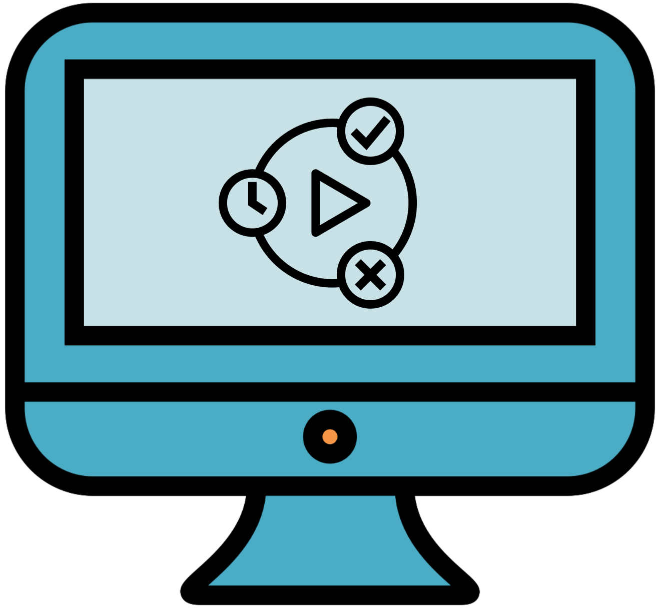
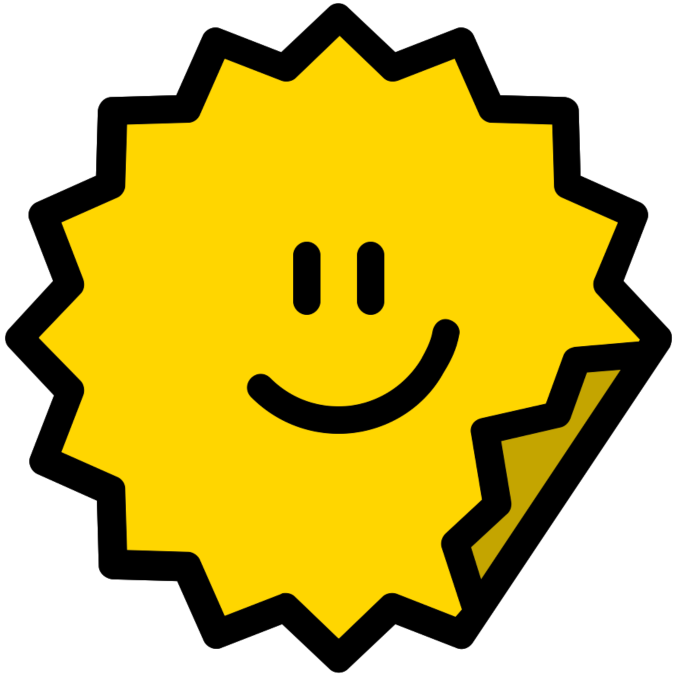
Overview



Test to evaluate:

- Strengths of all security controls
  - Procedurals
  - Operational
  - Technological

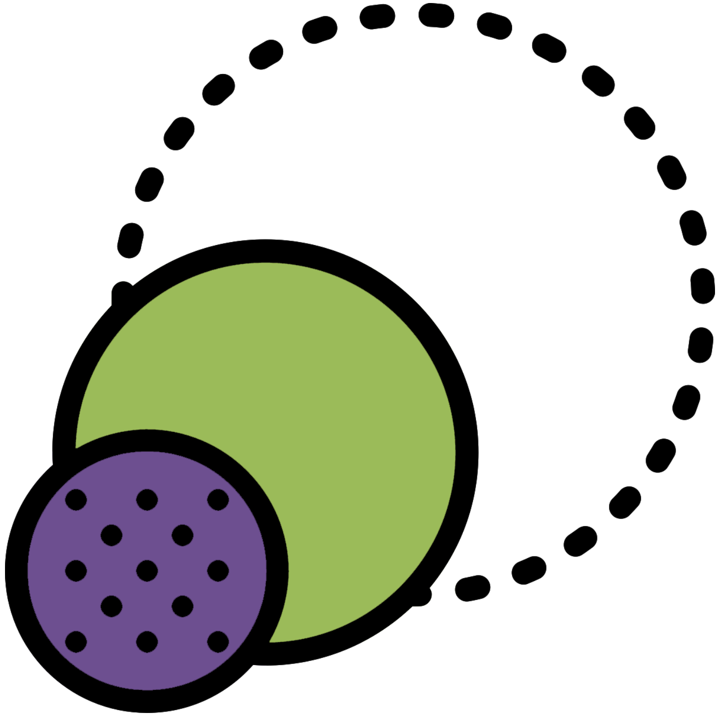
Overview



Benefits:

- Security of network
- Discovery of Vulnerabilities
- Demonstration of Threats

Overview



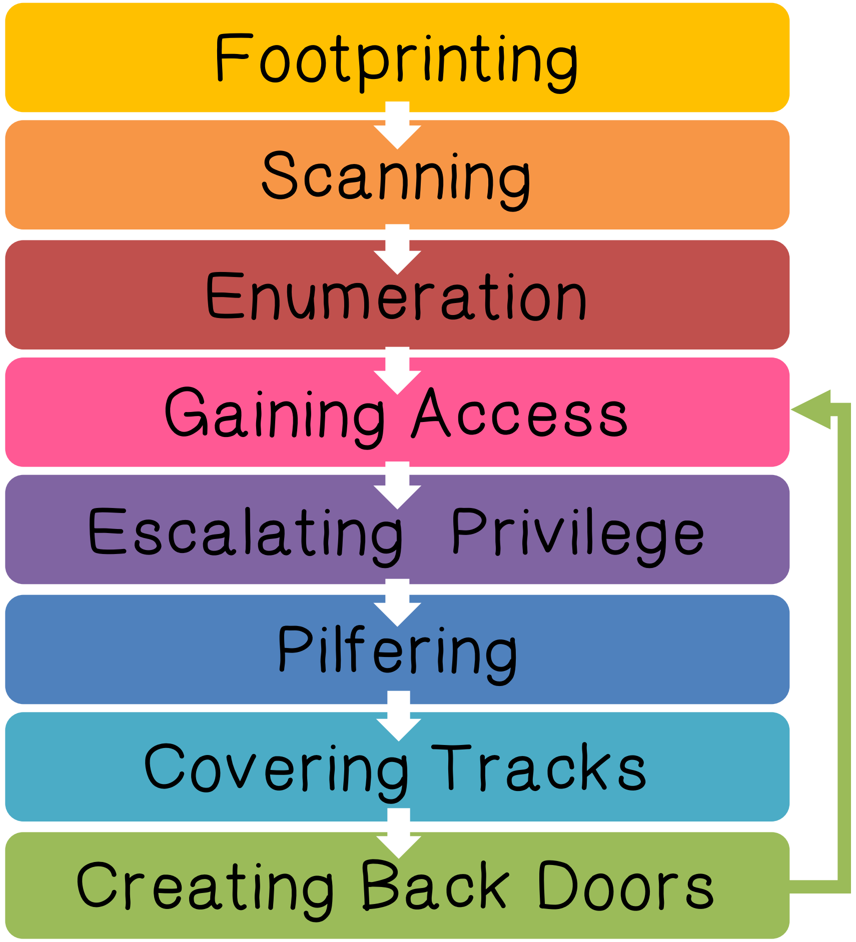
Scope:

