Techniques

Phishing

A type of social engineering in which an attacker attempts to obtain sensitive information from users by masquerading as a trusted entity in an e-mail or instant message sent to a large group of often random users.

Types

Smishing

Smishing is an attack using Short Message Service (SMS) on victims' cell phones. It is a version of phishing via SMS.

Vishing

Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking. Vishing takes advantage of the trust that some people place in the telephone network.

Spear Phishing

Spear phishing is a term created to refer to a phishing attack that targets a specific person or group of people with something in common.

Higher probability of success because a targeted attack will seem more plausible than a message sent to users randomly.

Spam

It is bulk unsolicited e-mail.

the purpose of spam is to get an unsuspecting user to click malicious content or links, thus initiating the attack.

Spam over Instant Messaging (SPIM)

Basically spam delivered via an instant messaging application.

Pretexting

A form of social engineering in which the attacker uses a narrative (the pretext) to influence the victim into giving up some item of information

An example would be calling up, posing as a fellow student from college, or a fellow admin to a senior executive.

Dumpster Diving

The process of going through a target's trash in hopes of finding valuable information.

An organization should have policies about discarding materials.

Sensitive information should be shredded and the organization should consider securing the trash receptacle so that individuals can't forage through it.

Whaling

High-value targets are referred to as whales.

A whaling attack is thus one where the target is a high-value person, such as a CEO or CFO.

Shoulder Surfing

The attacker directly observes the individual entering sensitive information on a form, keypad, or keyboard.

The attacker may simply look over the shoulder of the user at work, for example, or may set up a camera or use binoculars to view the user entering sensitive data.

Pharming

Misdirecting users to fake websites made to look official.

Once at the fake site, the user might supply personal information, believing that they are connected to the legitimate site.

Tailgating (Piggybacking)

The simple tactic of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.

An attacker can thus gain access to the facility without having to know the access code or having to acquire an access card.

Influence Campaigns

Influence campaigns involve the use of collected information and selective publication of material to key individuals in an attempt to alter perceptions and change people's minds on a topic.

One can engage in an influence campaign against a single person, but the effect is limited.

Influence campaigns are even more powerful when used in conjunction with social media to spread influence through influencer propagation.

Watering Hole Attack

It involves the infecting of a target website with malware.

These are not simple attacks, yet they can be very effective at delivering malware to specific groups of end users.

Typosquatting

An attack form that involves capitalizing upon common typographical errors.

If an attacker has registered the mistyped URL, then the user would land on the attacker's page.

There are several reasons that an attacker will pursue this avenue of attack. The most obvious is one of a phishing attack.

The fake site collects credentials, passing them on to the real site, and then steps out of the conversation to avoid detection once the credentials are obtained.

Credential Harvesting

Credential harvesting involves the collection of credential information, such as user IDs, passwords, and so on, enabling an attacker a series of access passes to the system.

The objective of a credential harvest is just to obtain credentials.

Invoice Scamming

Invoice scams use a fake invoice in an attempt to get a company to pay for things it has not ordered.

Identity Fraud

The use of fake credentials to achieve an end.

Physically as in pretending to be a delivery agent, show up with a box— or better yet, a server—and attempt direct delivery to the server room.

Can be done physically or online

Works best when the victim is expecting the person

Defense against identity fraud is the same as most other social engineering attacks: use strong policies and procedures without exceptions.

Prepending

Prepending is the act of supplying information that another will act upon, frequently before they ask for it, in an attempt to legitimize the actual request, which comes later.

Example: stating that they were sent by the target's boss, or another authority figure, as a means to justify why the target should perform a specific action

Eliciting Information

Calls to or from help desk and tech support units can be used to elicit information.

Posing as an employee, an attacker can get a password reset, information about some system, or other useful information.

The call can go the other direction as well, where the social engineer is posing as the help desk or tech support person. Then, by calling employees, the attacker can get information on system status and other interesting elements that they can use later.

Exam Tips

Phishing, smishing, vishing—these are attacks against users' cognitive state. Using the principles for effectiveness, one can craft a message that makes falling victim to these attacks more likely.

The attack is a combination of technical elements and psychological pressure, and together they cause the user to take the bait and click the link.

Phishing is now the most common form of social engineering attack related to computer security. The target could be a computer system and access to the information found on it (as is the case when the phishing attempt asks for a user ID and password), or it could be personal information, generally financial, about an individual (in the case of phishing attempts that ask for an individual's banking information).