15.2.1 User Security

Click one of the buttons to take you to that part of the video.

User Security 0:00-0:23

In this lesson, we're going to discuss several measures that you can take to increase user security. Let's begin by discussing the importance of using strong passwords.

A serious security weakness that I've observed over the years is the use of weak passwords. Now, a weak password is one that can be easily guessed or cracked.

Weak Passwords 0:24-1:10

Here are some examples of very weak passwords: your last name, your spouse's name, your mother's maiden name, your child's name, your birthdate, your pet's name, using the word password for your password-- yes, I have seen that-- using really short passwords like one, or even using blank passwords. You would be surprised how often users use these types of passwords, and this isn't good.

For example, a simple social media search off the internet could help an attacker find this information within about 15 minutes max. And that exposes all the information that your account has access to on the system. Instead, what we need to do is train your users to use strong passwords.

Strong Passwords 1:11-2:08

A strong password uses at least eight characters--more is better. The longer the password, the more secure it is. Because the harder it is to guess, then the harder it is for a cracking utility to crack it. It also contains a combination of both numbers and letters. It should contain both upper and lowercase letters, not just all lowercase or not all uppercase.

And, this is a hard one, it needs to not contain words found in the dictionary. And, if you really want to make your password strong, include a bunch of non-alphanumeric characters in the password such as punctuation marks.

So, take a look at this password right here. What do you think? Is that a strong password? Let's evaluate whether it meets the criteria. Is it longer than eight characters? Yep. Does it use a combination of numbers and letters? Yep.

Upper and lowercase letters? Yep. Does it contain words not found in the dictionary? I don't think you're going to find that word in the dictionary. This is a strong password.

Strong Password Check 2:09-2:56

Now, be aware that the password management utilities that come with most Linux distributions are configured by default to evaluate your user passwords when you set them to make sure they meet the criteria for a strong password.

Now it won't prevent you from using a bad password, it'll just yell at you a little bit. For example, here I'm changing the password for the lmorgan user with the passwd command, and I used a really, really bad password.

I don't remember exactly what I typed, but I think it was something like AAA or something like that. And it yelled at me saying, "Hey, that's a really bad password, don't use it." But, it let me do it anyway.

So even though these utilities will yell at you if you use a bad password, they'll still let you do it. So, you still have to train your users to use good passwords.

Password Aging 2:57-5:11

Now, in addition to using strong passwords, you should also configure your user accounts such that the passwords expire after a certain period of time. This is called password aging. Now, why would you want to age your passwords?

The idea here is that the longer a user has the same password, the more likely it is to be compromised. By forcing users to periodically rotate their password, you constantly keep intruders guessing. Even if they do manage to get a user's password at some point, it will be rendered useless eventually.

Now, it's not a perfect system, but it does make that password invalid after a certain amount of time. Now, some of the more security minded organizations may mandate a maximum password age of maybe 30 days. Less paranoid organizations might go 45 days. I've seen some go 60.

The longest I've ever seen is 90, and that's almost too long. That's three months with the same password. Most of your organizations today are going to be right here in this range-- 30 to 45 days. Now, you configure aging for your password using the chage command.

The syntax is shown here. We enter chage, followed by the option we want to set, followed by the name of the user account that we want to apply that setting to. Some of the more commonly used options are shown here. -m specifies the minimum number of days that are allowed between password changes, while -M specifies the maximum number of days between password changes.

Now, you might be thinking, I understand the maximum number of days between password changes, but why would you want to specify the minimum number of days between password changes? Well, we need to do this because sometimes end users will desperately want to keep using their same old comfortable password.

So, if we specify a maximum number of days before a user has to change their password, they'll go ahead and change it like they have to, and then they'll change it again really fast and change it back to their original password. By specifying a minimum number of days, we force that user to keep that same password for a long time before they're allowed to change it again.

You can also use the -W option to specify the number of warning days before a password change is required.

Password Protection 5:12-6:17

You should also train your users to use good common sense when they're working with passwords. Now, one security breach I see all the time is this one right here. End users write their password and their username a lot of times on a sticky note and they stick it somewhere on their desk.

I've even seen the sticky note being attached right to the monitor or right to the keyboard; and this sounds ridiculous, but I see it over and over and over. Now, some-- a little bit smarter users-- actually try to hide the sticky note under the keyboard. Or maybe they put it in a drawer or a cabinet, but it's still a significant security issue.

All the intruder has to do is watch the user log in and observe where they've hidden that sticky note with their password on it, and then they have everything they need to break into the system.

I was in an office just the other day and just for fun I lifted up the keyboard just to see. And guess what I found underneath that keyboard? You guessed it. A yellow sticky note with a username and a password on it. I just slap my head when I see that kind of thing.

