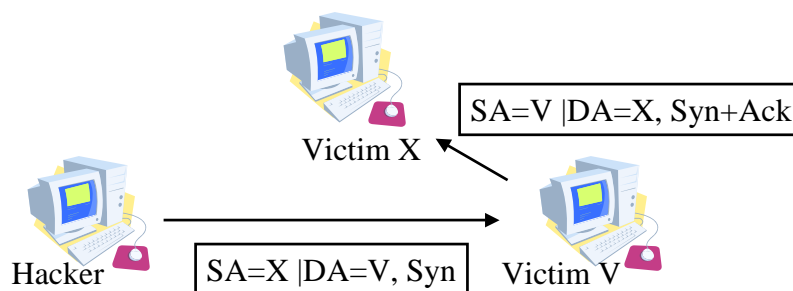
- Invalid Combinations

Syn	Fin	Psh	Rst
1	1	0	0
1	1	1	0
1	1	0	1
1	1	1	1

- May cause recipient to crash or hang

## Syn Flood

- A sends Syn request with IP address of X to Server V.
- V sends a syn+ack to X
- X discards syn+ack leaving an half open connection at V.
- Many open connections exhausts resources at V  $\Rightarrow$  DoS



## Ping of Death

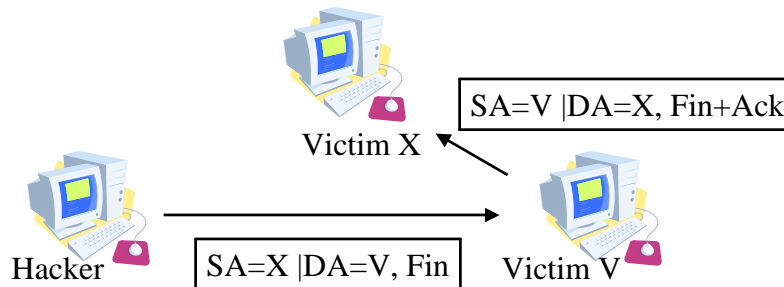
- Send a ping with more than 64kB in the data field.
- Most systems would crash, hang or reboot.

## Smurf

- Send a broadcast echo request with the V's source address.
- All the echo replies will make V very busy.

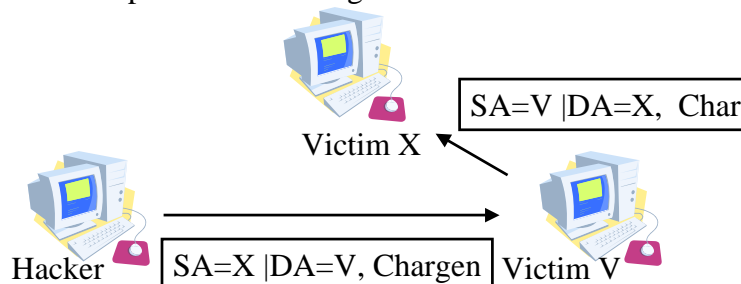
## Fin

- ❑ In the middle of conversation between X and V.
- ❑ H sends a packet with Fin flag to V.
- ❑ V closes the connection and disregards all further packets from X.
- ❑ RST flag can be used similarly



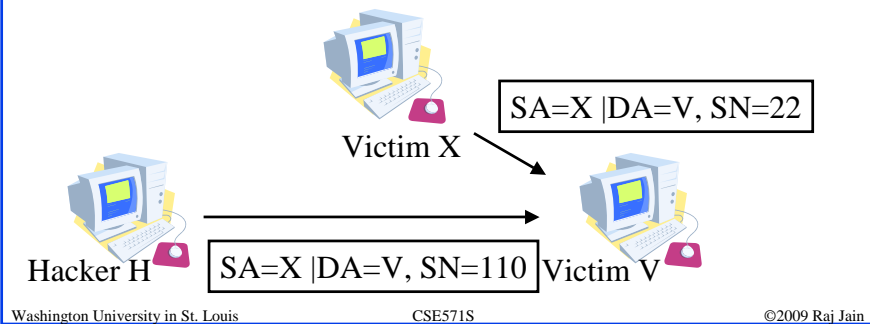
## UDP Flood Attack

- ❑ Character Generator (Chargen) request results in a response with random characters being returned.
- ❑ Used to diagnose lost packets on the path between two hosts.
- ❑ Uses TCP/UDP port 19.
- ❑ H can send a chargen request from X to V.
- ❑ V can respond to X wasting their bandwidth.