- Can include social engineering, physical access

Scale:

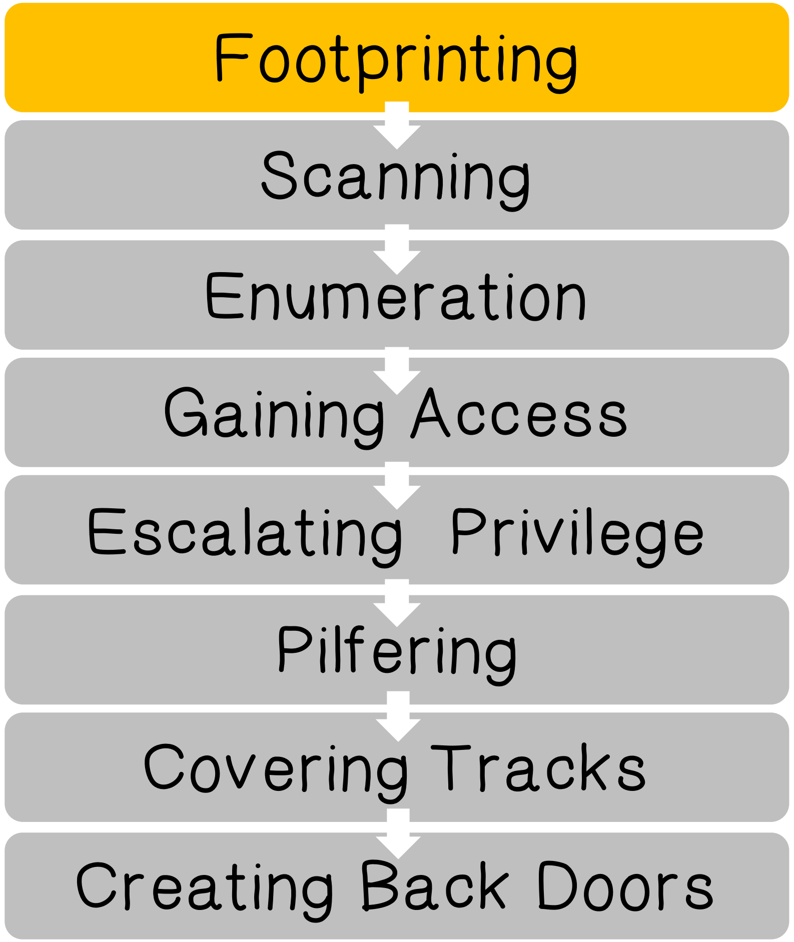
- Security of network

Methodology



Footprinting	whois, nslookup
Scanning	Nmap, fping
Enumeration	dumpACL, showmount legion, rpcinfo
Gaining Access	Tcpdump, Lophtcrack NAT
Escalating Privilege	Johntheripper, getadmin
Pilfering	Rhosts, user data, Config files, registry
Covering Tracks	zap, rootkits
Creating Back Doors	Cron, at, startup folder netcat, keystroke logger remote desktop

Footprinting



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

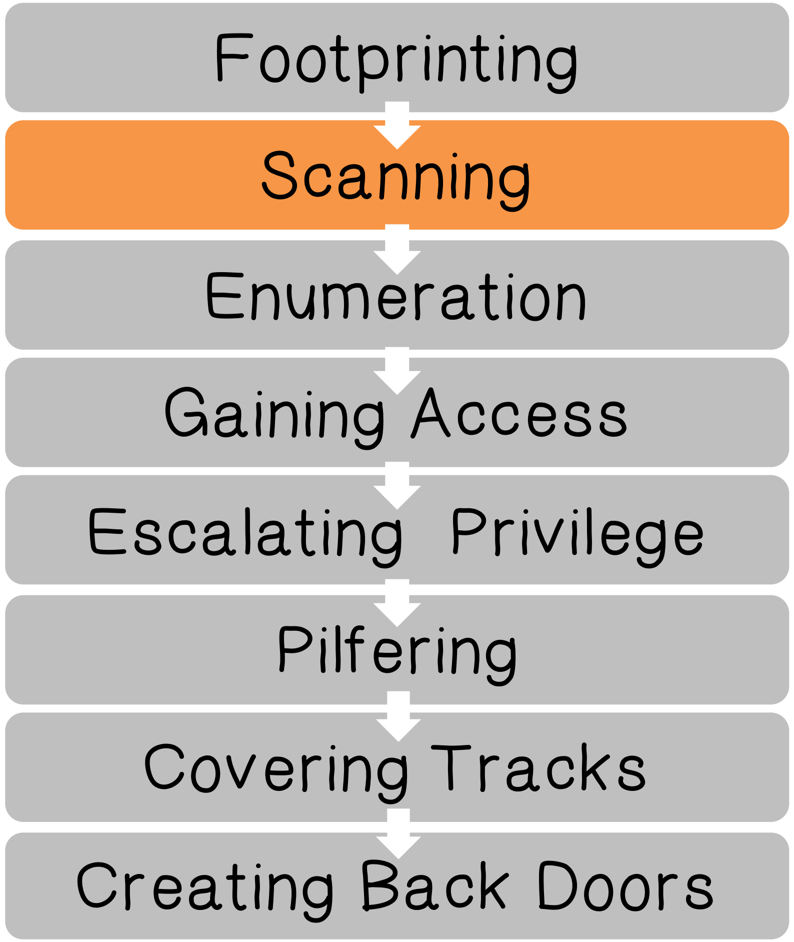
- Reconnaissance and information gathering
- Find out target IP address/phone number range
- Namespace acquisition
- Network Topology (visualRoute)
- Essential to a “surgical” attack

Footprinting

Footprinting

Techniques	Open Source search	Find domain name, admin, IP addresses name servers	DNS zone transfer
Tools	Google, search engine, Edgar	Whois (Network solution; arin)	Nslookup (ls –d) dig Sam Spade

