Corporate Computer Security, 4th Edition
Randall J. Boyle & Raymond R. Panko

The Threat Environment

Chapter 1

What's Next?

- 1.1 Introduction & Terminology
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror

1.1: Basic Security Terminology

- **The Threat Environment**
  - The threat environment consists of the types of attackers and attacks that companies face

1.1: Basic Security Terminology

- **Security Goals**
  - Confidentiality
    - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.

1.1: Basic Security Terminology

- **Security Goals**
  - Integrity
    - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.

1.1: Basic Security Terminology

- **Security Goals**
  - Availability
    - Availability means that people who are authorized to use information are not prevented from doing so

1.1: Basic Security Terminology

- **Compromises**
  - Successful attacks
  - Also called *incidents*
  - Also called *breaches* (not breeches)

1.1: Basic Security Terminology

- **Countermeasures**
  - Tools used to thwart attacks
  - Also called *safeguards*, *protections*, and *controls*
  - Types of countermeasures
    - Preventative
    - Detective
    - Corrective

1.1: The Sony Data Breaches

- **Sony Corporation**
  - Japanese multinational corporation founded in 1946 that focuses on electronics, games, entertainment, and financial services
  - Employs about 146,300 people and has annual revenues of about $72.3 billion
  - Sony is widely known for its televisions, digital imaging, audio/video hardware, PCs, semiconductors, electronic components, and gaming platform.

1.1: The Sony Data Breaches

- **The First Attack**
  - April 17–19, 2011
  - Attacks happened a few weeks after the large earthquake, tsunami, and reactor meltdowns
  - Used SQL injection to steal 77 million accounts
  - Turned off access to PlayStation Network (PSN)
  - Publicly acknowledges intrusion a week after the intrusion, on April 26th
  - CEO, Kazuo Hirai, issues public apology
  - Hacking group "Anonymous" is suspected

1.1: The Sony Data Breaches

- **The Second Attack**
  - May 1st, 2011 – Sony Online Entertainment
  - Similar SQL injection attack used to steal additional 24.6 million accounts
  - Turned off access to all Sony Online Entertainment servers
  - CEO, Kazuo Hirai, issues written response to US Congress (May 4th) about steps to prevent future attacks
  - Some PSN services start to come online on May 15th

1.1: The Sony Data Breaches

- **The Third Attack**
  - June 2nd, 2011 – SonyPictures.com
  - Similar SQL injection attack used to steal additional 1 million accounts
  - SonyPictures.com is immediately shut down
  - Hacking group LulzSec claims responsibility and issues press statement

1.1: The Sony Data Breaches

- **LulzSec press statement**

“Greetings folks. We're LulzSec, and welcome to Sownage. Enclosed you will find various collections of data stolen from internal Sony networks and websites, all of which we accessed easily and without the need for outside support or money.

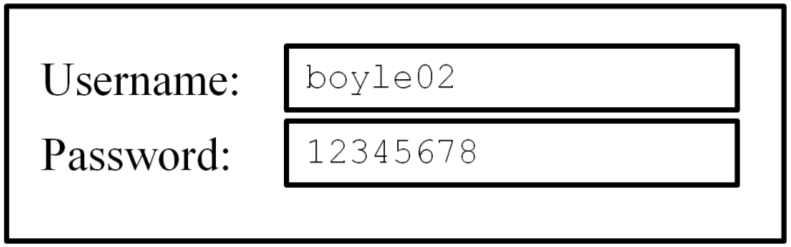
We recently broke into SonyPictures.com and compromised over 1,000,000 users' personal information, including passwords, email addresses, home addresses, dates of birth, and all Sony opt-in data associated with their accounts. Among other things, we also compromised all admin details of Sony Pictures (including passwords) along with 75,000 ‘music codes’ and 3.5 million ‘music coupons’.”

1.1: The Sony Data Breaches

- **SQL injection** is an attack that involves sending *modified* SQL statements to a web application that will, in turn, modify a database.
- Attackers can send *unexpected input* through their web browser which will enable them to read from, write to, and even delete entire databases.