## Connection Hijacking

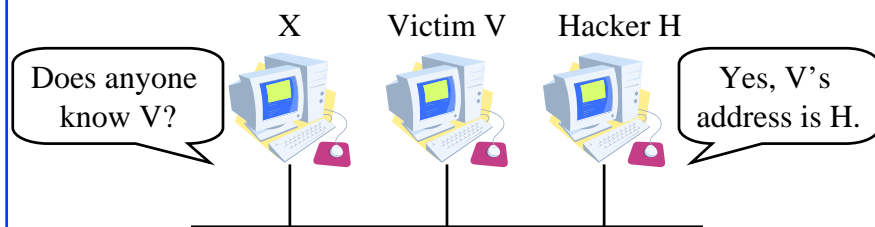
- ❑ H sends packets to server V which increments the sequence number for connection from X.
- ❑ All further packets from X are discarded at V.
- ❑ Responses for packets from H are sent to V - confusing him.



3-15

## ARP Spoofing

- ❑ X tries to find the MAC address of Victim V
- ❑ Hacker H responds to ARP request pretending to be V.
- ❑ All communication for V is captured by H.
- ❑ Hacker may flood fraudulent ARP requests and replies
- ❑ Countermeasure: Use static ARP



Washington University in St. Louis

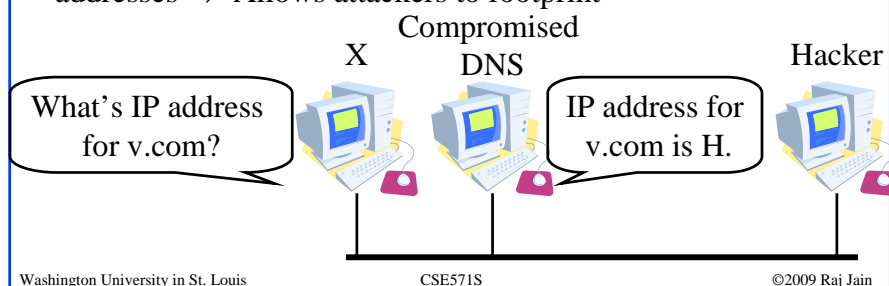
CSE571S

©2009 Raj Jain

3-16

## DNS Spoofing

- ❑ DNS server is compromised to provide H's IP address for V
- ❑ Virus can modify hosts files
- ❑ Access router modified to point to poisoned DNS ⇒ Pharming
- ❑ Phishing: security patch from [www.microsoft.com.128.252.160.33/download](http://www.microsoft.com.128.252.160.33/download)
- ❑ DNS zone transfer ⇒ Ask DNS for all domain names and addresses ⇒ Allows attackers to footprint



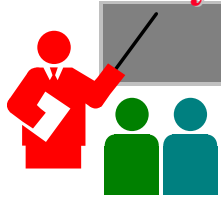
## E-Mail Spoofing

- ❑ From address is spoofed.
- ❑ Malware attachment comes from a friendly address.
- ❑ From: God@heavens.com

## Web Spoofing

- ❑ The web site looks like another
- ❑ Southwest Airline,  
<http://airlines.ws/southwest-airline.htm>
- ❑ For every .gov site there is a .com, .net giving similar information: nsf.com, tsa.com, whitehouse.com
- ❑ For misspellings of popular businesses, there are web sites: microshoft.com

