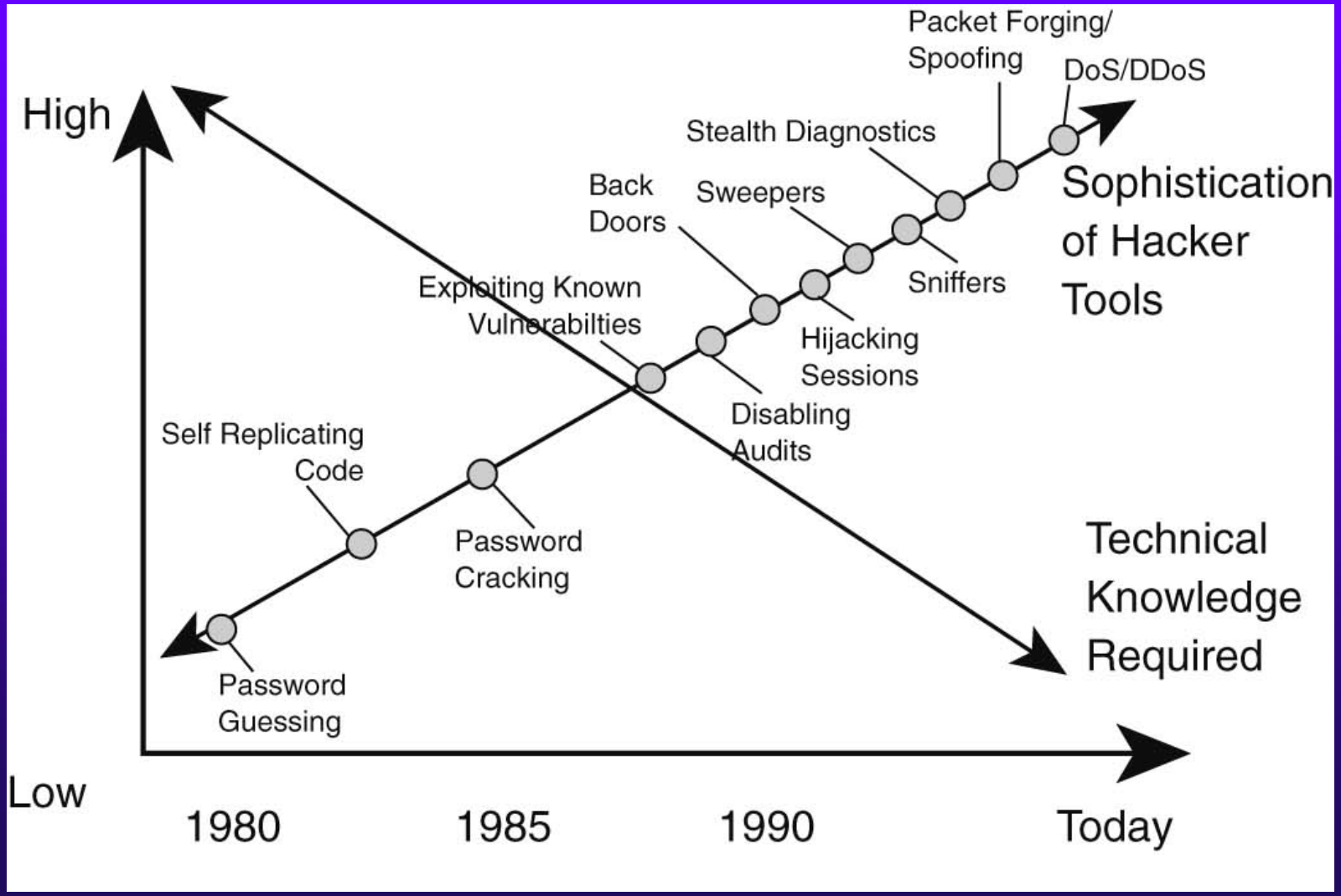
