Gaining Access

Everything is a Computer

Two main approaches

Server Side

Do not require user interaction, all we need is a target IP!

Start with information gathering, find open ports, OS, installed services, and work from there.

Client Side

Require user interaction, such as opening a file, a link.

Information gathering is key here, create a trojan and use social engineering to get the target to run the it.

What if the target uses the same network as us??

1. Server Side Attacks

- Need an IP address.
- Very simple if target is on the same network (netdiscover or zenmap).
- If target has a domain, then a simple ping will return its IP.

```
> ping www.facebook.com
```

- Getting the IP is tricker if the target is a personal computer, might be useless if the target is accessing the internet through a network as the IP will be the router IP and not the targets, client side attacks are more effective in this case as reverse connection can be used.

1. Server Side Attacks

Information Gathering

- Try default password (ssh iPad case).
- Services might be mis-configured, such as the “r” service. Ports 512, 513, 514
- Some might even contain a back door!
- Code execution vulnerabilities.

1. Server Side Attacks

Metasploit

Metasploit is an exploit development and execution tool. It can also be used to carry out other penetration testing tasks such as port scans, service identification and post exploitation tasks.

> msfconsole – runs the metasploit console
> help – shows help
> show [something] – something can be exploits, payloads, auxiliaries or options.
> use [something] – use a certain exploit, payload or auxiliary.
> set [option] [value] – configure [option] to have a value of [value]
> exploit – runs the current task

1. Server Side Attacks

Metasploit Community

Metasploit community is a GUI that can discover open ports and installed services on the target machine, not only that but it maps these services to metasploit modules and exploits and allow us to run these modules from the web GUI.

1. Download it from https://www.rapid7.com/products/metasploit/metasploit-community-registration.jsp
2. Change permissions to executable.
   ```
   > chmod +x [installer file name]
   ```
3. Run installer
   ```
   > ./[installer file name]
   ```
4. Once complete, metasploit community can be started as a service.
   ```
   > service metasploit start
   ```
5. Now navigate to https://localhost:3790 and enter your product key.

1. Server Side Attacks

Nexpose

Nexpose is a vulnerability management framework, it allows us to discover, assess and act on discovered vulnerabilities, it also tells us a lot of info about the discovered vulnerabilities, weather they are exploitable and helps us write a report at the end of the assessment.

1. Download it from http://www.rapid7.com/products/nexpose/compare-downloads.jsp
2. Stop postgresql `> service postgresql stop`
3. Change permissions to executable. `> chmod +x [installer file name]`
4. Run installer `> ./[installer file name]`