

How Hackers Attack Networks



This presentation is based on a PowerPoint by security expert Adrian Crenshaw.
You can view his original presentation [here](#).



Common platforms for attacks

- Windows 98/Me/XP Home Edition
- Linux, OpenBSD, Trinux, and other low-cost forms of UNIX



Local and remote attacks

- Local: Attacks performed with physical access to the machine
- Remote: Attacks launched over the network



Why worry about local attacks on workstations?

- Hackers can collect more information about a network and its users.
- Hackers can obtain the administrator password on a workstation, which can lead to server access.
- Spyware can be installed to gather more sensitive information.



Common local attacks

- Getting admin/root at the local machine
 - Windows Workstation: Rename or delete
c:\winnt\system32\config\SAM
 - Linux: at LILO prompt, type **linux s**
- Cracking local passwords
 - L0phtcrack (LC)
- Removing hard drive to install in another box
- Exploiting files or commands available upon login
 - C:\Documents and Settings\All Users\Start Menu\Programs\Startup
 - Registry commands, such as adding users



Cracking over the network: A four-step program

1. Footprinting
2. Scanning and enumerating
3. Researching
4. Exploiting



Footprinting

Finding out what an organization owns:

- Find the network block.
- Ping the network broadcast address.



Scanning and enumerating

- What services are running?
- What accounts exist?
- How are things set up?



Scanning and enumerating: Methods and tools

- Port scanning

- Nmap

- Sniffing

- ngrep

- SNMP

- Solarwinds

- Null session

- NBTenum

- Nbt dump



Scanning and enumerating: Methods and tools (cont.)

- Null session

- NBTenum
- Nbt dump

- NetBIOS browsing

- Netview
- Legion

- Vulnerability
scanners

- Nessus
- Winfingerprint
- LANGuard



Researching

Researching security sites and hacker sites can reveal exploits that will work on the systems discovered during scanning and enumerating.

- <http://www.securityfocus.com/>
- <http://www.networkice.com/advice/Exploits/Ports>
- <http://www.hackingexposed.com>
- <http://www.ntsecurity.net/>
- <http://www.insecure.org/>



Exploits

- Brute force/dictionary attacks
- Software bugs
- Bad input
- Buffer overflows
- Sniffing



Countering hackers

■ Port scanning

- Block all ports except those you need
- Block ICMP if practical
- NT: IPsec; Linux: iptables

■ Sniffing

- Use switched media
- Use encrypted protocols
- Use fixed ARP entries



Countering hackers (cont.)

■ Null sessions

- Set the following registry value to 2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous]

■ Use IDS

- Snort
- BlackICE



Identifying attacks

- On Windows, check the event log under Security.
- On Linux, check in `/var/log/`.
- Review IIS logs at `\winnt\system32\LogFiles`.
- Check Apache logs at `/var/log/httpd`.



Administrative shares:

- Make life easier for system admins.
- Can be exploited if a hacker knows the right passwords.
- Standard admin shares:
 - Admin\$
 - IPC\$
 - C\$ (and any other drive in the box)



Control the target

- Establish connection with target host.
 - `net use \\se-x-x\ipc$ /u:se-x-x\administrator`
- Use Computer Management in MMC or Regedit to change system settings.
- Start Telnet session.
 - `at \\ se-x-x 12:08pm net start telnet`
- Turning off file sharing thwarts these connections.



