****

**Course: CYB302**

 **Ethical Hacking
(Canadian Context)**

 **Lab 12: Social Engineering in Action, &
Cybersecurity Career Pathways**

**Coordinator and Instructor:**

 **Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

Activity 1: Sneakers (1992)

00:00:00 to 00:10:50 – Background and Pen Test

This is the setting of a scenario in which Martin and his team are carrying out a penetration test in a bank.

Social Engineering Techniques:

1. The team of Martin employs disguise of legitimacy and authority to make themselves look real and get the job done successfully.

2. Phishing by Phone (Vishing) – The ruse was carried out by the perpetrators who were imitating bank managers or IT support personnel on the phone, who asked not only passwords and other sensitive data but also provided the account and bypassed the authentication.

3.tTechnician Impersonation – The attackers obtain physical access to a building by dressing and acting as a technician or security guard.

4.tTailgating – A person can secretly follow another person walking in front of him/her to enter the secured building without the required card, etc. One hopes that the other person will be nice and let them enter the building.

5.tDumpster Diving (implied) – Someone has obviously collected data from different locations, which might have included trash cans.

00:25:30 to 00:32:50 – Ransomware

This is the tactic where the gang uses sneak attacks to gain access to a lab and steal the equipment at the same time. Stealth is their best ally.

Social Engineering Methods:

1. Pretexting / Impersonation – The subjects of these attacks have always been those who showed up without any invitation or credential but pretended they were on a hurried, important visit.

2. Baiting – Carl used women power of flirtation to distract the target while her cohorts exploit the vulnerable space.

3.Abuse of Power – These criminals are able to carry on their illegal activities because they either have managed to produce fabricated documents that look like the original ones or have courageously talked and moved as if they were staff. And it is very easy to abuse the power of a certain position without the knowledge of the rest of the staff.

4. Emotional Manipulation / Diversion – Whistler typically creates a diversion that might be in the form of simply a slight disorder or chaos till one of his fellow members enters the target zone without being seen.

5. Piggybacking – This refers to a practice where people use doors that are already opened to the environment or just simply use someone else to gain unauthorized access to the restricted areas.

00:40:00 – 00:43:50 – Crypto Cracking Box

In this part, the crew is fond of the performance of the dark side box.

This is not social engineering per se, but the part is an analogy that highlights how and why social engineering is so dangerous:

• The thing that becomes a major point of concern is the black box cracking practically any encryption, and it shows that unauthorized entry (achieved through social engineering) can lead to the worst-case scenario.

• It is a shocking realization that more often than not, social engineering serves as the entrance for technical intrusions.

Activity 2: Hackers 2: Operation Takedown (2000)

00:04:10 – 00:10:20 – Learning the SAS system

Social Engineering Techniques:

1. Pretexting – Kevin Mitnick talks with a staff member who is a rightful one like him, and he does so in order to acquire technical data. He creates fake identities so that other people are deceived and provide him with the information.

2. Authority Exploitation – He adopts a confident yet harmful stance through his speech and by using slang in order to sound more convincing, while also giving veiled physical[?] threats to force people to give up their data.

3. Phone Phishing (Vishing) – He pretends to be someone he is not, e.g., he gives a call to employees and tries to convince them that he is from the IT department or their vendor. Then he persuades or misleads them to extend technical help to him by disclosing certain system details.

4. Name-Dropping – Knowing that he can get more cooperation from people by mentioning the real employee of the organization, he gives imaginary names to those he masks as his victim, using his alias name as a verification that it is valid.

5. Gathering Information – This is the phase where Kevin depicts how important passive information retrieval is – getting information prior to the actual attack.

Social Engineering Techniques:

1. Blending In / Insider Threat Tactic – Kevin realizes that he can gain remote access to a system and then use the knowledge of internal behavior and systems to be perceived as a regular user.

2. Phone-Based Deception – The person calls the only desk or the system administrators who pretend to be a co-worker to reset the password or to have access to the level.

3. Trust Exploitation – He counts on the human mind to be helpful - this is especially true for education.

4. Baiting – He is also willing to insert a new threat somewhere (or find someone to do it) without suspecting that it’s a malicious act.

5. Exploiting Weak Security Policies – See how he upgrades his access level through various weak authentication methods and denial of multi-factor authentication despite being the weakest link or lack of multi-factor authentication.

Activity 3A: The Beekeeper (2024)

Type of Fraud / Attack Phishing Scam (Social Engineering): The movie, which is titled Teacher, tells the story of Eloise Walker, a retired teacher, who is a victim of a highly skillful phishing crime. The scammers push her to transfer more than $2 million from a charity fund she was managing, thus causing her to commit suicide.​ncyberTAP.