1.1: The Sony Data Breaches

- SQL statement below shows parameters passed to a database for a *legitimate* login



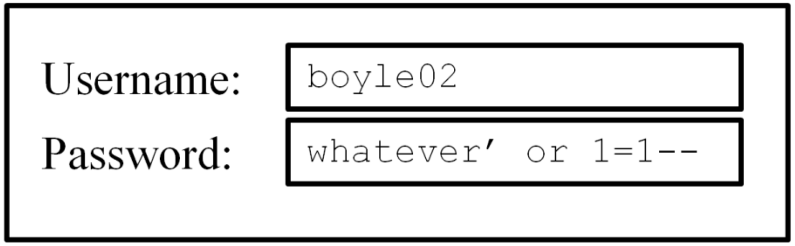
Username: boyle02

Password: 12345678

- SELECT FROM Users WHERE username=‘**boyle02**’ AND password=‘**12345678**’;

1.1: The Sony Data Breaches

- Malformed SQL statement below shows SQL injection by passing *unexpected* parameters through a Web interface
- Will *always* return a true value



Username:	boyle02
Password:	whatever' or 1=1--

- SELECT FROM Users WHERE username=‘**boyle02**’ AND password=‘**whatever’ or 1=1--**’;

1.1: The Sony Data Breaches

- **The attackers**
  - Members of both LulzSec and Anonymous are involved
  - Just before attacks on Sony, Anonymous announced the launch of operation “#OpSony” for lawsuits against George Hotz
  - George Hotz was being sued by Sony for jailbreaking PlayStation 3
  - Cody Kretsinger was arrested on Sept. 22, 2011 and pled guilty for his involvement in the Sony attacks
  - Hector Monsegur, facing 122 years in prison, was key informant who identified other attackers

1.1: The Sony Data Breaches

- **The Fall-Out: Lawsuits and Investigations**
  - Sony offered 1 year of free identify theft services, month of free gaming, and a few free games from a limited selection
  - To date, no known credit fraud directly tied to the Sony data breaches
  - Fined $395,000 by UK because “security measures were simply not good enough”
  - Sony estimates losses at $171 million
  - Difficult to estimate damage to Sony’s reputation

What's Next?

- 1.1 Introduction & Terminology
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror

1.2: Employee and Ex-Employee Threats

- **Employees and Ex-Employees Are Dangerous**
  - Dangerous because
    - They have knowledge of internal systems
    - They often have the permissions to access systems
    - They often know how to avoid detection
    - Employees generally are trusted
  - IT and especially IT security professionals are the greatest employee threats (*Qui custodiet custodes?)*

1.2: Employee and Ex-Employee Threats

- Employee Sabotage
  - Destruction of hardware, software, or data
  - Plant time bomb or logic bomb on computer
- Employee Hacking
  - Hacking is intentionally accessing a computer resource without authorization or in excess of authorization
  - Authorization is the key

1.2: Employee and Ex-Employee Threats

- Employee Financial Theft
  - Misappropriation of assets
  - Theft of money
- Employee Theft of Intellectual Property (IP)
  - Copyrights and patents (formally protected)
  - Trade secrets: plans, product formulations, business processes, and other info that a company wishes to keep secret from competitors

1.2: Employee and Ex-Employee Threats

- Employee Extortion
  - Perpetrator tries to obtain money or other goods by threatening to take actions that would be against the victim's interest
- Sexual or Racial Harassment of Other Employees
  - Via e-mail
  - Displaying pornographic material

1.2: Employee and Ex-Employee Threats

- **Internet Abuse**
  - Downloading pornography, which can lead to sexual harassment lawsuits and viruses
  - Downloading pirated software, music, and video, which can lead to copyright violation penalties
  - Excessive personal use of the Internet at work

1.2: Employee and Ex-Employee Threats

- Carelessness
  - Loss or theft of computers or data media containing sensitive information
- Other “Internal” Attackers
  - Contract workers
  - Workers in contracting companies

What’s Next?

1.1 Introduction & Terminology

1.2 Employee and Ex-Employee Threats

1.3 Malware

1.4 Hackers and Attacks

1.5 The Criminal Era

1.6 Competitor Threats

1.7 Cyberwar and Cyberterror

1.3: Classic Malware: Viruses and Worms

- **Malware**
  - A generic name for any “evil software”
- **Viruses**
  - Programs that attach themselves to legitimate programs on the victim’s machine
  - Spread today primarily by e-mail
  - Also by instant messaging, file transfers, etc.