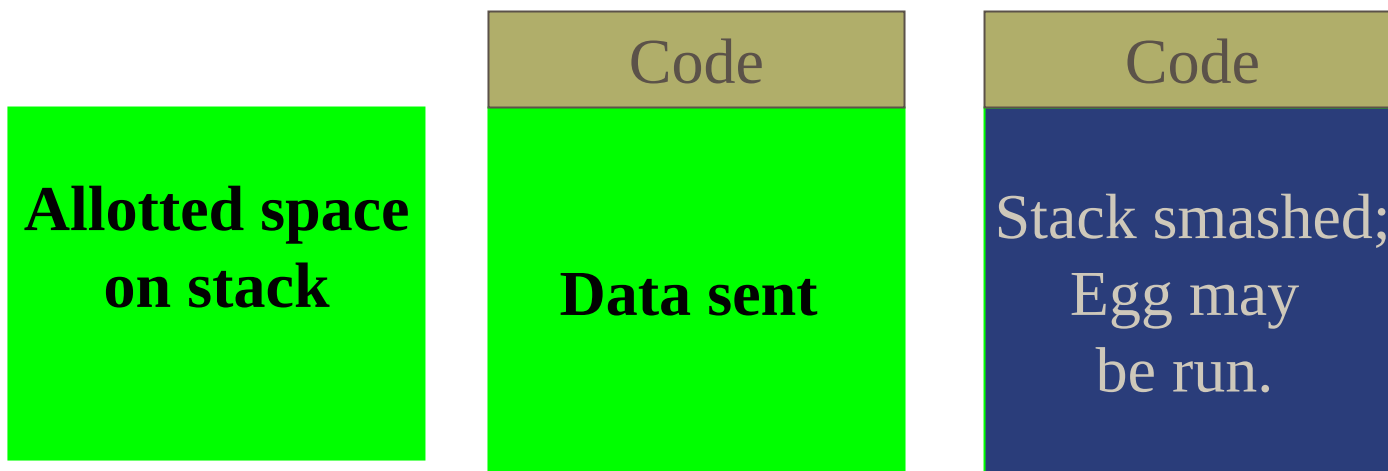
Counters to brute force/dictionary attacks

- Use good passwords.
 - No dictionary words
 - Combination of alpha and numeric characters
 - At least eight-character length
- Use account lockouts.
- Limit services.
 - If you don't need, it turn it off.
- Limit scope.

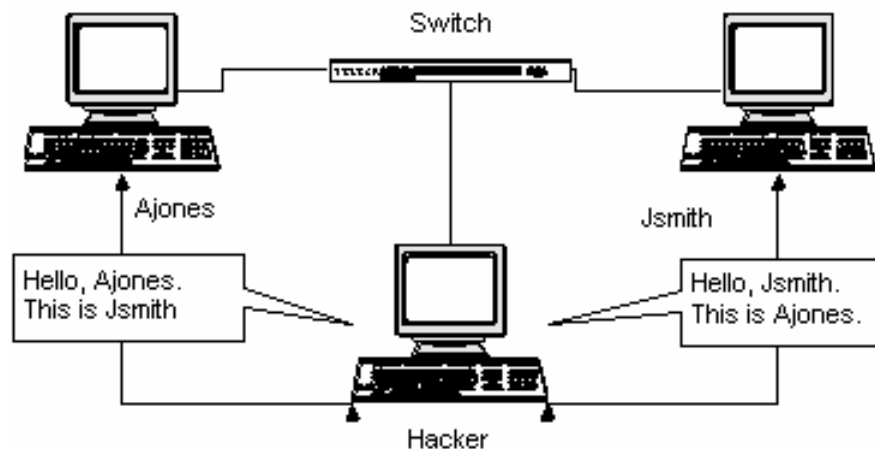


Buffer overflow

Cracker sends more data then the buffer can handle, at the end of which is the code he or she wants executed.



Hacker = Man in the middle





Sniffing on local networks

- On Ethernet without a switch, all traffic is sent to all computers.
- Computers with their NIC set to promiscuous mode can see everything that is sent on the wire.
- Common protocols like FTP, HTTP, SMTP, and POP3 are not encrypted, so you can read the passwords as plain text.



Sniffing: Switched networks

- Switches send data only to target hosts.
- Switched networks are more secure.
- Switches speed up the network.



ARP Spoofing

Hackers can use programs like arpspoof to change the identify of a host on the network and thus receive traffic not intended for them.



ARP spoofing steps

1. Set your machine to forward packets:

Linux: `echo 1 > /proc/sys/net/ipv4/ip_forward`
`echo 1 > /proc/sys/net/ipv4/ip_forward`

BSD: `sysctl -w net.inet.ip.forwarding=1`

2. Start arpspoofing (using two terminal windows)

`arpspoof -t 149.160.x.x 149.160.y.y`

`arpspoof -t 149.160.y.y 149.160.x.x`

3. Start sniffing

`ngrep host 149.160.x.x | less`

OR

`Dsniff | less`



Counters to ARP spoofing

- Static ARP tables
- ARPWatch
 - Platforms: AIX, BSDI, DG-UX, FreeBSD, HP-UX, IRIX, Linux, NetBSD, OpenBSD, SCO, Solaris, SunOS, True64 UNIX, Ultrix, UNIX



IP spoofing:

- Fakes your IP address.
- Misdirects attention.
- Gets packets past filters.
- Confuses the network.



DoS

Denial of service attacks make it slow or impossible for legitimate users to access resources.

