## Worms , Trojan Horses and Root Kits

## Worms

- A worm is a type of Virus that is capable of spreading and replicating itself autonomously over the internet.

- “Famous” Worms
  - Morris Internet worm (1988)
  - Currently:
    - Ramen Worm
    - Lion worm
    - Adore Worm

## Ramen Worm

- First discovered in January of 2001
- Attacks RedHat Linux 6.2, 7.0 systems
- The worm randomly selects a class B address and attempts to use well known exploits against rpc.statd, wu-ftpd and LPRng to gain access

## Ramen Worm: Detection

- If you're running a web server, the worm replaces your index.html with the page on the following slide.

- Starts a http daemon on tcp port 27374 for newly infected hosts to download code *index.html*

# RameN Crew

Hackers looooooooooooooooove noodles™

This site powered by

## Ramen Worm: Countermeasures

- Apply vendor patches for vulnerable services
- Note: The worm patches the holes it used to gain access so no other system cracker can get in. (Isn't that nice of them!)

## Lion Worm

- Exploits weakness in BIND to gain root access
- Listens on port 27374
- Sends out email to huckit@china.com with /etc/passwd, /etc/shadow and network settings
- Randomly generates class B network addresses to scan
- Scans network for exploitable hosts

## Lion Worm (cont'd)

- Once it exploits a host, it installs the tOrn root kit.
- Ports 60008/tcp and 33567/tcp get bound to a backdoor root shell
- A trojaned version of SSH gets bound to 33568/tcp

## Lion Worm: Detection/Countermeasures

- Apply latest vendor patches
- A system integrity checker will detect the presence of modified binaries
- Scan hosts/network for open signature ports
- Use IDS to detect Lion Worm traffic
- Lionfind is a utility that checks for the presence of the binaries/ports associated with Lion

## Adore Worm

- First appeared around April 1, 2001
- Similar to Ramen and Lion
- Exploits BIND, rpc.statd, LPRng on Redhat Linux systems
- Emails information, including /etc/passwd to a few different email addresses
- Countermeasures:
  - Same as other worms
  - Adorefind utility will detect it on a system.

## Trojan Horses

- A program which appears to be legitimate, but performs unintended actions.
- Trojan Horses can install backdoors, perform malicious scanning, monitor system logins and “su”.

## Back Doors

- A Backdoor allows a malicious attacker to maintain privileged access to a compromised host
- Unix back doors are typically installed via a Worm, Root Kit or manually after a system has been initially compromised
- Windows back doors are typically installed via a Virus, Worm or Trojan Horse.
  - Virus and Worms via Email, sharing infected files, Open Windows shares
  - Trojan Horses typically included with “legitimate” application such as a game etc.

## Windows Backdoors

- Back Orifice
- Back Orifice 2000 (BO2K)
- NetBus
- WinVNC (Virtual Network Computing)
- SubSeven

## Back Orifice/BO2k

- A “Remote Administration” tool for windows 9x and NT.
- Runs on remote system without user knowing
- Client can control several servers simultaneously
- Allows client complete control over server system including logging all keystrokes at the console. (Passwords, email, etc)
- By default server listens on tcp 54320 or udp 54321

## BO/BO2k: Countermeasures

- Password protect all windows file shares
- Run Anti-virus software. (Most detect BO/BO2k)
- Configure Firewall/IDS system to watch ports 54320 and 54321
- Check hosts and scan network for those open ports on systems
- Buttsniff, BO Detect, BOPing, BORED are all tools to detect the presence of BO

## Netbus

- Provides "Remote Administration" of Windows 9x and NT systems
- Allows full control over windows and devices.
  - (open and close windows remotely, Screen capture, open and close CDROM tray)
- Logs keystrokes
- Listens on TCP/UDP 12345 and 12346 (configurable v 1.7 and up) for connections
- Listens on TCP/UDP 20034 (v.2.x) for connections