Scanning



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

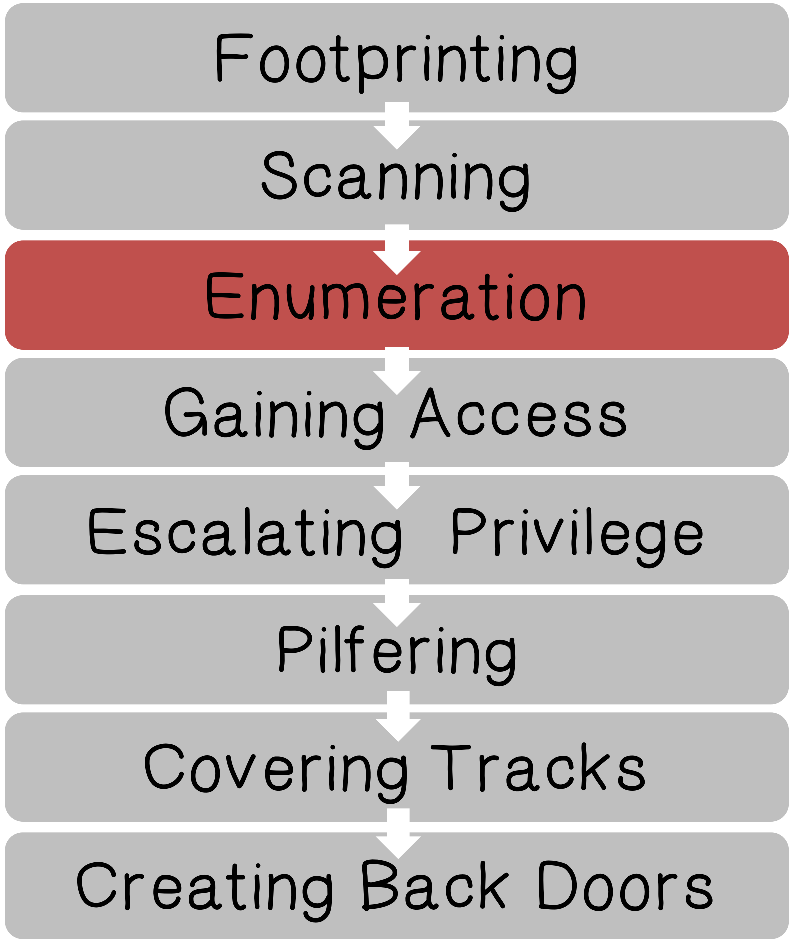
- Which machine is up and what ports are open
- Which services are running
- Their versions and configurations
- Look up corresponding vulnerability info on the web
- Focus on most promising avenues of entry
- Reduce frequency of scanning and randomize the ports or IP addresses to be scanned in the sequence

Scanning

Scanning

Techniques	Ping sweep	TCP/UDP port scan	OS detection
Tools	Fping, icmpenum WS_Ping ProPack nmap	Nmap Superscan fscan	Nmap queso siphon

Enumeration



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

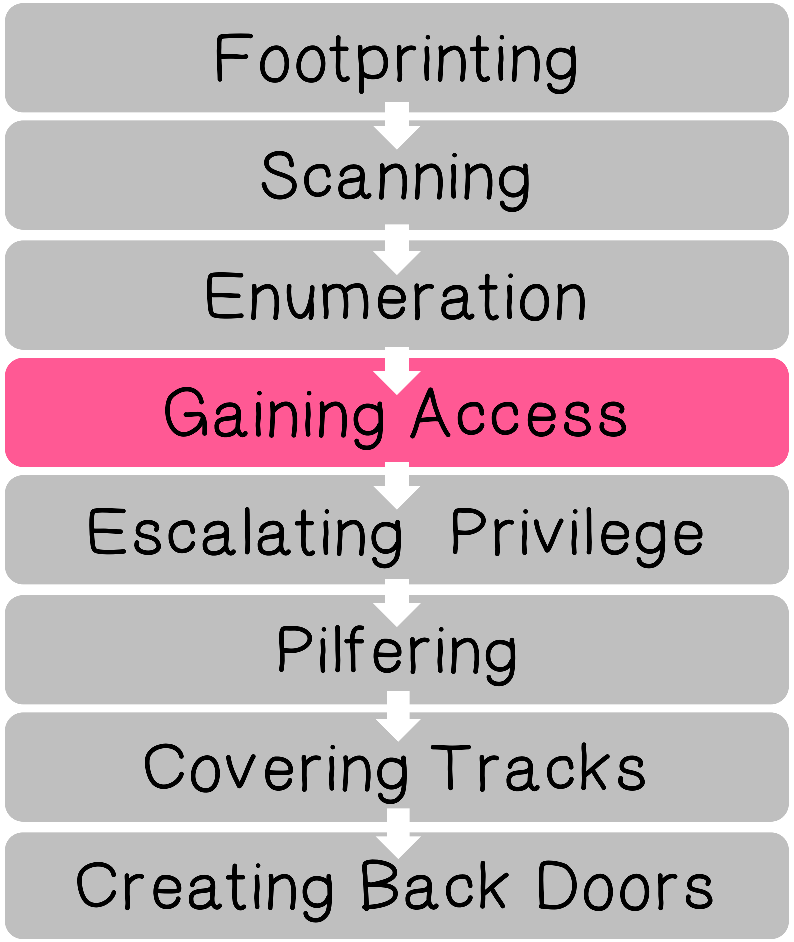
- Identify valid user accounts or poorly protected resource shares
- More intrusive probing than scanning step

Enumeration

Enumeration

Techniques	List user accounts	List file shares	Identify applications
Tools	Null sessions DumpACL Sid2usre onSiteAdmin	Showmount NAT legion	Banner grabbing with telnet or netcat, rpcinfo

