Worms
Announcements

- Quiz on Friday October 1
- Guest lecture on Monday October 4
- Guest lecture on Friday October 8
Review of Malwares

- Backdoor, logic bomb
- Trojan horse
- Virus
- Worm
- Botnets
- Rootkit: user level, kernel level, under-kernel
- Spyware
- Scareware, ransomware
Morris Worm (November 1988)

- First major worm
- Written by Robert Morris
  - Son of former chief scientist of NSA’s National Computer Security Center

What comes next: 1 1 2 1 1 2 1 1 1 2 2 1?
Morris Worm Description

- Two parts
  - Main program to spread worm
    - look for other machines that could be infected
    - try to find ways of infiltrating these machines
  - Vector program (99 lines of C)
    - compiled and run on the infected machines
    - transferred main program to continue attack
Vector 1: Debug feature of sendmail

- Sendmail
  - Listens on port 25 (SMTP port)
  - Some systems back then compiled it with DEBUG option on

- Debug feature gives
  - The ability to send a shell script and execute on the host
Vector 2: Exploiting fingerd

- Finger output
  
  `arthur.cs.purdue.edu% finger ninghui`
  
  Login name: ninghui  
  In real life: Ninghui Li  
  Directory: /homes/ninghui  
  Shell: /bin/csh  
  Since Sep 28 14:36:12 on pts/15 from csdhcp-120-173 (9 seconds idle)  
  
  New mail received Tue Sep 28 14:36:04 2010;  
  unread since Tue Sep 28 14:36:05 2010  
  No Plan.
Vector 2: Exploiting fingerd

- Fingerd
  - Listen on port 79

- It uses the function gets
  - Fingerd expects an input string
  - Worm writes long string to internal 512-byte buffer

- Overrides return address to jump to shell code
Vector 3: Exploiting Trust in Remote Login

• Remote login on UNIX
  – rlogin, rsh

• Trusting mechanism
  – Trusted machines have the same user accounts
  – Users from trusted machines
  – /etc/host.equiv – system wide trusted hosts file
  – /.rhosts and ~/.rhosts – users’ trusted hosts file
Vector 3: Exploiting Trust in Remote Login

- Worm exploited trust information
  - Examining trusted hosts files
  - Assume reciprocal trust
    - If X trusts Y, then maybe Y trusts X
- Password cracking
  - Worm coming in through fingerd was running as daemon (not root) so needed to break into accounts to use .rhosts feature
  - Read /etc/passwd, used ~400 common password strings & local dictionary to do a dictionary attack
Other Features of The Worm

• Program is shown as 'sh' when ps
• Files didn’t show up in ls
• Find targets using several mechanisms:
  • 'netstat -r -n', /etc/hosts, …
• Compromise multiple hosts in parallel
  – When worm successfully connects, forks a child to continue the infection while the parent keeps trying new hosts
• Worm has no malicious payload
• Where does the damage come from?
Damage

- One host may be repeatedly compromised
- Supposedly designed to gauge the size of the Internet
- The following bug made it more damaging.
- Asks a host whether it is compromised; however, even if it answers yes, still compromise it with probability $1/8$. 
Increasing propagation speed

• **Code Red, July 2001**
  – Affects Microsoft Index Server 2.0,
    • Windows 2000 Indexing service on Windows NT 4.0.
    • Windows 2000 that run IIS 4.0 and 5.0 Web servers
  – Exploits known buffer overflow in Idq.dll
  – Vulnerable population (360,000 servers) infected in 14 hours

• **SQL Slammer, January 2003**
  – Affects in Microsoft SQL 2000
  – Exploits known buffer overflow vulnerability
    • Server Resolution service vulnerability reported June 2002
    • Patched released in July 2002 Bulletin MS02-39
  – Vulnerable population infected in less than 10 minutes
Slammer Worms (Jan., 2003)

- MS SQL Server 2000 receives a request of the worm
  - SQLSERVR.EXE process listens on UDP Port 1434
Slammer’s code is 376 bytes long.

This byte signals the SQL Server to store the contents of the packet in the buffer.

UDP packet header

This is the first instruction to get executed. It jumps control to here.

The 0x01 characters overflow the buffer and spill into the stack right up to the return address.

Main loop of Slammer: generate new random IP address, push arguments onto stack, call send method, loop around.

NOP slide

The value overwrites the return address and points it to a location in sqlsort.dll which effectively calls a jump to %esp.

Restore payload, set up socket structure, and get the seed for the random number generator.
Nimda worm (September 18, 2001)

- **Key Vulnerability to Exploit**
  - A logic bug in IE’s rendering of HTML
  - Specially crafted HTML email can cause the launching of an embedded email

- **Vector 1:** e-mails itself as an attachment (every 10 days)
  - runs once viewed in preview plane

- **Vector 2:** copies itself to shared disk drives on networked PCs
  - Why this may lead to propagating to other hosts?
Nimda Worm

- Vector 3: Exploits various IIS directory traversal vulnerabilities
  - Use crafted URL to cause a command executing at
  - Example of a directory traversal attack:
    - http://address.of.iis5.system/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:
- Vector 4: Exploit backdoors left by earlier worms
- Vector 5: Appends JavaScript code to Web pages

```javascript
<script language="JavaScript">
window.open("readme.eml", null, "resizable=no,top=6000,left=6000")
</script>
```
Nimda worm

• Nimda worm also
  – enables the sharing of the c: drive as C$
  – creates a "Guest" account on Windows NT and 2000 systems
  – adds this account to the "Administrator" group.

• 'Nimda fix' Trojan disguised as security bulletin
  – claims to be from SecurityFocus and TrendMicro
  – comes in file named FIX_NIMDA.exe
    • TrendMicro calls their free Nimda removal tool FIX_NIMDA.com
Research Worms

- **Warhol Worms**
  - infect all vulnerable hosts in 15 minutes – 1 hour
  - optimized scanning
    - initial hit list of potentially vulnerable hosts
    - local subnet scanning
    - permutation scanning for complete, self-coordinated coverage
  - see paper by Nicholas Weaver

- **Flash Worms**
  - infect all vulnerable hosts in 30 seconds
  - determine complete hit list of servers with relevant service open and include it with the worm
  - see paper by Stuart Staniford, Gary Grim, Roelof Jonkman, Silicon Defense
Storm botnet

• First detected in Jan 2007
• Vectors (primarily social engineering):
  – Email attachments
  – Download program to show a video
  – Drive-by exploits
• DDoS spam fighting sites, and whichever host discovered to investigate the botnet
• Peer-to-peer communications among bots
  – for asking for C&C server
Conficker (November 2008)

- Also known as **Downup**, **Downadup** and **Kido**.
- Five variants
  - A (2008-11-21); B (2008-12-29); C (2009-02-20)
  - D (2009-03-04); E (2009-04-07)
- Estimated between 9 and 15 millions computers are compromised
- Microsoft offers $250,000 reward to catch creator
- Highly secure mechanism for updating itself.
- Several self-defense mechanism
  - Disable several security critical programs
  - Disable DNS lookup related to anti-virus vendors, and windows update
Conficker

- Vector 1: Vulnerability in (MS08-067)
  - Bulletin October 23, 2008
  - Vulnerability in MS Server service
  - Exploited by remote RPC request
  - Lead to code execution without authentication

- Vector 2: Dictionary attack on ADMIN$ share

- Vector 3: Creates DLL-based AutoRun trojan on attached removable drive

Why is it able to compromise more hosts than SQL slammer & code red?
Readings for This Lecture

- Wikipedia
  - Morris Worm
  - Conficker
Coming Attractions …

- Dealing with Malwares