1.3: Classic Malware: Viruses and Worms

- **Worms**
  - Full programs that do *not* attach themselves to other programs
  - Like viruses, can spread by e-mail, instant messaging, and file transfers

1.3: Classic Malware: Viruses and Worms

- **Worms**
  - In addition, *direct-propagation* worms can jump from one computer to another without human intervention on the receiving computer
  - Computer must have a vulnerability for direct propagation to work
  - Direct-propagation worms can spread extremely rapidly because they do not have to wait for users to act

1.3: Classic Malware: Viruses and Worms

- **Blended Threats**
  - Malware propagates in several ways—like worms, viruses, compromised webpages containing mobile code, etc.
- **Payloads**
  - Pieces of code that do damage
  - Implemented by viruses and worms after propagation
  - Malicious payloads are designed to do heavy damage

1.3: Trojan Horses and Rootkits

- **Nonmobile Malware**
  - Must be placed on the user’s computer through one of a growing number of attack techniques
  - Placed on computer by hackers
  - Placed on computer by virus or worm as part of its payload
  - The victim can be enticed to download the program from a website or FTP site
  - Mobile code executed on a webpage can download the nonmobile malware

1.3: Trojan Horses and Rootkits

- **Trojan Horses**
  - A program that replaces an existing system file, taking its name
- **Trojan Horses**
  - Remote Access Trojans (RATs)
    - Remotely control the victim’s PC
  - Downloaders
    - Small Trojan horses that download larger Trojan horses after the downloader is installed

1.3: Trojan Horses and Rootkits

- Trojan Horses
  - Spyware
    - Programs that gather information about you and make it available to the adversary
    - Cookies that store too much sensitive personal information
    - Keystroke loggers
    - Password-stealing spyware
    - Data mining spyware

1.3: Trojan Horses and Rootkits

- Trojan Horses
  - Rootkits
    - Take control of the super user account (root, administrator, etc.)
    - Can hide themselves from file system detection
    - Can hide malware from detection
    - Extremely difficult to detect (ordinary antivirus programs find few rootkits)

1.3: Other Malware Attacks

- **Mobile Code**
  - Executable code on a webpage
  - Code is executed automatically when the webpage is downloaded
  - Javascript, Microsoft Active-X controls, etc.
  - Can do damage if computer has vulnerability

1.3: Other Malware Attacks

- **Social Engineering in Malware**
  - Social engineering is attempting to trick users into doing something that goes against security policies
  - Several types of malware use social engineering
    - Spam
    - Phishing
    - Spear phishing (aimed at individuals or specific groups)
    - Hoaxes

What's Next?

- 1.1 Introduction & Terminology
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror

1.4: Traditional External Attackers: Hackers

- **Traditional Hackers**
  - Motivated by thrill, validation of skills, sense of power
  - Motivated to increase reputation among other hackers
  - Often do damage as a byproduct
  - Often engage in petty crime

1.4: Traditional External Attackers: Hackers

- Anatomy of a Hack
  - Reconnaissance probes (Figure 1-11)
    - IP address scans to identify possible victims
    - Port scans to learn which services are open on each potential victim host