Gaining Access



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

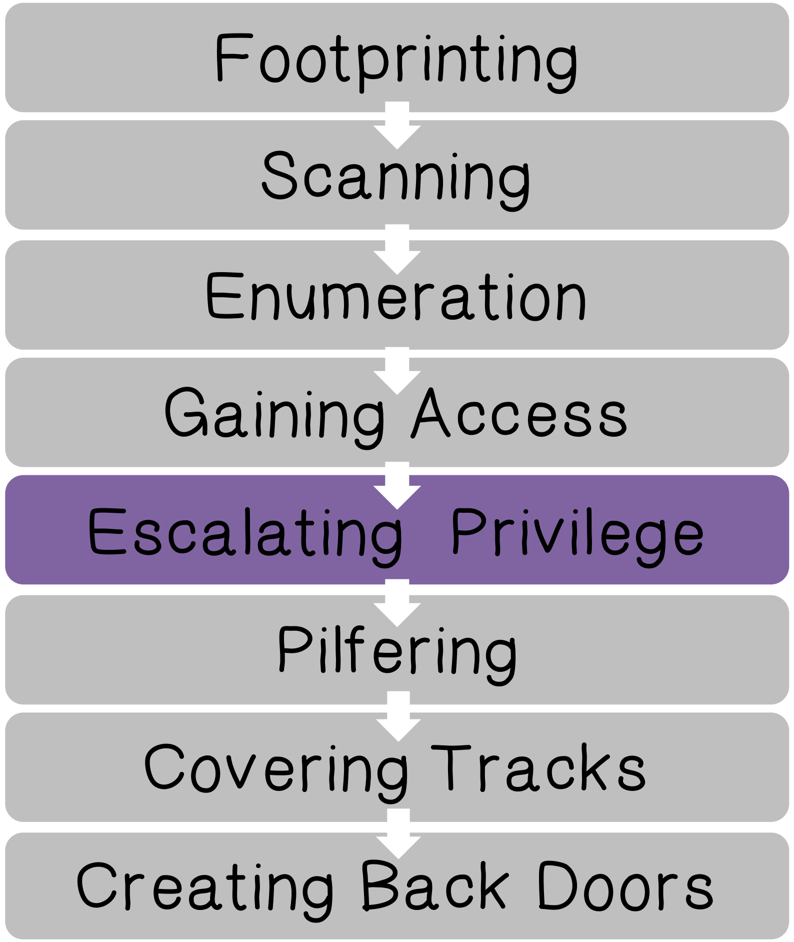
- Identify a vulnerability of the target from scanning
- Exploit it
  - Often with existing tool/script; may need modifications
- In general, automatically generating a working exploit from a new vulnerability is still an open problem

Gaining Access

Gaining Access

Techniques	Password eavesdropping	File share brute forcing	Password file grab	Buffer overflow
Tools	tcpdump/ssldump L0phtcrack readsmb	NAT legion	tftp pwddump2	ttdb, bind IIS .HTR/ISM.DLL

Escalating Privilege



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

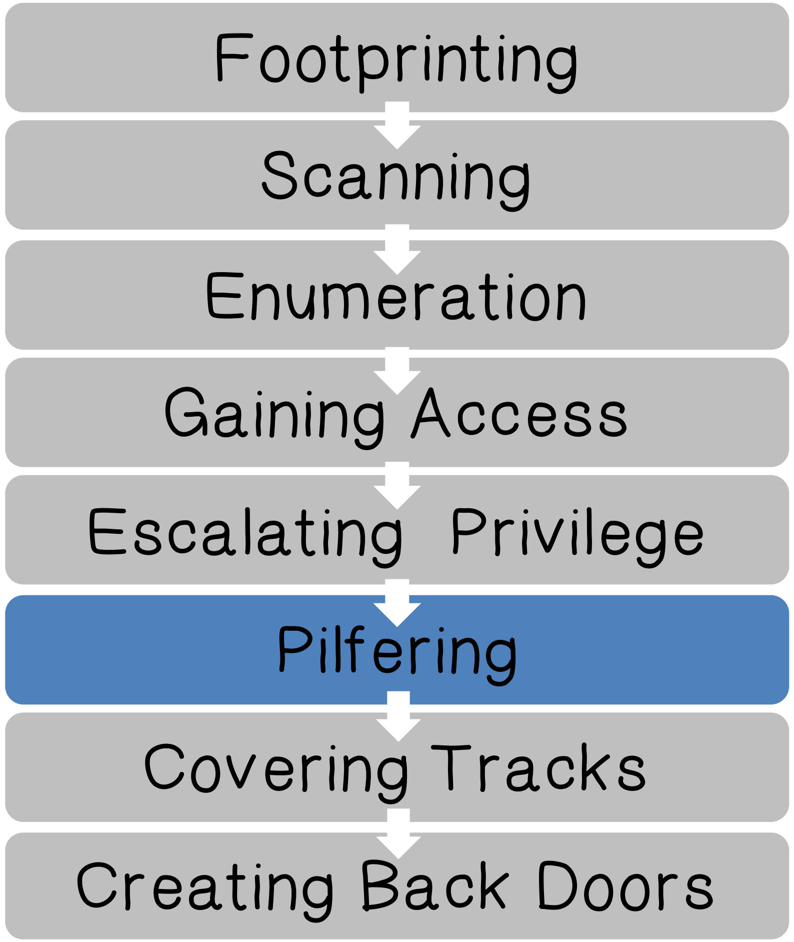
- If only user-level access was obtained in the last step, seek to gain complete control of the system

Escalating Privilege

Escalating Privilege

Techniques	Password cracking	Known Exploits
Tools	John the ripper L0phtcrack	Lc_messages, Getadmin, sechole

Pilfering



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

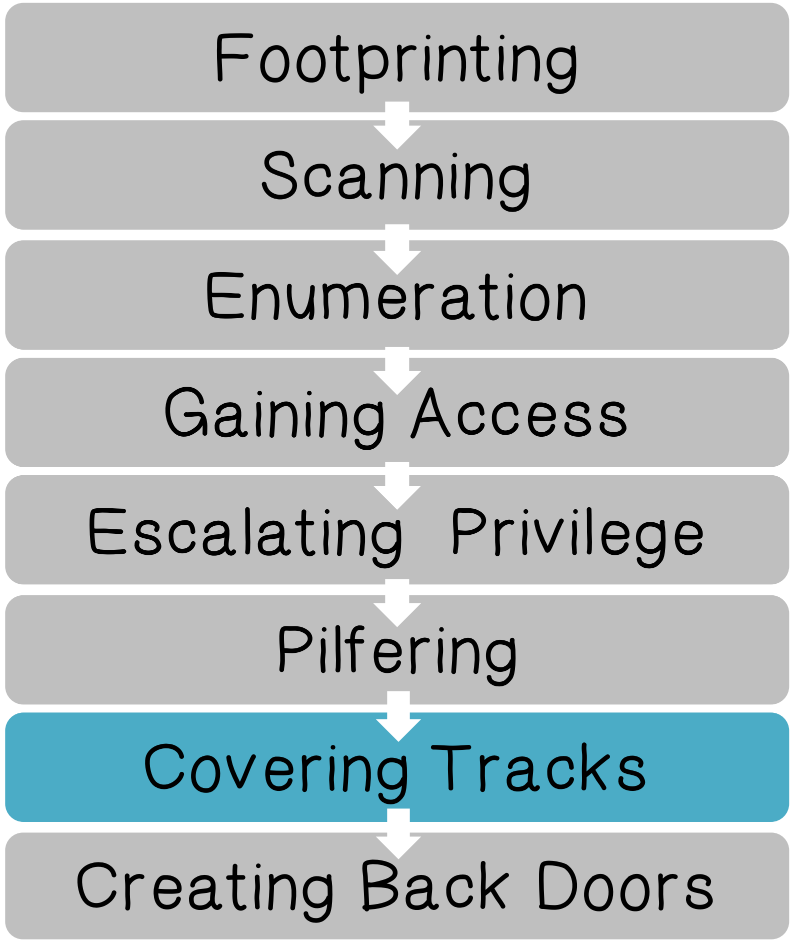
- Gather info to allow access of trusted systems

