

2.3.6 Social Engineering Techniques Facts

Not all attackers are the same. They all have different motives, attributes, and attack characteristics. Attackers also can employ various techniques to obtain what they want from the target.

This lesson covers the following topics:

- Attack types
- Elicitation
- Pretexting, preloading, and impersonation
- Interview and interrogation

Attack Types

A single hacker trying to exploit a vulnerability will have different attack profile than an organized crime group waging an assault on a network. The following table describes the typical attack type used by each.

| Attack | Description |
|---------------|--|
| Opportunistic | An opportunistic attack is typically automated and involves scanning a wide range of systems for known vulnerabilities. Known vulnerabilities can include old software, exposed ports, poorly secured networks, and default configurations. When a vulnerability is found, the hacker will exploit the vulnerability, steal whatever is easy to obtain, and get out. This type of attack is typically used by a single hacker. |
| Targeted | A targeted attack is much more dangerous. A targeted attack is extremely methodical and is often carried out by multiple entities that have substantial resources. Targeted attacks almost always use unknown exploits, and the attackers go to great lengths to cover their tracks and hide their presence. Targeted attacks often use completely new programs that are specifically designed for the target. This attack type is typically used by an organized crime group. |

Elicitation

Elicitation is a technique used to extract information from a target without arousing suspicion. The following table describes some elicitation tactics.

| Tactic | Description |
|--------------------|---|
| Compliments | An attacker may give a target a compliment about something the target did. The attacker waits for the target to take the bait and elaborate on the subject. Even if the target downplays the skill or ability involved, talking about it might give the attacker valuable information. |
| Misinformation | Using the misinformation tactic, the attacker makes a statement with the wrong details. The attacker's intent is for the target to provide the accurate details that the attacker wants to confirm. The more precise the details given by the attacker, the better the chance that the target will take the bait. |
| Feigning ignorance | Attackers might make a wrong statement and then admit to not knowing much about the subject. The intent is to get the target to not only correct the attacker, but also explain in |

| | |
|-----------------------|---|
| | detail why the attacker is wrong. The explanation might help the attacker learn, or at least have a chance to ask questions without looking suspicious. |
| Being a good listener | An attacker may approach a target and carefully listen to what the target has to say, validate any feelings the target expresses, and share similar experiences, which may be real or fabricated. The point is to be relatable and sympathetic. As the target feels more connected to the attacker, barriers go down and trust builds. This leads the target to share more information. |

Pretexting, Preloading, and Impersonation

All social engineering techniques involve some pretexting, preloading, and impersonation. The following table describes these steps.

| Step | Description |
|---------------|--|
| Pretexting | Pretexting is conducting research and information gathering to create convincing identities, stories, and scenarios to be used on selected targets. |
| Preloading | Preloading is used to set up a target by influencing the target's thoughts, opinions, and emotions. |
| Impersonation | Impersonation is pretending to be trustworthy and having a legitimate reason for approaching the target to ask for sensitive information or access to protected systems. |

Interview and Interrogation

Another technique social engineers use often is interviews and interrogation. The following table describes some of the most important concepts of conducting a successful interview and interrogation.

| Concept | Description |
|----------------------------|--|
| Interview vs interrogation | In the interview phase, the attacker lets the target do the talking while the attacker mostly listens. In this way, the attacker has the chance to learn more about the target and how to best extract information. Then the attacker leads the interview phase into an interrogation phase. It's most effective when done smoothly and naturally, and when the target feels a connection and trusts the attacker. In the interrogation phase, the attacker talks about the target's statements. The attacker is mostly leading the conversation with questions and statements that will flow in the direction the attacker needs to obtain information. |
| Environment | <p>The environment the attacker chooses for conducting an interview and interrogation is essential to setting the mood.</p> <ul style="list-style-type: none"> ▪ The location should not be overly noisy or overly crowded. ▪ The environment should be a relaxing and stress-free setting that puts the target at ease. ▪ The attacker shouldn't sit between the target and the door. The target should never feel trapped in any way. ▪ Lighting should be good enough for both parties to see each other clearly. This will allow the attacker to better read the target's micro expressions and movements. It will also inspire trust in the target. |
| Observation | |

During these interviews and interrogations, the hacker pays attention to every change the target displays. This allows the attacker to discern the target's thoughts and topics that should be investigated further. Every part of the human body can give a clue about what is going on inside the mind. Most people don't realize they give many physical cues, nor do they recognize these cues in others. A skilled observer pays close attention and puts these clues together to confirm another person's thoughts and feelings.

Copyright © 2022 TestOut Corporation All rights reserved.