1.4: Probe and Exploit Attack Packets

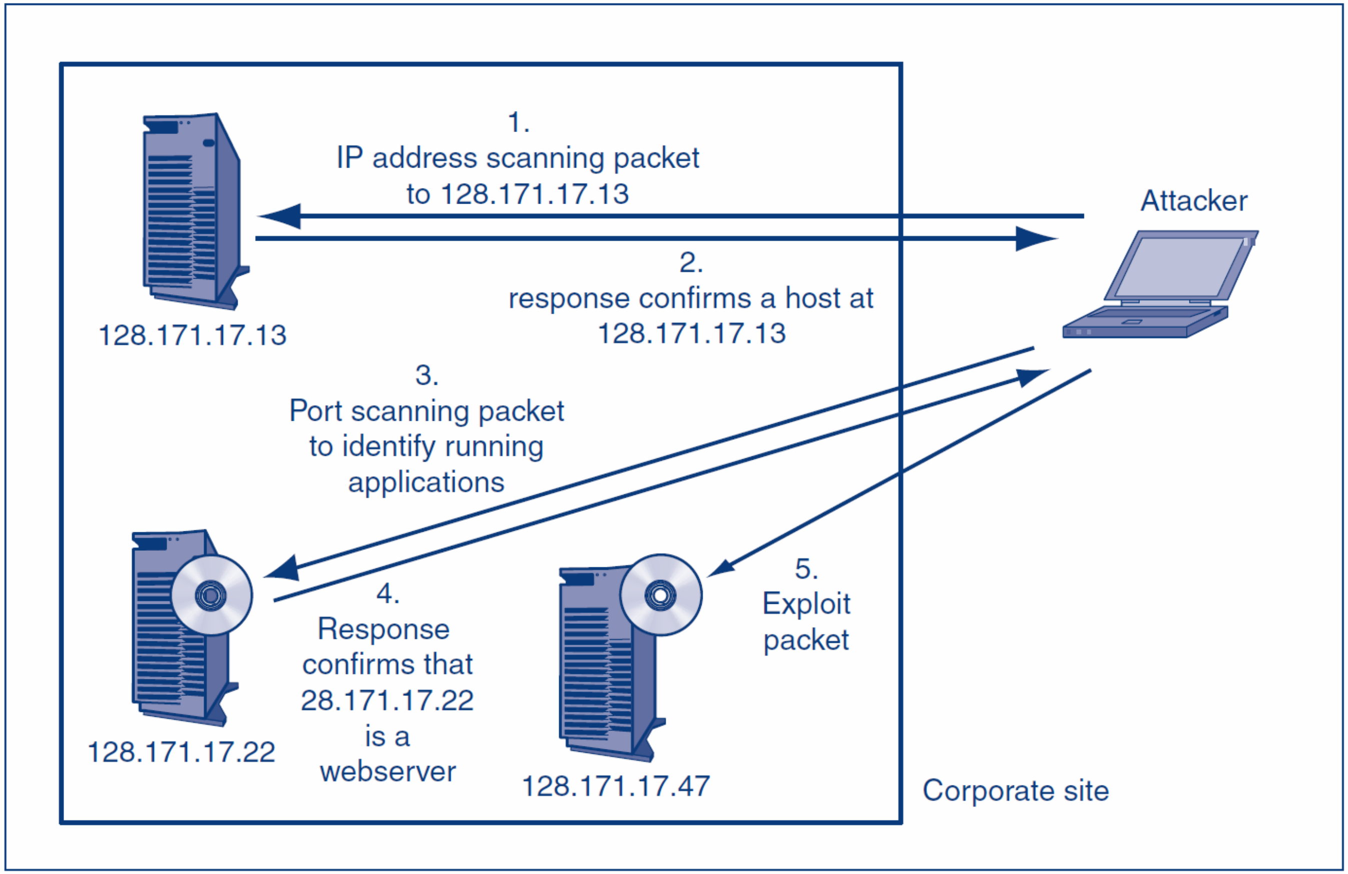


FIGURE 1-11 Probe and Exploit Attack Packets

1.4: Traditional External Attackers: Hackers

- **Anatomy of a Hack**
  - The exploit
    - The specific attack method that the attacker uses to break into the computer is called the attacker’s exploit
    - The act of implementing the exploit is called exploiting the host