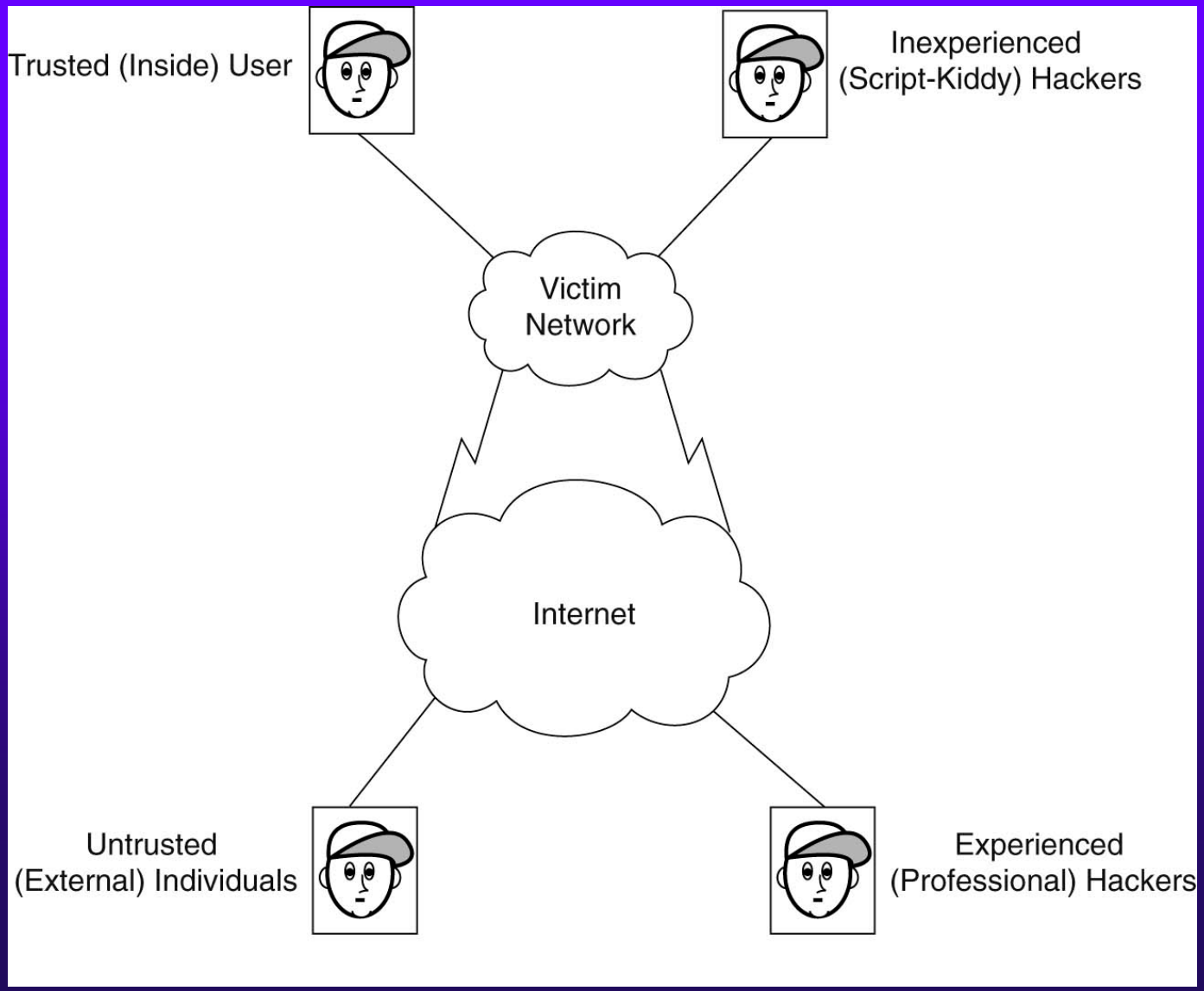
Chapter 14
Intrusion Detection