■ Consume resources

- Drive space
- Processor time

■ Consume Bandwidth

- Smurf attack
- DDoS



SYN flooding

- Numerous SYN packets are transmitted, thus tying up connections.
- Spoofing IP prevents tracing back to source.

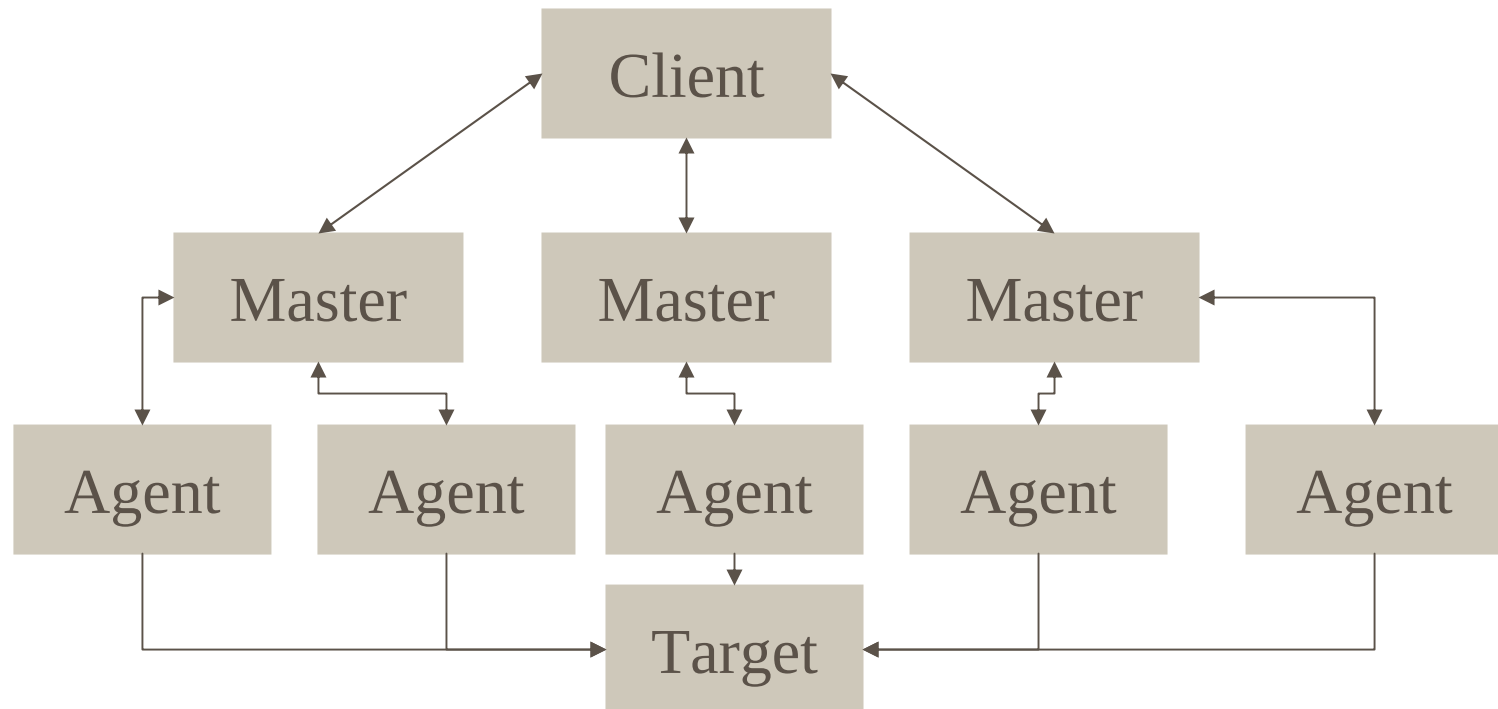


Smurf attack

- Ping requests are sent to the broadcast address of a Subnet with a spoofed packet pretending to be the target.
- All the machines on the network respond by sending replies to the target.
- Someone on a 56K line can flood a server on a T1 by using a network with a T3 as an amplifier.
 - Example command:
`nemesis-icmp -I 8 -S 149.160.26.29 -D 149.160.31.255`

Distributed denial of service

Use agents (zombies) on computers connected to the Internet to flood targets.





Common DDoS zombie tools:

- Trinoo
- TFN
- Stacheldraht
- Troj_Trinoo
- Shaft

Sniff the network to detect them or use [ZombieZapper](#) from Razor Team to put them back in their graves.