1.4: Source IP Address Spoofing

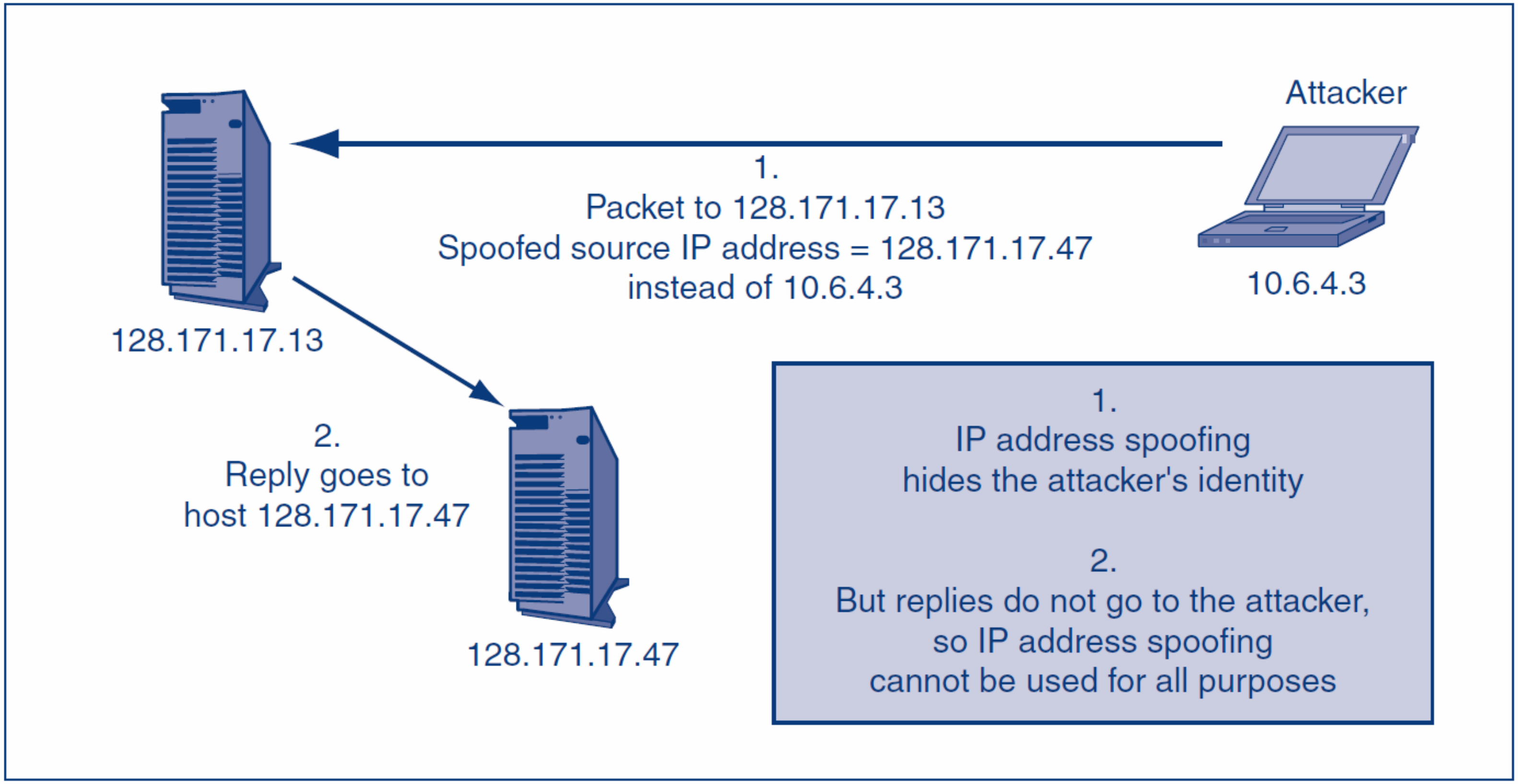
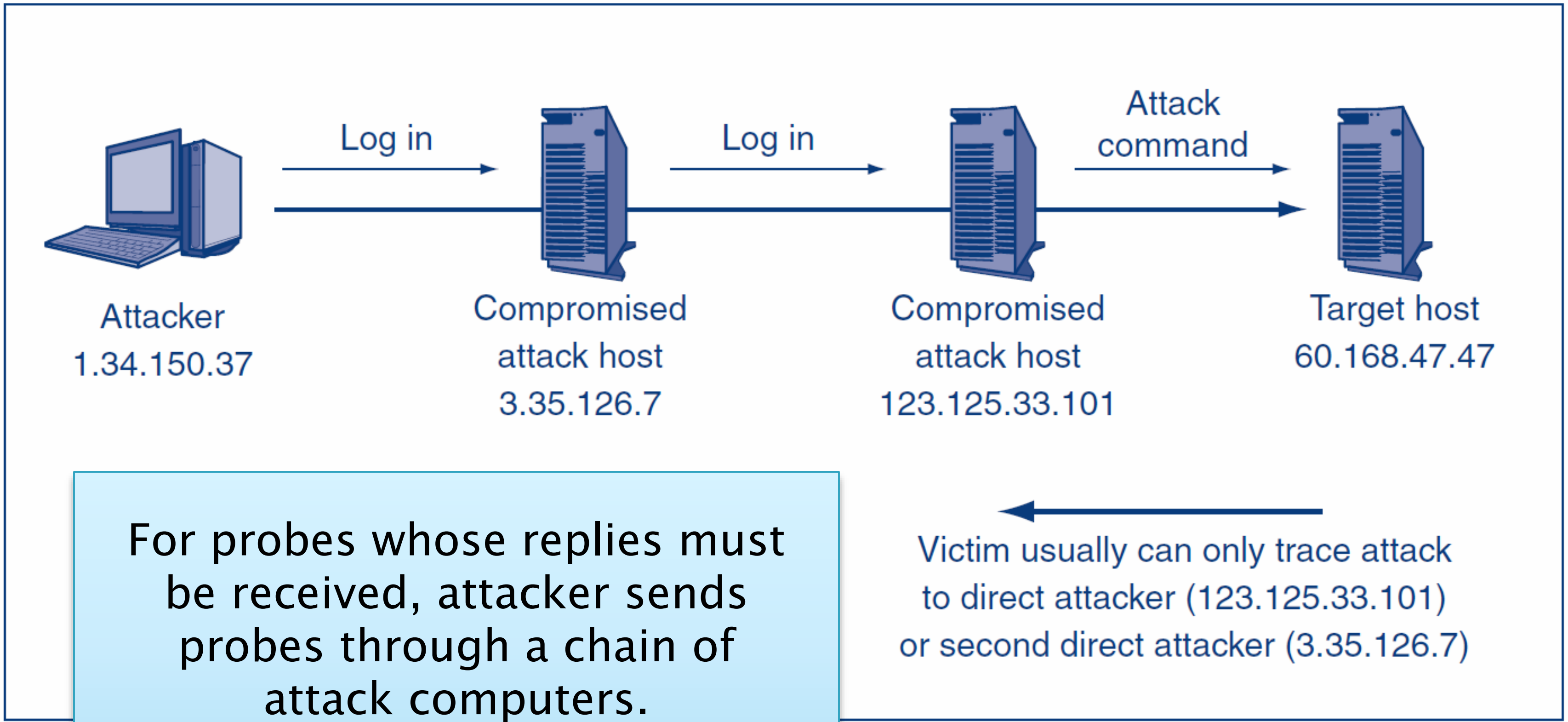