## Summary



1. TCP port numbers, Sequence numbers, ack, flags
2. IP addresses are easy to spoof.  
ARP and DNS are not secure.
3. Flags: Syn Flood, Fin
4. Ping of Death, Smurf, Connection Hijacking
5. UDP Flood Attack
6. Application addresses are not secure

## References

1. Jan L. Harrington, "Network Security," Morgan Kaufmann, 2005, ISBN:0123116333
2. Gert De Laet and Gert Schauwers, "Network Security Fundamentals," Cisco Press, 2005, ISBN:1587051672

## Lab Homework 3

- ❑ This lab consists of using the following tools:
- ❑ XP Keylogger, <http://www.bestvistadownloads.com/download/t-free-xp-keylogger-download-zhtdqdn.html>
- ❑ SMBdie: A tool to crash windows server described at [http://www.windowsecurity.com/articles/SMBDie\\_Crashing\\_Windows\\_Servers\\_with\\_Ease.html](http://www.windowsecurity.com/articles/SMBDie_Crashing_Windows_Servers_with_Ease.html) download from <http://packetstormsecurity.org/0208-exploits/SMBdie.zip>
- ❑ Snort, vulnerability scanner, <http://www.codecraft-canada.com/Snort/>
- ❑ Password dump, Pwdump3, <http://www.openwall.com/passwords/dl/pwdump/pwdump3v2.zip>
- ❑ John the ripper, Brute force password attack, <http://www.openwall.com/john/>

## Lab Homework 3 (Cont)

- ❑ If you have two computers, you can install these programs on one computer and conduct these exercises.
- ❑ Alternately, you can remote desktop to CSE571XPC and conduct exercises 1-4 and then remote desktop to CSE571XPS and conduct exercise 5.
- ❑ Use your last name (with spaces removed) as your user name.

## 1. Keylogger

- ❑ Delete all previous log files, if any,  
e:\program files\xp keylogger\logs\\*.\*
- ❑ Start xp keylogger
- ❑ Browse to [www.google.com](http://www.google.com) and search for your name
- ❑ Stop keylogger
- ❑ CD to e:\program files\xp keylogger\logs\  
❑ Open the htm file in the browser
- ❑ Note down the texts shown there on a paper and submit.
- ❑ Delete the log e:\program files\xp keylogger\logs\\*.\*

## 2. Snort

- ❑ Delete all the previous logs, if any, e:\snort\log\new\\*.\*
- ❑ Start snort
- ❑ Go back to your machine
- ❑ Run smbdiie to attack CSE571XPC
- ❑ When the program stops, connect back to CSE571XPC
- ❑ Use control-C to stop snort
- ❑ Type the log file e:\snort\log\new>alert.ids
- ❑ Count how many time smbdiie is mentioned.
- ❑ Delete the logs, e:\snort\log\new\\*.\*

## 3. PWDump3

- ❑ Goal: Get the password hash from the server CSE571XPS
- ❑ On CSE571XPC, open a dos box
- ❑ CD to e:\pwdump3
- ❑ Run pwdump3 without parameters for help
- ❑ Run pwdump3 with parameters to get the hash file from server CSE571XPS
- ❑ You will need the administrator account and password supplied in the class.
- ❑ Open the hash file obtained in notepad. Delete all lines except the one with your last name.
- ❑ Save the file as e:\johntheripper\

## 4. Find your password

- On CSE571XPC, use the command box
- CD to e:\johntheripper
- Delete john.pot
- Run johntheripper without parameters to get help
- Run johntheripper with the file you created in step 3
- This will tell you your password, write it down on a paper to submit with the homework.
- Close your remote desktop session.

## 5. Change your password

- Now remote desktop to CSE571XPS
- Login using your last name as username and the password you obtained in step 4.
- Change your password to a strong password.  
Do this from your own account (not the administrator account).
- Note the time and date you change the password.  
Submit the time as homework answer.
- Logout