Pilfering

Pilfering

Techniques	Evaluate Trusts	Search for cleartext passwords
Tools	rhosts LSA secrets	User data, Configuration files Registry

Covering Tracks



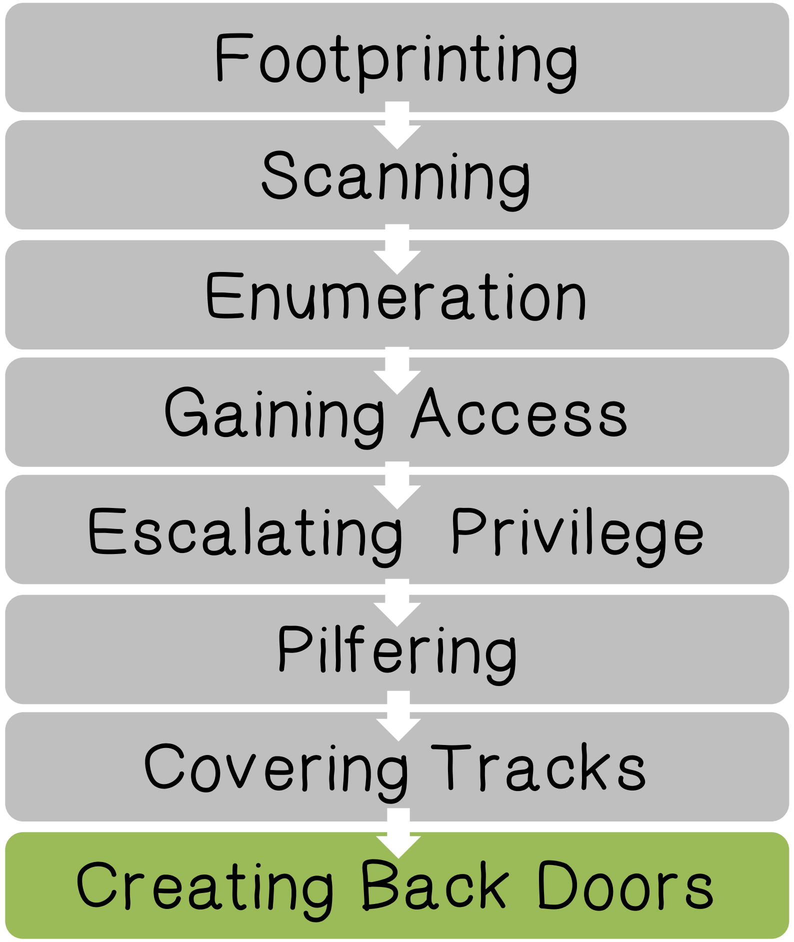
- Once total ownership of the target is secured, hiding this fact from system administrators become paramount, lest they quickly end the romp

Covering Tracks

Covering Tracks

Techniques	Clear Logs	Hide tools
Tools	Zap, Event Log GUI	Rootkits file streaming

Creating Back Doors



Footprinting

Scanning

Enumeration

Gaining Access

Escalating Privilege

Pilfering

Covering Tracks

Creating Back Doors

- Trap doors will be laid in various parts of the system to ensure that privilege access is easily regained whenever the intruder decides

Creating Back Doors

Creating Back Doors

Techniques	Create rogue user accounts	Schedule batch jobs	Infect startup files
Tools	Members of wheel, admin	cron, at	rc, startup folder, registry keys
Techniques	Plant remote control services	Install monitoring mechanisms	Replace apps with Trojans
Tools	Netcat, remote.exe VNC, B02K remote desktop	Keystroke loggers, add acct. to secadmin mail aliases	Login, fpnwcint.dll

Penetration Testing Quiz

Which events should trigger a penetration test?

- ☑ Infrastructure is added or modified
- ☑ Applications are added or modified
- ☑ End user policies are changed
- ☑ Security patches are installed

Persistence and Stealth

- Installation of backdoor or malware
  - A permanent foothold

- Insertion of proxies or man-in-the-middle systems, or simply "listening/recording"

- Capture credentials and identify valuable target
  - Impersonation and Data thefts

- Iterate Persistence and Stealth - I.e., move from one host/account to next; hide tracks

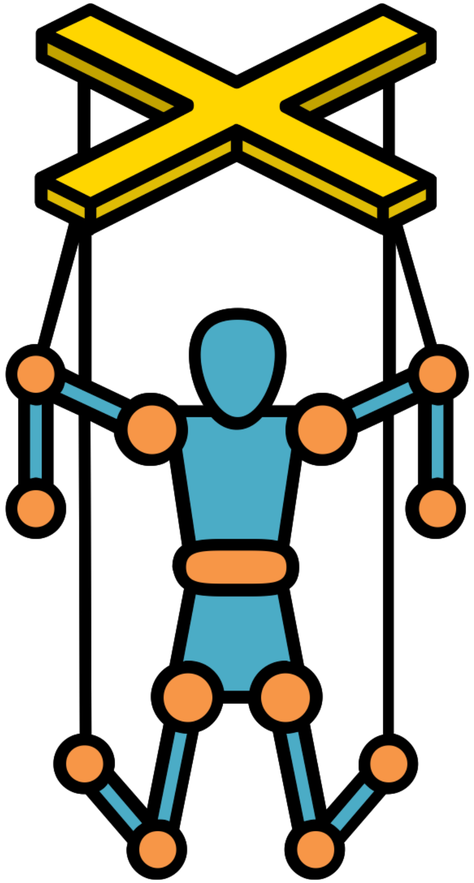
Social Engineering

Users are the Weakest Link

Use "social engineering" attack techniques to evaluate user population

- Identify vulnerable user groups
- Identify policy gaps
- Fix policies and mechanisms, including user education and training

Social Engineering



Why is Social Engineering Effective?