FIGURE 1-12 Source IP Address Spoofing

1.4: Traditional External Attackers: Hackers

- **Chain of attack computers (Figure 1-13)**
  - The attacker attacks through a chain of victim computers
  - Probe and exploit packets contain the source IP address of the last computer in the chain
  - The final attack computer receives replies and passes them back to the attacker
  - Often, the victim can trace the attack back to the final attack computer
  - But the attack can usually only be traced back a few computers more

1.4: Chain of Attack Computers



For probes whose replies must be received, attacker sends probes through a chain of attack computers.

Victim only knows the identity of the last compromised host (123.125.33.101), not that of the attacker.

1.4: Traditional External Attackers: Hackers

- **Social Engineering**
  - Social engineering is often used in hacking
    - Call and ask for passwords and other confidential information
    - E-mail attack messages with attractive subjects
    - Piggybacking
    - Shoulder surfing
    - Pretexting
    - Etc.
  - Often successful because it focuses on human weaknesses instead of technological weaknesses

1.4: Traditional External Attackers: Hackers

- **Denial-of-Service (DoS) Attacks**
  - Make a server or entire network unavailable to legitimate users
  - Typically send a flood of attack messages to the victim
  - Distributed DoS (DDoS) Attacks (Figure 1-15)
    - Bots flood the victim with attack packets
    - Attacker controls the bots

