# Targeted Break-in, DoS, & Malware attacks (I)

(February 18, 2015)



## Learning Objectives

- Understand Targeted attacks' preparation
- Discuss Break-in attacks



## Targeted attacks' preparation

- Before launching targeted attacks, attackers engage in:
  - Unobtrusive info gathering
  - Host scanning
  - Port scanning
  - Network scanning
  - Fingerprinting

## Unobtrusive Information Collection

- Sending packets into a network is "noisy"
- Need to do unobtrusive info gathering, first, by
  - Visiting target corporate website for
    - Employees' names and emails
    - Officers names and organizational structure, etc.
  - Reading trade press (often online & searchable) for
    - Info about products under development
    - Firms' financial prospects, etc.
  - Searching U.S. EDGAR* system online for
    - Ownership, shareholder information, etc.
  - Searching the Whois database at:
    - NetworkSolutions.com/whhois/index.jsp, internic.net/whois.html, etc.



* Electronic Data Gathering, Analysis, and Retrieval

## Sample of Whois entries

- **Domain Name: PUKANUI.COM**
  **Administrative Contact :**
  **Panko, Ray Ray@Panko.com**
  **1456 KALANIIKI ST HONOLULU, HI 96821 US**
  **Phone: (808) 377-1149**
- **Domain servers in listed order:**
  **NS75.WORLDNIC.COM 205.178.190.38**
  **NS76.WORLDNIC.COM 205.178.189.38**

DNS Servers



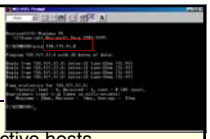
## Attacks preps: examining email headers

**Received:** from hotmail.com (bay103-f21.bay103.hotmail.com [65.54.174.31])
by barracuda1.eiu.edu (Spam Firewall) with ESMTP id B10BA1F52DC
for <aillia@eiu.edu>; Wed, 8 Feb 2006 18:14:59 -0600 (CST)
**Received:** from mail pickup service by hotmail.com with Microsoft SMTPSVC;
Wed, 8 Feb 2006 16:14:58 -0800
**Message-ID:** <BAY103-F2195A2F82610991D56FEC0B1030@phx.gbl>
**Received:** from 65.54.174.200 by by103fd.bay103.hotmail.msn.com with HTTP;
Thu, 09 Feb 2006 00:14:58 GMT
**X-Originating-IP:** [192.30.202.14] ← Source IP Address
**X-Originating-Email:** [macolas@hotmail.com]
**X-Sender:** macolas@hotmail.com
**In-Reply-To:** <10E30E5174081747AF9452F4411465410C5BB560@excma01.cmamdm.enterprise.corp>
**X-PH:** V4.4@ux1
**From:** <macolas@hotmail.com>
**To:** aillia@eiu.edu
**X-ASG-Orig-Subj:** RE: FW: Same cell#
**Subject:** RE: FW: Same cell#
**Date:** Thu, 09 Feb 2006 00:14:58 +0000
**Mime-Version:** 1.0
**Content-Type:** text/plain; format=flowed
**X-OriginalArrivalTime:** 09 Feb 2006 00:14:58.0614 (UTC) FILETIME=[DCA31D60:01C62D0D]
**X-Virus-Scanned:** by Barracuda Spam Firewall at eiu.edu
**X-Barracuda-Spam-Score:** 0.00

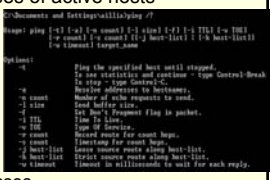
IP Address Locator: http://www.geobytes.com/IpLocator.htm

Display email headers in Gmail, Yahoo!, Hotmail: http://aruljohn.com/info/howtofindipaddress/

## Host Scanning



- Objective: identify IP addresses of active hosts
- Pinging individual hosts



- Ping scanning
  - Pinging a range of IP addresses
  - IP scanning software: fping, gping, Ping Sweep, Pinger
- SYN/ACK scanning used when firewall configured to block pinging from outside

7

## Network Scanning

- Objective: understand a network internal structure including routers, firewalls location
- Also called network mapping
- Main tools used
  - Tracert (in Windows) or Traceroute (in Linux)
  - Network scanning software, e.g **NetScanner**

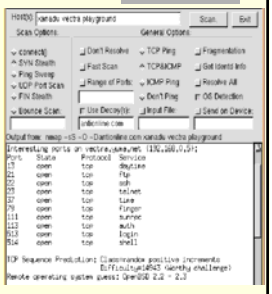
8

## Port Scanning

- Port Scanning
  - Most break-ins exploit specific services/applications

| Service | Default Port |
|---|---|
| www | 80 |
| FTP | 21 |
| SMTP | 25 |

  - Scan target for open ports
    - Send SYN segments to a particular port number
    - Observe SYN/ACK or reset (RST) responses