Social Engineering 6:18-8:41

So with this in mind, we need to shift gears and talk about another security issue that you have to train your users how to deal with, and that is the issue of social engineering. This is actually one of the easiest and, also, one of the most effective tools in a hacker's toolbox today.

Social engineering bypasses technical attacks at a system and, instead, exploits human weaknesses. Here's how a typical social engineering exploit might work. An intruder calls an employee of an organization posing as another employee.

The employee says, "Hey, I'm Larry. I work in sales, and I'm on the road, and I'm at a client site. I have a very important file I've got to get off of the server, and I can't remember my password." And then Larry will demand that user Fred over here give him Fred's password so he can log in, just this once, to get at the file that he needs.

Now why does this exploit work? It's because most employees want to be team players and they want to help out in an emergency. Therefore, they're all too willing to hand out their password, granting the intruder access to the system.

Think about how easy this is compared to trying to crack a password and attack a system from outside the company. That takes a lot of work. And that takes a lot of time. And it takes a lot of computing horsepower. This social engineering exploit takes a few seconds and all it requires is a cell phone.

Now, some social engineering attempts are less direct. Instead of calling and asking for passwords, the intruder instead will sift through the company garbage, looking for those infamous little yellow sticky notes that have the user's passwords and usernames written on them because their boss told them to get rid of them and throw them away. So they threw them in the trash.

Well, the attacker pulls them right out of there. Now, some social engineering attacks are a little more in your face.

For example, the intruder might sift through the trash to find out the name of a very high-ranking person in the company and then he calls this employee again, poor Fred over here, and instead of posing as Larry from sales, he will instead pose as that high-ranking person and demand that Fred give him that password and if he doesn't, he's going to fire them.

Okay. That's pretty sneaky, right? Fred wants to keep his job, so he gives the attacker his password.

Phishing Emails 8:42-12:37

And the attacker then has access to the system. In addition to these exploits, you also need to be diligent against the flood of phishing emails that have been plaguing organizations for the last several years.

Now, phishing emails are very, very successful. In fact, they're responsible for many huge security breaches in the last several years.

Now a phishing email is drafted such that it appears to have come from a legitimate organization. In this example, it looks like we have an email coming from Amazon.com. The key here is that they try to convince the user to click a link right down here.

Now this link looks legitimate when you look at it, but in fact what it's going to do is take them to a malicious website that looks like Amazon.com, but is not Amazon.com and will try to trick them in to revealing sensitive information such as their Amazon username and password.

Now, phishing emails are really a low-tech hack, but they are extremely popular because they are very, very successful. All it takes is for one or two employees in an organization to be unwise enough to open this message and click on the link, and they're in.

So, to defend against this, you need to be able to identify the key characteristics of a phishing email. Now, just at first glance, this email looks legitimate, but there are several key attributes that will identify it as a scam. For example, it's common for the source address of the message to not match the domain of the company that claims to be coming from. Now, at first glance, you say well I'm looking right here.

It says that it's coming from Amazon.com. Well that text up there is very easy to fake, that's not a problem at all. You need to look at the message source and see where it actually was sent from and, more than likely, you'll find that it did not come from Amazon.com at all.

You'll find that it came from a rogue email server somewhere else in the world. In addition, the message will usually try to create a sense of urgency, and that's what this email does right here. It says, "Revision to your Amazon.com account." Right here it tells us that "We are contacting you to remind you that the review team identified that your account has been limited."

And it says right here that "Your online access will be blocked if this issue is not resolved immediately." Sense of urgency, right? And it tells us that if we don't do something about it, we're going to lose whatever privilege it is that's provided by that organization.

I've even seen some of these that claim that you will be arrested if you don't click on that link. The idea is to make the person panicky, so they will do whatever it is that you want to do.

Another key giveaway is the fact that if you hover your mouse over the link that they want you to click on, you'll see where that link actually leads and you'll probably find that the URL within the link itself does not match the text of the link that's actually displayed in the message.

So, if that link is not pointing to that organization's URL, pretty good chance that the message is an exploit. So how do you deal with these issues? Honestly, you can implement all the technology you want, but your best defense really is to train your users.

First of all, teach them not to write down their passwords. Also, teach them not to throw sensitive data in the trash. Shred it instead. You also need to educate them about social engineering phone calls and how to deal with them.

Now, most organizations will simply tell their employees to forward any calls they get like the ones we described to their help desk and, more than likely, all they're going to hear at the other end of the line is a click when they do that.

You should also teach your end users how to recognize the characteristics of a phishing email and how to respond properly, which is to junk it. Delete it. Don't click on the link.

Summary 12:38-12:46

That's it for this lesson. In this lesson, we talked about several key security issues regarding users. We talked about using strong passwords. We talked about password aging. And then we looked at social engineering.