1.4: Distributed Denial-of-Service (DDoS) Flooding Attack

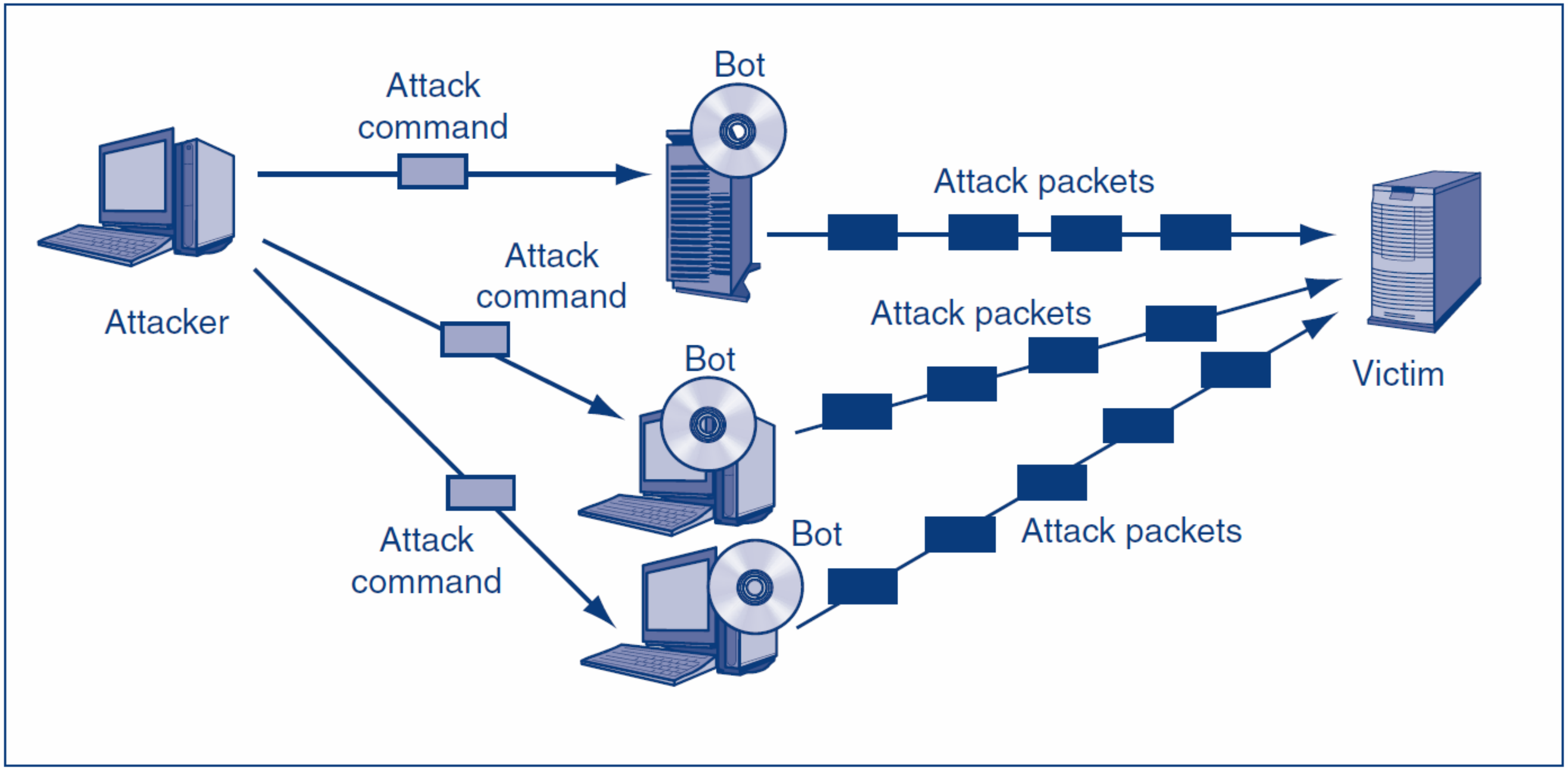


FIGURE 1-15 Distributed Denial-of-Service (DDoS) Flooding Attack

1.4: Traditional External Attackers: Hackers

- Skill Levels
  - Expert attackers are characterized by strong technical skills and dogged persistence
  - Expert attackers create hacker scripts to automate some of their work
  - Scripts are also available for writing viruses and other malicious software

1.4: Traditional External Attackers: Hackers

- Skill Levels
  - Script kiddies use these scripts to make attacks
  - Script kiddies have low technical skills
  - Script kiddies are dangerous because of their large numbers

What's Next?

