This talk: Common Remote Exploitation Techniques

A recent case study.

Common attacks on networks.

Common defenses.
A Case Study: Freedom Hosting

- Attacking Tor Hidden service: Lecture 14
- XXS attack? Lecture 12
- Memory attack? Lecture 17
- JavaScript on website attack: Lecture 13
- Attack binary analysed using IDA pro: Lecture 17

The injected shell code sent the browsers IP address and info to a server.

The FBI recently admitted they carried out the attack.
What are the attack vectors?

WebServer
Comp1
DataBase
Comp2
E-mail Server
SSH/RDP
Web Proxy
...
NAT
Wi-Fi
Some Common Attack Vectors

- Attacks on Web Page
- Attacks from incoming e-mail
- Attacks on all servers
- Local attacks via wi-fi
- Insider attacks.
Footprinting

• Find out as much as possible about the business’s footprint.
  – What does it do?
  – What does it provide for its employees?
  – What IP addresses does it use?
  – How does user contact support?

• Lots of this information is on a companies website.
Footprinting

• Web searchers for the company can also provide a lot of information.

• WHOIS and DNS lookup will tell an attacker all the IP address range used by a business.

• traceroute may reveal the IP address of routers.
  – These routers may use default passwords
Scanning and Enumeration

• Find out what services are running

• What version of each service.

• What operating system.
nmap

- nmap is a network mapping tool.
- It can tell you want ports are open.
- It will try to guess the service.
- By default does TCP on low ports only.
  - Can also do UDP and any ports.
Fingerprint

• What is the OS?

• Different OS will set different values in the IP & TCP packets.
  – TCP sequence number
  – IP packet time to live.

• Find OS with nmap –A or namp -O
More advanced Nmap Scanning

• Stateless firewalls may block incoming SYN but not incoming ACK.

• Statefull firewalls make block incoming ACK but not incoming SYN.

• Nmap has can scan with both -PS and –PA and many other scan options.

• See http://www.youtube.com/watch?v=Hk-21p2m8YY
Check for default/common logins

• Are any services using the default passwords?

• e.g. ssh is used for remote login (port 22)

• Default password for jail broken iPhones was “alpine” (big attack on iPhones 2 years ago).
Footprinting and Scanning

• Ensure that as little information about the company appears publically.
  – Password protect parts of the website

• External attacker can always find the IPs and open ports on the public computers.

• In the worst case they can find the entire network architecture.

• Internal attackers are harder to stop
Search for Known Exploits

• There are many databases of vulnerabilities on the web e.g.

  http://cve.mitre.org/
  http://nvd.nist.gov/
  http://metasploit.com/modules/
Search for Known Exploits

• Finding and “weaponizing” a buffer overflow can take 6 months for a team of experts.

• So most hacker “script kiddies” use exploit code someone else has written.

• You are much more likely to be attacked via a known exploit, than a new one.
Metasploit

• Metasploit is a framework to perform memory attacks and deliver payloads
  – You select the module for the exploit.
  – The payload is the “arbitrary code” the victim system will run.

• The legitimate use of Metasploit is to test your own system for weaknesses.

• Never run it against a system you don’t own, without written permission.
What an attacker might do once they have access.

- Install RootKit
- Steal password file, credit card numbers, personal data.
- Create new user accounts and back doors.
- Replace existing libraries and application with malware.
- Log key strokes.
- Send Spam
- Performs DoS attacks
Defenses: Firewalls

- Firewalls block Internet traffic.
- May be on the computer (host) or built into a router (network).
- Firewalls can be stateless or statefull.
- Stateless firewalls could e.g. block all traffic not on port 80.
Defenses: Firewalls

- Stateful Firewalls record the traffic and use it to make future decisions.
- E.g. block incoming connection but allow outgoing connections.
- Can’t firewall services used by outside world.
A Typical Business Network

Payment Gateway e.g. Authorize.net

DMZ
WebServer
E-mail Server
NAT Proxy

Credit Card Processing
Comp1
Comp2
...

DataBase
Wi-Fi
Defenses: Fast Patches

- Most importantly of all
- Make sure all security patches are installed immediately.
- There is almost always a patch to stop any well known exploit.
Defenses: Anti-Virus

- Anti-Virus products scan the computer for known malware.
- Can also scan e-mail and network traffic
- Only as good as the last update.
- Can be disabled by an attacker with admin access.
Defenses: Intrusion Detection Systems

• A good system administrators will monitor their network.

• IDSs look at all packets (like wireshark) and report suspicious behavior.

• Can catch nmap and metasploit.

• E.g. Snort: www.snort.org
IDS: Snort Rules:

action proto src_ip src_port direction
dst_ip dst_port (options)

e.g.

alert tcp $WEB_SERVER !80 -> any any
msg:"Web Server making out going connection";

alert any 80 -> any any msg:"Active X attack";
content:"clsid:A105BD70-BF56-4D10-BC91-41C88321F47C"
Top Defenses:

1. Apply patches
2. Firewall
3. Anti-Virus
4. Intrusion Detection Systems
5. Check file hashes
6. Good password and user policies

First 2 should be fine for Linux or Mac, first 3 for windows. All 6 if you are a sys. admin.
Some things to try:

- Nmap scans on your home network
- Watch the nmap video linked to from the lectures page.
- Set up your firewall, on host and router.
- Install and set up snort.
- Search Metasploit for exploits against the oldest computer you have.
Conclusion

Attackers will:

• Scan your machines,
• Identify the services running,
• Try to use known exploits against these services.

Defend the system:

• Monitor for attacks, e.g. Anti-virus,
• Firewall to block unused ports,
• Apply Security Patches a.s.a.p
Next Lecture:

• What attackers are actually doing on the Internet
  – Virus, Worms and Trojans
  – DDoS
  – Phishing attacks.
  – Botnets
  – APTs.