LESSON GUIDE

INTRO TO CYBERSECURITY

Human Factor

2.1.1 - Social Engineering

Lesson Overview:

Students will:

- Define the steps used in typical digital attacks.
- Define social engineering as the human risk in organization security.
- Identify techniques for social engineering and how to mitigate against these techniques.

Guiding Question: How can we protect against Social Engineering?

Suggested Grade Levels: 8 - 12

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

GALANTECH with GARDEN STATE CYBER
CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Social Engineering

Materials

- Cut up sections of 7 steps of hacking - need 1 set of slips for each group of 3 students

Slide 1 - Intro Slide

Slide 2 - Activity - Seven Steps of Hacking

Slide 3 - Social Engineering - goals and methods

The Social Engineering unit addresses the "Human Factor" in cybersecurity. It is a sobering fact that most data breaches involved some measure of human factor, either mistakes or malicious actions. In this unit we examine how simple human characterstics make us vulnerable to social engineering techniques.

Click for animations.
"Threats against the human factor"...what does this mean??? It almost sounds like someone is threatening the humans in my organization. Are they going to attack a person? Will there be knives or punches or blood?

No - by "threat" we mean that social engineering will manipulate the humans in an organization to take action that ends up hurting the organization.

So, the goal is to get someone into giving us info we are NOT supposed to have...Or letting us into an area that we are NOT supposed to be in. How do we get them to do this? By using a CON or SCAM - i.e., tricking them into believing that it is all okay!

Slide 4 - Social Engineering - reasons for success

Click for animations.
We just completed an exercise to identify and order the 7 steps of hacking. Social engineering falls into two of those steps:
#1 Recon - because in order to con your target, you need to know and understand them which means you will gather info about them.

#3 Gaining Access - because many of the Social Engineering techniques will succeed in getting physical or digital access.

The sad news is that Social Engineering is highly successful. This means that malicious actors don't have to be great at coding or technology because they can get access by just preying on human errors. So, in the 3rd bullet point, translate "sloppy" to "stupid" - most users know they are not using best practices but they just are careless/unthing/impatient. In cybersecurity and IT this is known as being a "stupid user" and it is very frustrating to deal with !

Examples on next 2 slides.

Slide 5 - Social Engineering - real-life example

In 2015, TV5Monde was hit with a DOS (Denial of Service) attack by ISIS. It took them off the air for hours and also took over their social media accounts. This TV5Monde reporter was filmed in an interview about the attack BUT he is standing in front of a colleague's desk that has usernames and passwords visibly posted - and they are for Twitter, Instagram and YouTube.

This is really a DOUBLE sloppy mistake!

Full article: http://arstechnica.com/security/2015/04/hacked-french-network-exposed-its-own-passwords-during-tv-interview/

Slide 6 - Demo of a Vishing attack

The video is a great example of taking advantage of the human desire to be helpful. "Vishing" is when you use a phone to perform a social engineering attack.

Video is 2:29. Also at YouTube: https://www.youtube.com/watch?v=lc7scxvKQOo

Slide 7 - Techniques of Social Engineering

Here is a list of Social Engineering techniques. Go through each definition (see below) and ask students to categorize which of the 3 listed human qualities (blue box) is being taken advantage of in the technique.

- Baiting - offering something of value such as a prize if you click or leaving a USB drive to be found. (#3 Sloppy mistake - falling for a scam through greed)
- Shoulder surfing - look over their shoulder at ATM, charge cards, entry access code pads (#3 Mistake, be aware of surroundings)
- Piggybacking (aka tailgating) to get into a restricted space - this is where someone goes through a door after you have swiped in OR you hold the door open for them without making them authenticate. (#1 helpful to hold door open OR #3 Mistake - not noticing someone)
- Info written in workspace like on the wall, on monitor, or even in a desk drawer. (#3 Sloppy
- Dumpster diving to retrieve discarded paper information - can use phone lists for usernames or might get financial information that has been thrown away. (#3 Sloppy Mistake, should always shred!)
- Pretexting - impersonation with rushing or "emergency" - Mat Honan hack is an example where Apple bypassed the Security Questions or the video seen in this PPT where the woman has a crying baby (#1 Trying to be helpful). Pretextion - Wearing a "uniform" or using authority - an IT Tech support type of uniform that will get access to a computer. But could also be a janitor uniform or a security guard - in a school it could be a sports uniform! Or impersonating an authority to bully you into helping. (#2 Avoid confrontation by not asking for identification OR #3 Mistake, assuming people are what they look like or who they say they are).

- Scareware - making people believe that malware has been installed and that they need to give you access or install software to “fix it”. (#3 Sloppy mistake in not using a scanner to check if there is malware before taking any action).

Slide 8 - Protect against Social Engineering

Introduce these techniques before moving to the Activity slide where students will be assigned a Social Engineering technique and create a PSA video. Items #5 - 8 all can be protected against through educating users to be alert to these social engineering techniques. In addition, organizations can create policies that impose safe behaviors. Some examples policies:

- No door entry without swiping your employee card
- No using USBs on any company computer
- Require any uniformed person show identification before being given access

Slide 9 - Activity - Social Engineering Toolkit

- In the Cyber Range, students will use SET to create fake Google or Twitter login pages. When someone enters their credentials into the fake site, the SET tool captures those credentials and displays them behind the scenes. See lab instructions.
- IMPORTANT: all actions in this lab happen in the Virtual Machine, there is no actual site created on the public internet. In addition, no instructions are provided on how to use this tool in the real world. Using the SET tool in this safe enviroment provides students with a sobering look at what tools are out there to trick unwary users.

Closure discussion: ask students to describe what they saw in the lab results. What kind of situations have you seen where this technique could be used? How could a user protect themselves against this type of attack? Note that there are not specific right answers at this time, the objective is to get the students’ reaction and have them being thinking about social engineering vulnerabilities.