- Manipulates legitimate users into undermining their own security system
- Abuses trusted relationships between employees
- Very cheap for the attacker
- Attacker does not need specialized equipment or skills

RSA Breach Quiz

List the steps attackers used to access RSA’s Adobe Flash software:

Identify employees that are vulnerable

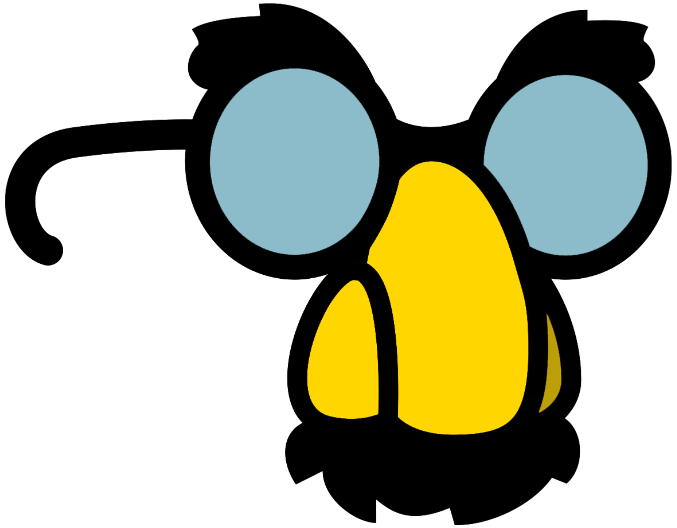
Craft an email subject line that entices an employee to open it

Hide an executable file in the email that will install onto the victim's computer when the email is opened

2011 RSA was compromised

- Social engineering was used to penetrate the company’s defenses
- Once in, the attackers installed a backdoor using an Adobe Flash vulnerability

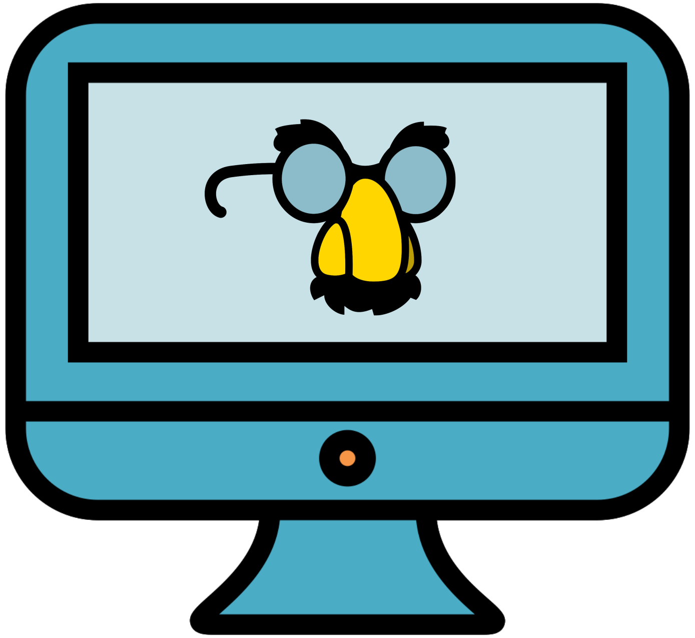
Common Social Engineering Techniques



Impersonation

- Help Desk
- Third-party Authorization
- Tech Support
- Roaming the Halls or Tailgating
- Trusted Authority/Repairman Figure
- Snail Mail

Common Social Engineering Techniques



Computer-Based Techniques

- Pop-up windows
- Instant Messaging and IRC
- Email Attachments
- Email Scams
- Chain Letters and Hoaxes
- Websites

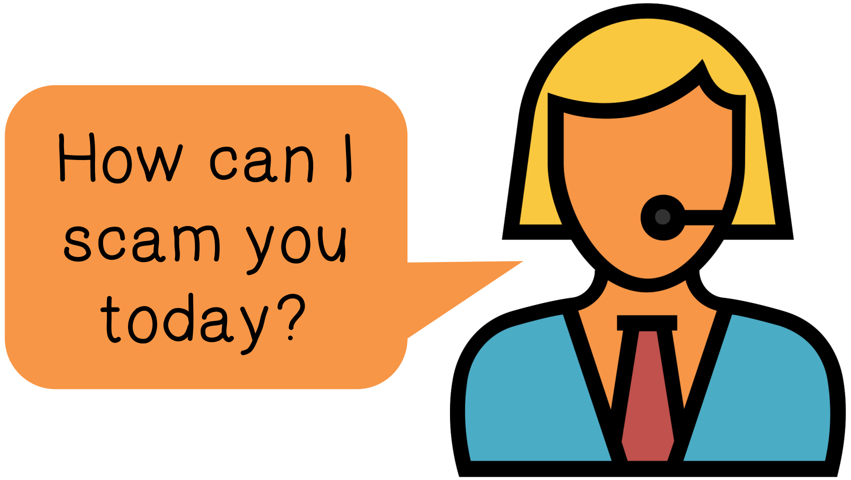
Impersonation: Help Desk

The attack:

- Attacker pretends to be an employee
- Recovers “forgotten” password

The exploit:

- Help desks often do not require adequate authentication



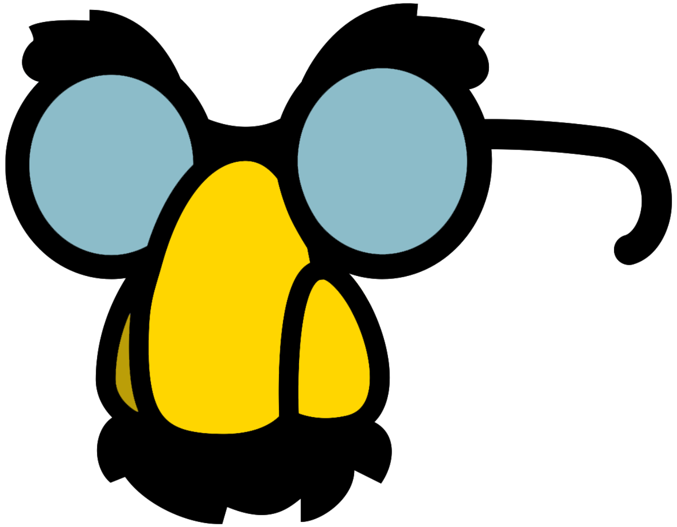
Impersonation: Third-Party Authorization

The attack:

- Access to assets
- Verification codes

The exploit:

- Claim that a third party has authorized the target to divulge sensitive information
- More effective if the third party is out of town