What Happens at the End of the Movie?

Technologies / Devices Used The bad actors apply different technologies and use various methods to carry out the phishing attack: Email Spoofing: They make use of fabricated emails that look as if they are sent from actual sources, Eloise is easily convinced by the source of the email#t0267==.​Fake Websites: The emails forwarded her to links of the fake websites that were similar in appearance to the real websites. On those pages, she unwittingly leaked sensitive information.​Call Centers: The calling center is a big network giving more power to the swindle and they also pose as fake customer service, thus making the scam look more real.

Activity 3: How easy is it to get someone’s password?
Processes for Evading Social Engineering and Phishing Attacks

Implement Multi-Factor Authentication (MFA):

Make it a necessary rule to use at least two different methods of confirmation to enter into the system so that the exposure to passwords is less.​

Regularly Done Security Awareness Training: Teach the staff how to spot phishing attacks, dubious links, and tricks used by hackers.​Carry out simulations to gauge and strengthen understanding.​

Clearly Defined Verification Processes: Implement protocols for confirming the legitimacy of the request for sensitive details, with an extra emphasis on those coming in through email or phone.

Make it a mandate for employees to confirm the requests via the official channels.

Access to Sensitive Data is Restricted: Only give permissions to the employees that are relevant to their job roles by following the principle of least privilege.​

Regularly Update and Patch Systems: On a regular basis, update all the software and systems so that they are well protected against possible attacks by those who take advantage of known vulnerabilities.​

 Activity 4: Investigating Keyloggers

**Types of Keyloggers**

1. Software Keyloggers

These are programs that secretly run in the background of an operating system and capture keystrokes.

* Types:
	+ Kernel-based: Installed at the OS kernel level, extremely difficult to detect.
	+ API-based: Hooks into keyboard APIs to record keystrokes.
	+ Form Grabbers: Record data submitted in web forms, bypassing encryption.

2.Hardware Keyloggers

These are physical devices connected to a computer that log keyboard input.

* Types:
	+ Inline Keyloggers: Plugged between the peripherals such as keyboard and the computer (typically via USB).
	+ Wi-Fi/Bluetooth Keyloggers: Broadcast data wirelessly to an attacker (fake keyboards overlaid to mimic the real one).

**How to Prevent Keyloggers in an Organization**

Technical Controls

* Use Endpoint Detection and Response (EDR): Detects suspicious behavior like logging or API hooking.
* Keep Anti-Malware/Anti-Keylogger Software Updated: Some Anti-Malwares has solutions specialize in keylogger detection.
* Restrict Admin Privileges: Prevents unauthorized software installations and limits malware persistence.

Policy

* Restrict USB Access: Never allow undocumented or unofficial USB devices, also disable ports not used or make use of endpoint protection tools to control physical devices.
* Educate Employees: Organize awareness training to detect suspicious hardware or behavior to all employees and stakeholders.
* Network Monitoring: Always be on the Lookout for strange outbound traffic (e.g., a keylogger remotely sending logs).

|  |  |  |  |
| --- | --- | --- | --- |
| **Keylogger Type** | **Acquisition Level** | **Detection Difficulty** | **Prevention Focus** |
| Software (API-based) | Easy (common) | Moderate | EDR, Anti-virus, least privilege |
| Software (Kernel) | Medium | High | EDR, behavioral detection |
| Hardware (Inline USB) | Easy (Amazon, etc.) | Low to moderate | Physical security, inspections |
| Wireless Keyloggers | Medium | High | RF monitoring, USB restrictions |
| Form Grabbers | Common in malware | High | Browser protection, HTTPS, MFA |

Activity 5: Decide your Career Path in Cybersecurity

**Cybersecurity Specialist**

* **Level:** Entry-Level
* **Feeder Roles:** Networking, IT Support, Systems Engineering, etc.
* **Transitions To:**
	+ Cybersecurity Analyst (Mid-Level)
	+ Cybersecurity Consultant (Mid-Level)
	+ Penetration & Vulnerability Tester (Mid-Level)
* **Essential Skills:**
	+ Network security
	+ Risk assessment
	+ Firewalls and intrusion detection/prevention systems (IDS/IPS)
	+ Basic scripting (Python, Bash)
	+ Operating systems (Windows/Linux)
* **Professional Skills:**
	+ Attention to detail
	+ Problem-solving
	+ Analytical thinking
	+ Collaboration
	+ Written and verbal communication