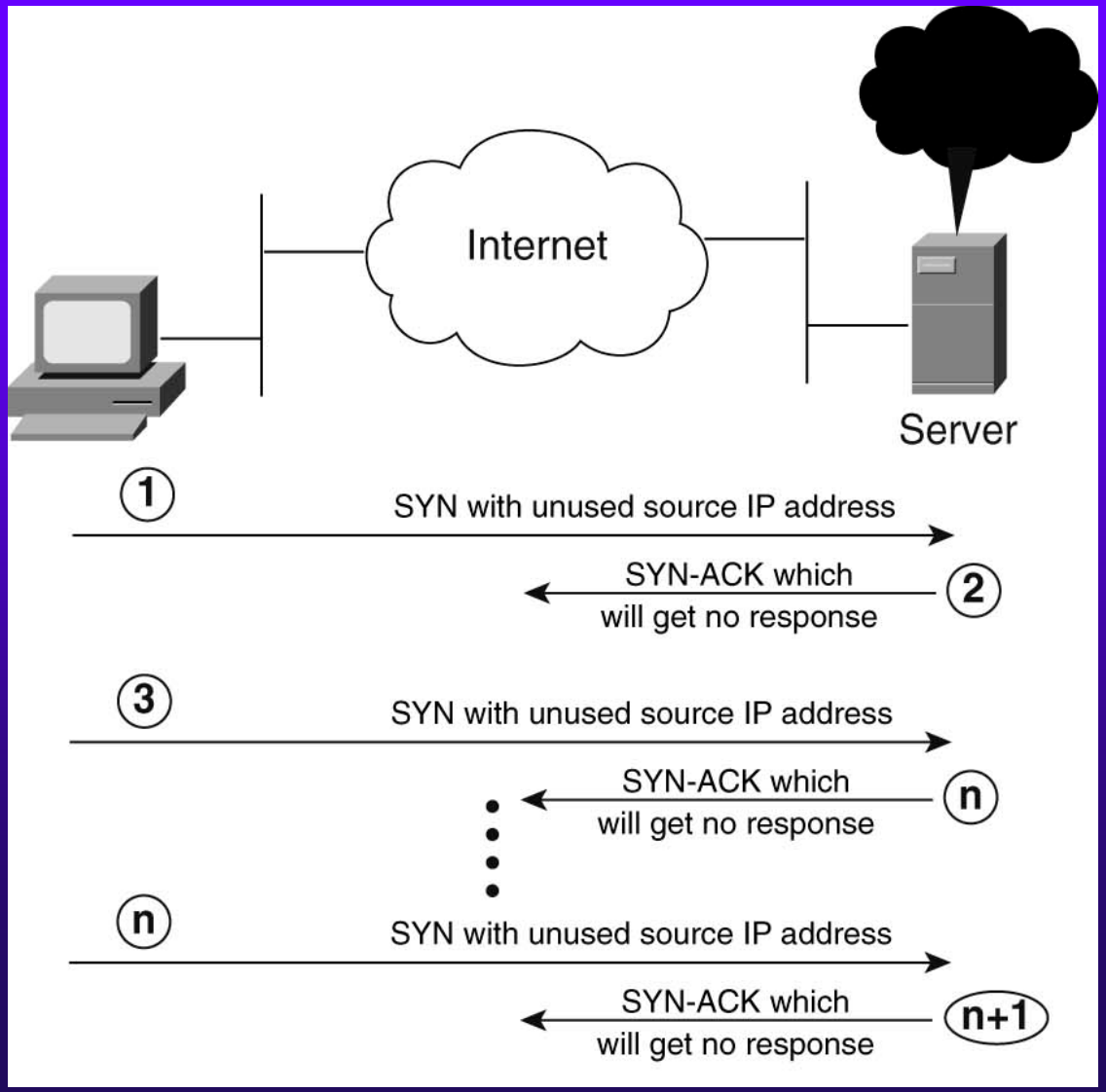
Hacker Capabilities



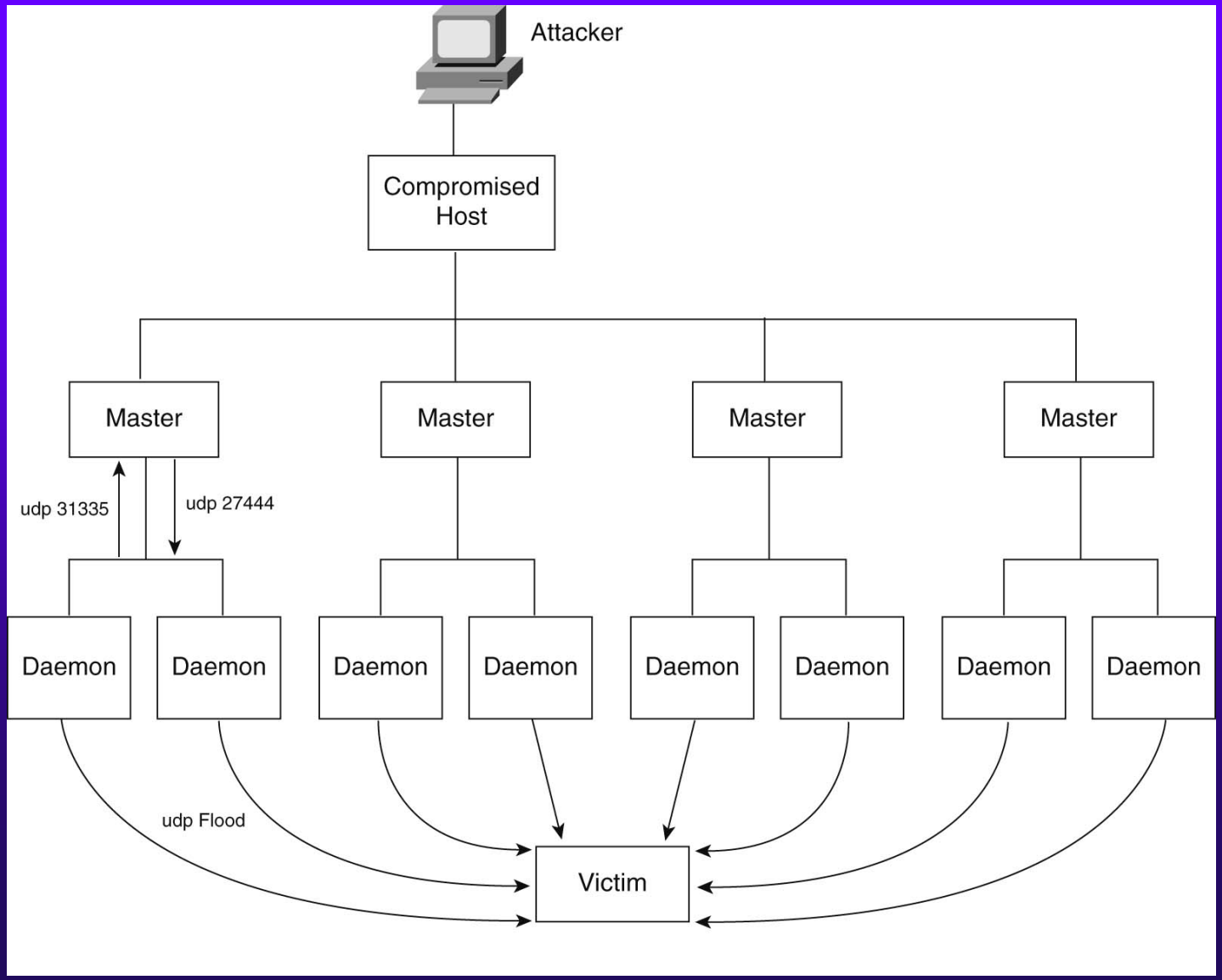
Types of Attackers



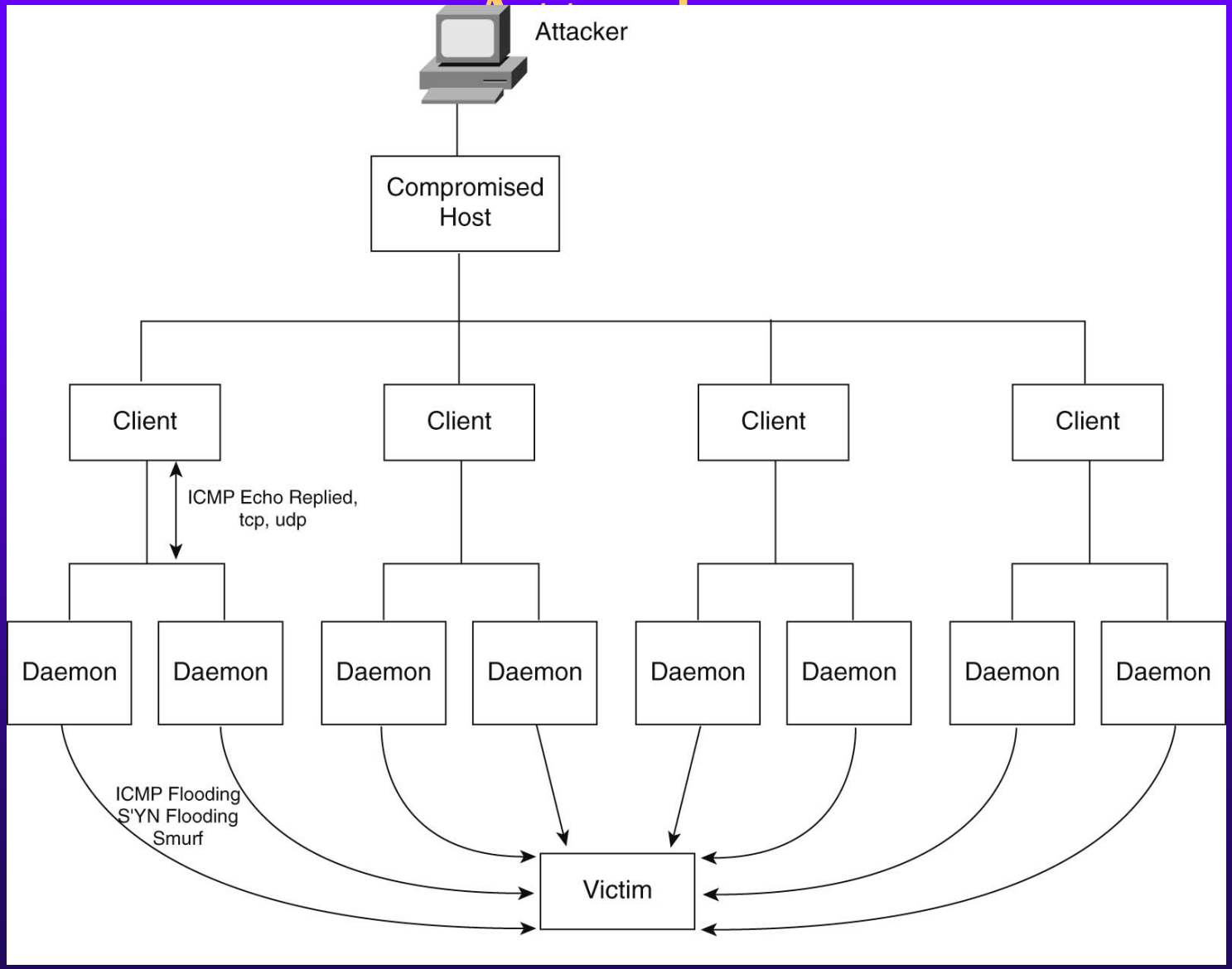
TCP SYN Flood DoS Attack



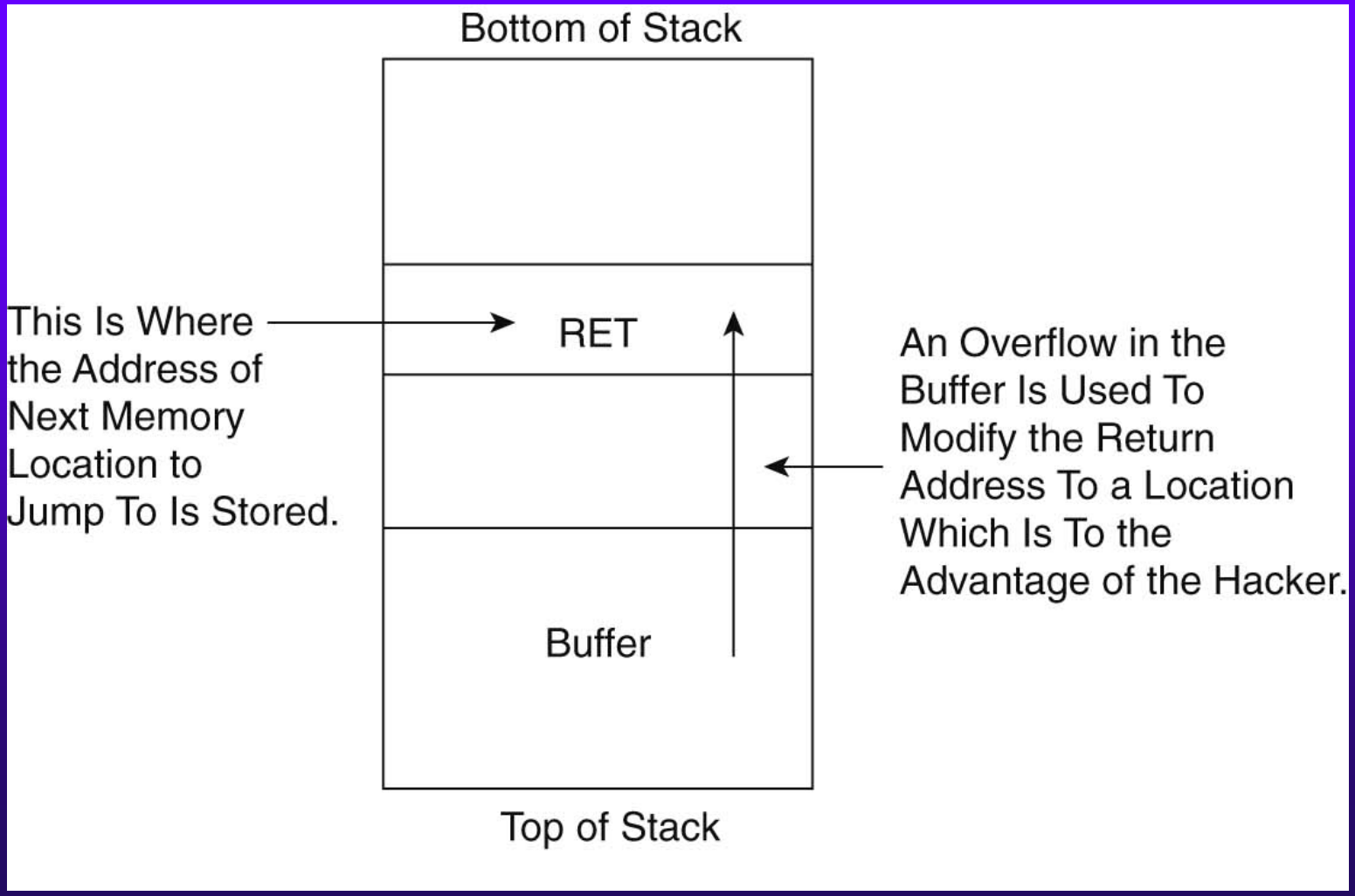
Trinoo Network Attack



Tribal Flood Network (TFN) Attack



Buffer Overflow Attack



Top 25 vulnerabilities

The table lists the most commonly found vulnerabilities on customer sites during internal and external Security Posture Assessments (SPAs). The vulnerabilites at the top of each column are the most common.

Rank	Internal	External