Impersonation: Tech Support

The attack:

- Attacker pretends to be tech support for the company and obtains user credentials for troubleshooting purposes

The exploit:

- Users must be trained to guard credentials

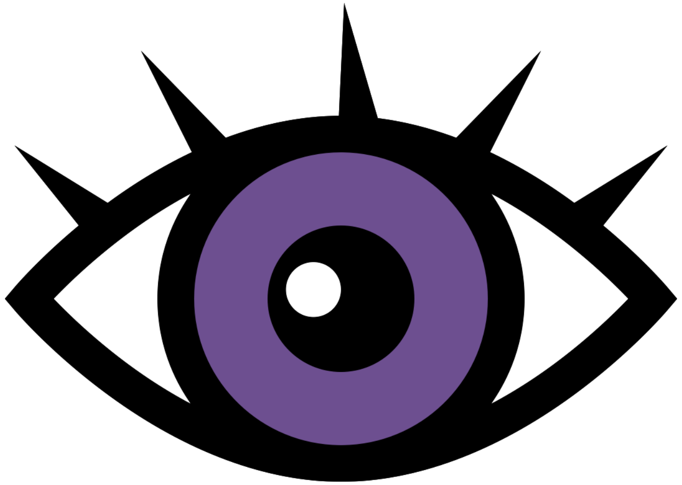
Impersonation: Roaming the Halls

The attack:

- Attacker dresses to blend in with the environment

The exploit:

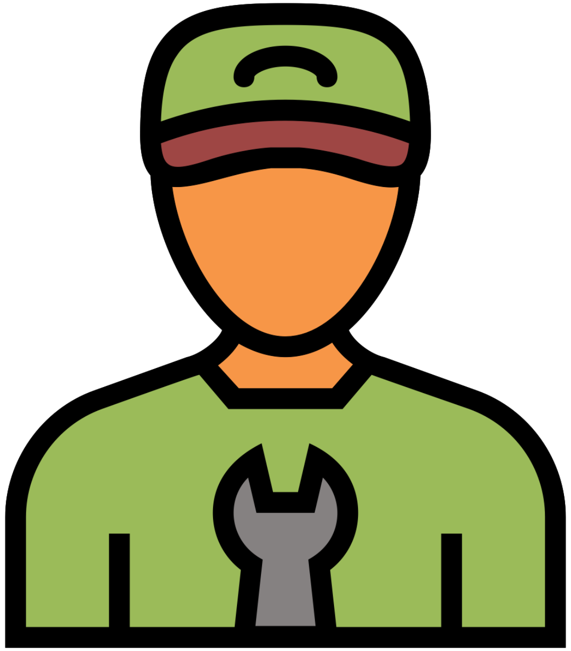
- Looks for sensitive information that has been left unattended
  - Passwords written down
  - Important papers
  - Confidential conversations



Impersonation: Repairman

The attack:

- Attacker wears the appropriate uniform
- Often allowed into sensitive environments
- May plant surveillance equipment
- Could find sensitive information



The exploit:

- People rarely question someone in a uniform

Impersonation: Trusted Authority Figure

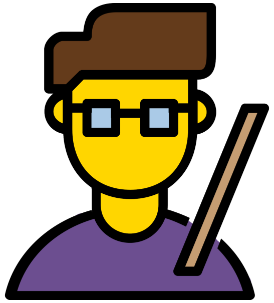
The attack:

- Attacker pretends to be someone in charge of a company or department
- Similar to “third-party authorization” attack
- Impersonation in person or via telephone

Examples of authority figures

Medical Personnel

Home Inspector



School Superintendent

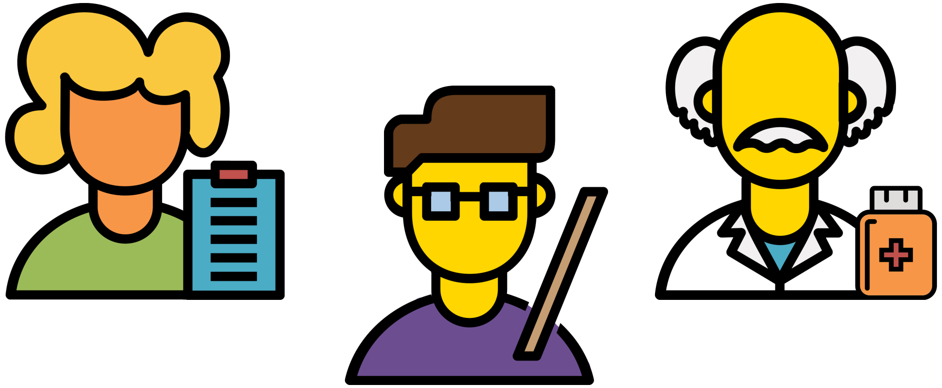
Impersonation: Trusted Authority Figure

The attack:

- Attacker pretends to be someone in charge of a company or department
- Similar to “third-party authorization” attack
- Impersonation in person or via telephone

The exploit:

- Trust in perceived authority



Impersonation: Snail Mail

The attack:

- Attacker sends mail that asks for personal information

The exploit:

- People are more trusting of printed words than webpages

Examples

- Fake sweepstakes
- Free offers
- Rewards programs
- More effective on older generations

Impersonation Quiz

Match each social engineering training tool with its description:

Attacks:

3 Flash or CD Autoplay

2 Reverse Shell Applet

1 Click Logger

4 Download Connection

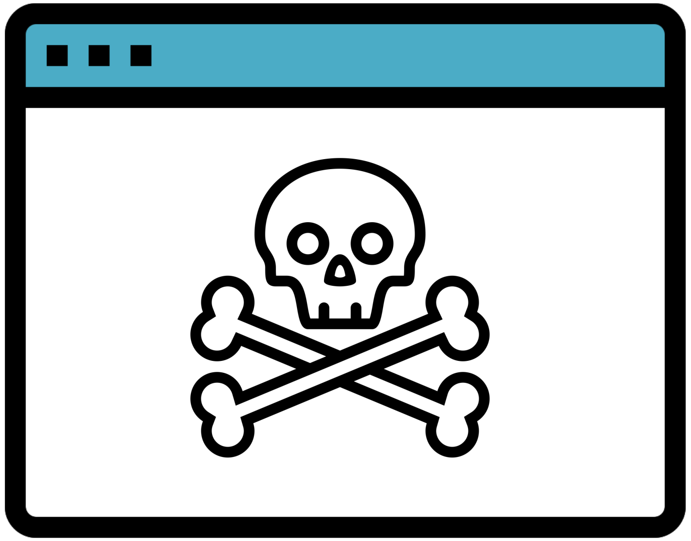
Descriptions:

1. Used to determine which users click on links in emails
2. A signed Java applet is sent to the user, if they accept it, a shell is sent back to the exploit server.
3. A flash is created that has a program that creates a connection to the exploit server
4. An email contains an attachment. When the attachment is downloaded an connection is made to the exploit server.