- 1.1 Introduction & Terminology
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror

1.5: The Criminal Era

- **The Criminal Era**
  - Today, *most* attackers are career criminals with traditional criminal motives
  - Adapt traditional criminal attack strategies to IT attacks (e.g., fraud, etc.)

1.5: The Criminal Era

- **The Criminal Era**
  - Many cybercrime gangs are international
    - Makes prosecution difficult
    - Dupe citizens of a country into being transshippers of fraudulently purchased goods to the attacker in another country
  - Cybercriminals use black market forums
    - Credit card numbers and identity information
    - Vulnerabilities
    - Exploit software (often with update contracts)

1.5: The Criminal Era

- **Fraud**
  - In fraud, the attacker deceives the victim into doing something against the victim's financial self-interest
  - Criminals are learning to conduct traditional frauds and new frauds over networks
  - Also, new types of fraud, such as click fraud

1.5: The Criminal Era

- **Financial and Intellectual Property Theft**
  - Steal money or intellectual property that can be sold to other criminals or to competitors
- **Extortion**
  - Threaten a DoS attack or threaten to release stolen information unless the victim pays the attacker

1.5: The Criminal Era

- **Stealing Sensitive Data about Customers and Employees**
  - Carding (credit card number theft)
  - Bank account theft
  - Online stock account theft
  - Identity theft
    - Steal enough identity information to represent the victim in large transactions, such as buying a car or even a house

1.5: The Criminal Era

- **Corporate Identity Theft**
  - Steal the identity of an entire corporation
  - Accept credit cards on behalf of the corporation
  - Pretend to be the corporation in large transactions
  - Can even take ownership of the corporation

What's Next?

- 1.1 Introduction & Terminology
- 1.2 Employee and Ex-Employee Threats
- 1.3 Malware
- 1.4 Hackers and Attacks
- 1.5 The Criminal Era
- 1.6 Competitor Threats
- 1.7 Cyberwar and Cyberterror

1.6: Competitor Threats

- **Commercial Espionage**
  - Attacks on confidentiality
  - Public information gathering
    - Company website and public documents
    - Facebook pages of employees, etc.
  - Trade secret espionage
    - May only be litigated if a company has provided reasonable protection for those secrets
    - Reasonableness reflects the sensitivity of the secret and industry security practices

1.6: Competitor Threats

- **Commercial Espionage**
  - Trade secret theft approaches
    - Theft through interception, hacking, and other traditional cybercrimes
    - Bribe an employee
    - Hire your ex-employee and solicite or accept trade secrets
  - National intelligence agencies engage in commercial espionage

1.6: Competitor Threats

- **Denial-of-Service Attacks by Competitors**
  - Attacks on availability
  - Rare, but can be devastating

What’s Next?

1.1 Introduction & Terminology

1.2 Employee and Ex-Employee Threats

1.3 Malware

1.4 Hackers and Attacks

1.5 The Criminal Era

1.6 Competitor Threats

1.7 Cyberwar and Cyberterror

1.7: Cyberwar and Cyberterror

- **Cyberwar and Cyberterror**
  - Attacks by national governments (cyberwar)
  - Attacks by organized terrorists (cyberterror)
  - Nightmare threats
  - Potential for far greater attacks than those caused by criminal attackers

1.7: Cyberwar and Cyberterror

- **Cyberwar**
  - Computer-based attacks by national governments
  - Espionage
  - Cyber-only attacks to damage financial and communication infrastructure
  - To augment conventional physical attacks
    - Attack IT infrastructure along with physical attacks (or in place of physical attacks)
    - Paralyze enemy command and control
    - Engage in propaganda attacks

1.7: Cyberwar and Cyberterror

- **Cyberterror**
  - Attacks by terrorists or terrorist groups
  - May attack IT resources directly
  - Use the Internet for recruitment and coordination
  - Use the Internet to augment physical attacks
    - Disrupt communication among first responders
    - Use cyberattacks to increase terror in physical attacks
  - Turn to computer crime to fund their attacks

The End