1	Possible Denial of Service (DoS) >>Read	TFTP Service Enabled>>Read
2	Weak Passwords>>Read	finger Global>>Read
3	finger Global>>Read	sendmail HELP>>Read
4	Microsoft SNMP Get Info>>Read	Mail Spam or Unsolicited Commercial E-mail (UCE)>>Read
5	finger Relay>>Read	Possible Denial of Service (DoS)>>Read
6	SNMP Community Name Guess -- Public>>Read	Weak Passwords>>Read
7	SNMP read community string>>Read	sendmail Reconnaissance: EXPN and VRFY>>Read
8	Mail Spam or Unsolicited Commercial E-mail (UCE)>>Read	SMTP HELP>>Read
9	finger Walk with Digits>>Read	IIS Unicode Remote Command Execution>>Read
10	sendmail HELP>>Read	Microsoft IIS .idq Requests Reveal Directory Paths>>Read
11	RPC portmapper Active>>Read	SMTP Relay>>Read
12	sendmail Reconnaissance: EXPN and VRFY>>Read	sendmail Program Sender (Pipe From) >>Read
13	IIS Unicode Remote Command Execution>>Read	HTTP MSADC vulnerability>>Read
14	Read Access to Netbios Share>>Read	SMTP-VRFY>>Read
15	TFTP Service Enabled>>Read	RPC portmapper Active>>Read
16	Anonymous FTP>>Read	IIS .htr Overflow>>Read
17	SMTP Relay>>Read	finger Walk Dot>>Read

Detecting Intrusions

- Statistical anomaly-based IDS
  - Uses thresholds for various types of activities
- Pattern matching or signature-based IDS
  - Uses a set of rules to detect an attack
  - Content-based and context-based signatures
- Cisco host-based and network-based IDS detect attacks based on signatures and anomalies

Types of Signatures

Context: (Header)	Ping of Death Land Attack	Port Sweep SYN Attack TCP Hijacking
Content: (Data)	MS IE Attack DNS Attacks	Telnet Attacks Character Mode Attacks
	"Atomic" Single Packet	"Composite" Multiple Packets

+ plus IP fragmentation reassembly

Case Study: Kevin Metnick's Attack on Tsutomu Simomura's Computers