Computer Attacks: Popup Windows

The attack:

- Window prompts user for login credentials
- Imitates the secure network login



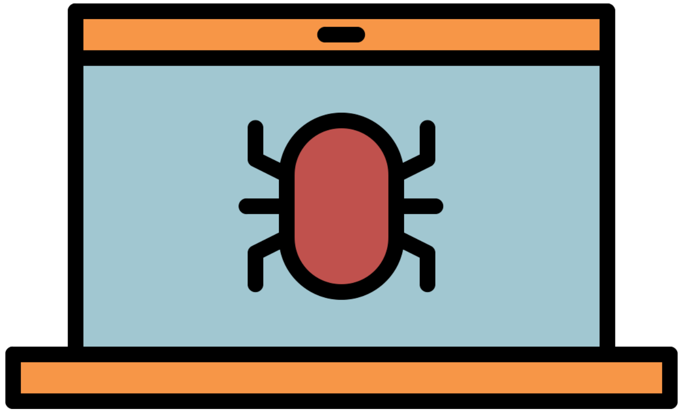
The defense:

- Users can check for visual indicators to verify security

Computer Attacks: IM & IRC

The attack:

- Attacker uses IM, IRC to imitate technical support desk
- Redirects users to malicious sites
- Trojan horse downloads install surveillance programs



Computer Attacks: Email Attachments

Attacker tricks user into downloading malicious software

Programs can be hidden in downloads that appear legitimate

Examples:

- Executable macros embedded in PDF files
- Camouflaged extension: “NormalFile.doc” vs. “NormalFile.doc.exe”

Computer Attacks: Email Scams

- More prevalent over time
- Begins by requesting basic information
- Leads to financial scams

Computer Attacks: Chain Emails

More of a nuisance than a threat

Spread using social engineering techniques

Productivity and resource cost

Computer Attacks: Websites

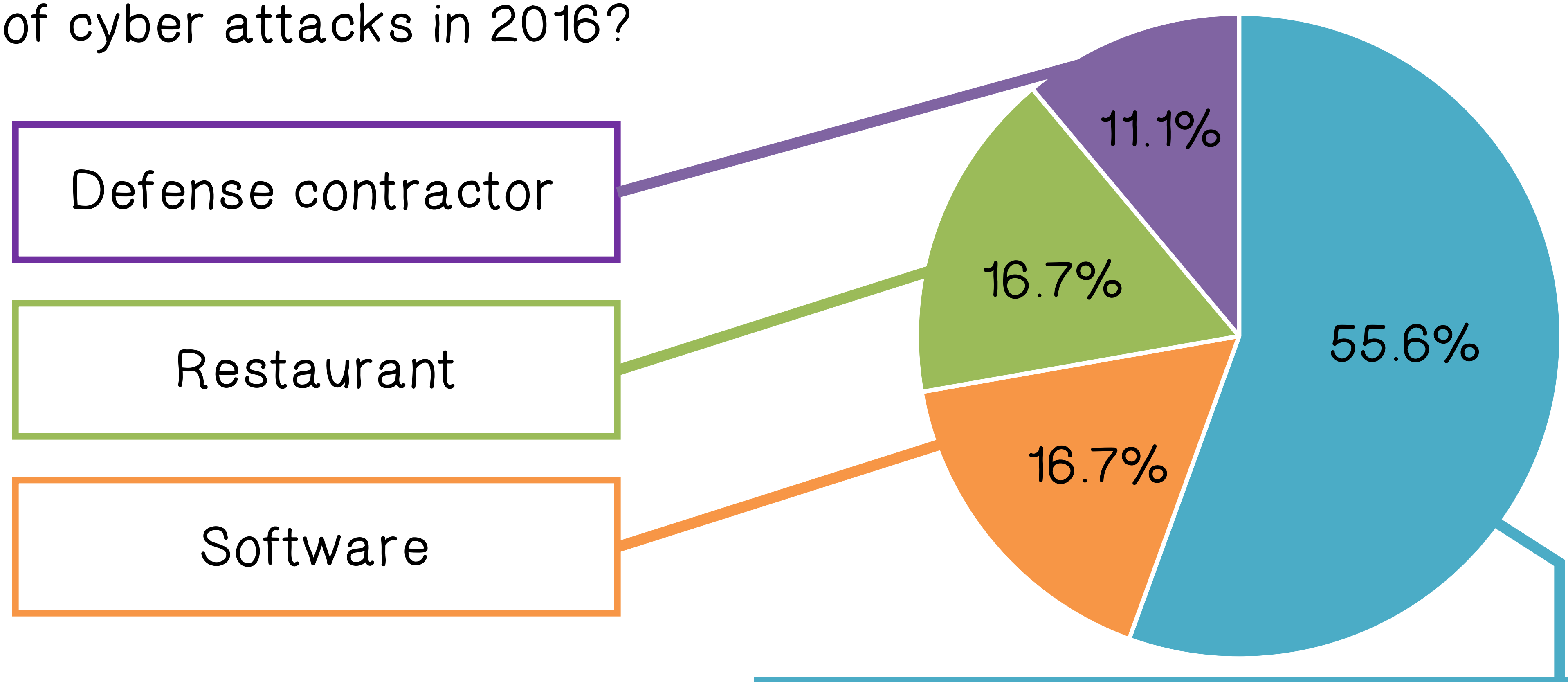
Offer prizes but require a created login

Attacker capitalizes on users reusing login credentials

Website credentials can then be used for illegitimate access to assets

Computer Attacks Quiz

On this pie chart, what are the top three industries that were targets of cyber attacks in 2016?



Defense contractor

Restaurant

Software

The 55.6% portion is for all other industries combined.

Countering Social Engineering Attacks

- Never disclose passwords
- Limit IT Information disclosed
- Limit information in auto-reply emails
- Escort guests in sensitive areas
- Question people you don't know
- Talk to employees about security
- Centralize reporting of suspicious behavior

This protects against attacks

- “Repairman”
- “Trusted Authority Figure”

Motivator Quiz

Match the motivation with its description:

2	Liking
1	Scarcity
3	Commitment
4	Social Proof

1. A desire to pursue a limited or exclusive item or service
2. A desire to fit in and to be more easily influenced by someone you like
3. A desire to act in a consistent manner
4. Looking to others for clues on how to behave