

Common System Exploits

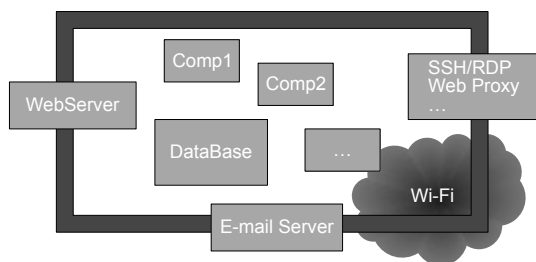
Tom Chothia
Computer Security, Lecture 17

This talk: Common Remote Exploitation Techniques

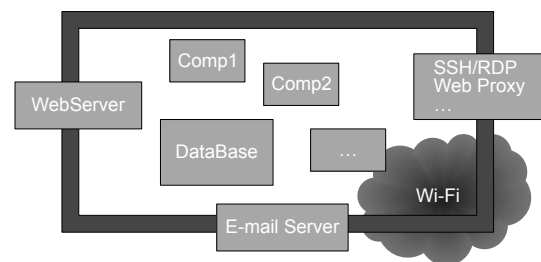
How does an attacker end up running the metasploit attack we saw last week against your system?

- Footprinting
- Scanning and Enumeration
- Exploiting services
- After gaining access

A Typical Business Network



What are the attack vectors?



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 company's 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

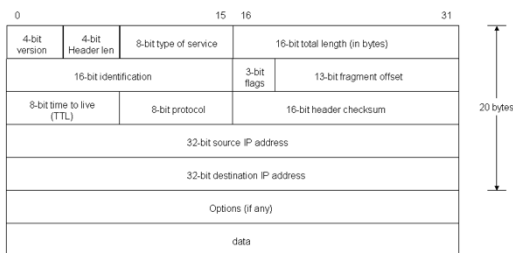
Scanning and Enumeration

- Find out what services are running
- What version of each services.
- What operating system.

nmap

- nmap is a network mapping tool.
- It can tell you what 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.

IP PACKET HEADER



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`

Check for default 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 this time last year).

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

Check for Public Files

- NetBios: Network Basic Input/Output System
- For sharing files across a network.
- Does the user have any public readable files?
`smbclient -L host -I IP address`

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 attack might do once they have access.

- Steal password file.
- Create new user accounts and back doors.
- Replace existing libraries and application with malware.
- Log key strokes.
- Send Spam
- Performs DoS attacks
- ...

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

Anti-Virus

- Anti-Virus products scan the computer for known malware.
- Can also scan e-mail.
- Only as good as the last update.
- Can be disabled by an attacker with admin access.

Defenses: Firewalls

- Firewalls can block most Internet traffic.
- May be on the computer or built into a router.
- Could for example block all traffic not on port 80.
 - Would stop the attack in this talk.
- Can't firewall services used by outside world.

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.

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.

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:

- Trusted Computing:
- Using hardware to provide security and control remote computers.