9

## Fingerprinting

- Determining specific software run by target
  - Identify a particular operating system or application program and (if possible) version
    - For example, Microsoft Windows 2000 Server
    - For example, BSD LINUX 4.2
    - For example, Microsoft IIS 5.0
  - Useful because most exploits are specific to particular programs or versions

10

## Active vs. Passive fingerprinting

- Active Fingerprinting
  - Send odd messages and observe replies
  - Different operating systems and application programs respond differently
  - Active fingerprinting may set off alarms
    - Attackers usually use rate of attack messages below IDSs volume thresholds
- Passive Fingerprinting
  - Read headers (IP-H, TCP-H, etc.) of normal response messages
    - e.g. Windows 2000 uses TTL = 128 and Window Size = 18000
  - Passive Fingerprint difficult b/c Admin could change default values

| Time To Live (8 bits) | Protocol (8 bits) 1=ICMP, 6=TCP,17=UDP | Window Size (16 bits) |
|---|---|---|

11

## Fingerprinting by reading banners

- Many programs have preset banners used in initiating communications
- Using telnet or FTP to connect to a server could display the banner

```
Details:
220----------------------------------------------------------------------
220-This is the "Banner" message for the Mac OS X Server's FTP server process.
220-
220-            FTP clients will receive this message immediately
220-            before being prompted for a name and password.
220-
220-PLEASE NOTE:
220-
220-      Some FTP clients may exhibit problems if you make this file too long.
220-
220----------------------------------------------------------------------
220-
220 battery.eiu.edu FTP server ready.
530 Guest login disabled.
```

12

## Summary Questions 1

- In preparing his attack, the attacker used the **ping** command to determine whether or not the target computers are connected and responsive. Which of the following did the attacker do?
  a) Network scanning
  b) Port scanning
  c) None of the above

13

## Summary Questions 1 (cont.)

- In preparing his attack, the attacker sent normal HTTP requests to a web server. Then, he spent some time analyzing the protocol-related information in the response received from the web server in order to determine what software are installed on the web server. Which of the following did the attacker do?
  a) Active learning
  b) Network scanning
  c) Passive fingerprinting
  d) None of the above

14

## Break-In Attacks

- Take advantage of known vulnerabilities that have not been patched
  - Exploits are easy to use
  - Frequently effective
- Intruder needs
  - User manes and passwords, or
  - Hijack another user's session

15

## Obtaining passwords

- By using social engineering
- By intercepting authentication communications
- With physical access
  - Can install keystroke capture programs
  - Can copy password file and crack it later by password "guessing"
    - Windows 2000, XP: \windows\system32\config
    - Linux: /etc/passwd

16

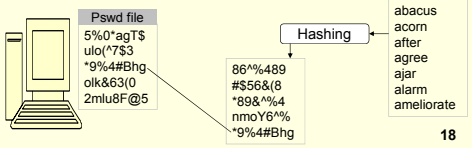
## Password guessing

- Brute force
  - Generating possible password combinations by changing one character at a time
    - If password is 4 decimal numbers
      - Start with 0000; next try 0001; then 0002; etc.
      - How many possible combinations? _____
    - If password is 6 alphabetical characters, how many possible combinations? _____
  - Brute force password cracking software available

17

## Password guessing (cont.)

- Dictionary attack
  - Does not try all possible combinations
  - Takes each word from a "dictionary", then
    - Encodes it in the same way the target computer encodes passwords
    - Compares encoded word with password file entries




18

## Summary Questions 2

- You want to crack the passwords in the SAM file on a Windows XP computer. The Operating system is installed on the C: drive. At what specific location is the SAM file located?
  a) C:\
  b) C:\root
  c) C:\Windows\system32
  d) C:\Windows\system32\config

19

## Summary Questions 2 (cont.)

- Assume that a password is 2 decimal number long. What is the maximum number of passwords that an attacker would have to try in order to crack the password?
  a) 4
  b) 67108864
  c) 1024
  d) None of the above
- How much time (in minutes) will it take to crack the password if it requires 1.2 second to try each password?

**Answer:** a maximum of _____ minutes.

20

## Session Hijacking

- Exploiting of a valid communication session to gain unauthorized access
- Many servers use session IDs to continue communication with returned users
- Session could be hijacked using
  - Session sniffing

## Session Hijacking (cont.)

- Session Hijacking could also be done through
  - Theft of session cookie file used for authenticating users by web servers

22

## Break-In: Posthack

- Install rootkit for posthack activities
  - Usually downloaded through trivial file transfer protocol (TFTP)
- Create backdoors for reentry if original hacking vulnerability is fixed
  - Backdoor accounts
  - Trojanized programs that permit reentry
- Collect needed info or damage the system
- Weaken system's security
- Delete audit logs

23