## Netbus: Countermeasures

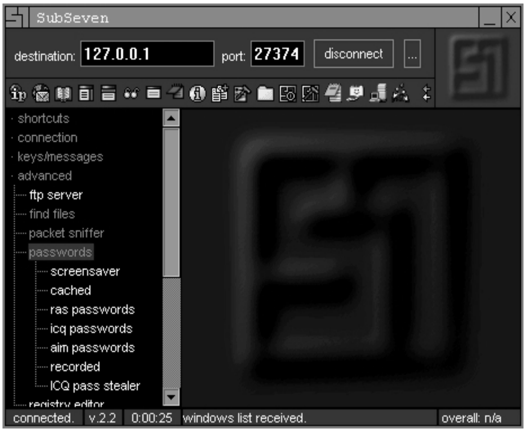
- Password protect windows file shares
- Run Anti-virus software (Most detect Netbus)
- Looks for open signature ports (Locally or scan the network)
- NetBuster is a program that runs on the local system to detect Netbus

## SubSeven

- Windows “remote administration” utility.
- Allows full control over windows and devices.
- Many features not found in other remote admin. Tools
  - get Windows CD-Key
  - retrieve dialup usernames/passwords, phone numbers
  - AOL/Microsoft/Yahoo - IM spy
  - ICQ hijacking

## SubSeven: Client

- www.sub7files.com
- Easy to use interface
- Extremely configurable



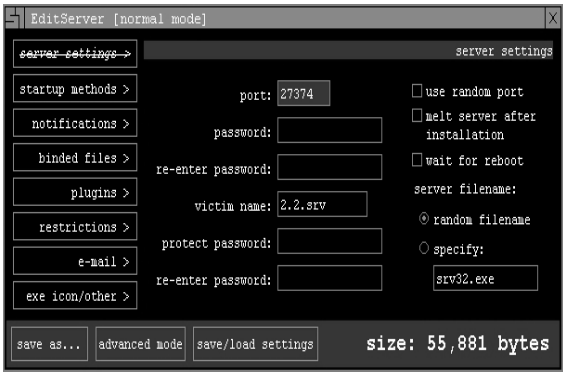
SubSeven

destination: 127.0.0.1 port: 27374

connected. v.2.2 0:00:25 windows list received. overall: n/a

## SubSeven: Server

- Easy to use interface
- Extremely configurable



EditServer [normal mode]

port: 27374

password:

re-enter password:

victim name: 2.2.srv

protect password:

re-enter password:

□ use random port

□ melt server after installation

□ wait for reboot

server filename:

● random filename

○ specify: srv32.exe

size: 55,881 bytes

## SubSeven: Countermeasures

- Password protect windows file shares
- Run Anti-virus software (Most detect Netbus)
- Check hosts and scan the network for open signature ports.
- Run IDS system to detect SubSeven traffic

## Unix Backdoors

- Backdoors on Unix are typically a shell bound to a network port.
  - A remote attacker can connect to the network port and execute commands
- A trojaned daemon such as SSH (included in a root kit) may provide root access without a password.

## Root Kits

- A rootkit is a collection of tools that allows the hacker to provide a backdoor to the system, collect information about other hosts on the network, mask the fact that the system is compromised
- Hides the intruder’s activity on the system
- Allows intruder to keep the privileged access - NOT to initially obtain it
- Root Kits are Trojan Horses and typically provide a Back Door.
- Most root kits can be detected by running an integrity checker such as Tripwire

## T0rn Kit

## T0rn Kit: Detection

## Knark

- Kernel based root kit for Linux using Loadable Kernel Module
- Hide files
- Hide running processes
- Hide active network connections
- Change the user and group permissions of running processes

## Knark: Detection

- Processes hidden by Knark, and Knark itself can be unhidden by sending a “kill -32” to the process.
- By sending a “kill -32” to every possible process ID, you can unhide Knark
- LIDS: Linux Intrusion Detection System
  - “Seals” the kernel from modification
  - Prevents loading and unloading of kernel modules
  - Locks shared memory segments
  - Protects sensitive /dev/ files
  - Protects against process ID manipulation