ICSI MODULE 9:

User Policies Definition

9.1 User Policies Definition

Misuse of systems is a major problem for many organisations. A large part of the problem comes from the difficulty in defining what exactly misuse is. Some things might be obvious misuse, such as using company time and computers to search for another job or to view forbidden websites.

However, other areas are not so clear, such as an employee using her lunchtime to look up information about a car she is thinking of buying. Generally, good user policies outline specifically how people may use systems and how they may not. For a policy to be effective, it needs to be very clear and quite specific. Statements such as **"computers and Internet access are only for business use"** are simply inadequate.

Every organisation must have specific policies that will be applied fairly across the organisation. In the previous example, using a general statement of **"computers and Internet access are only for business use"** can be problematic. Assume you have an employee who occasionally takes just a few minutes to check home e-mail with the company computer. You decide that this is acceptable, and choose not to apply the policy. Later another employee spends two to three hours per day surfing the Net and you fire him for violating company policy. That employee might sue the company for wrongful termination.

Other areas for potential misuse are also covered by user policies, including password sharing, copying data, leaving accounts logged on while employees go to lunch, and so on. All of these issues ultimately have a significant impact on your network's security and must be clearly spelled out in your user policies. We will now examine several areas that effective user policies must cover:

- Passwords
- Internet use
- E-mail attachments
- Software installation and removal
- Instant messaging
- Desktop configuration
- BYOD

9.1.1 Passwords

Keeping passwords secure is critical. Appropriate passwords are part of operating system hardening. You should recall that a good password has in the past been defined as one that is six to eight characters long, uses numbers and special characters, and has no obvious relevance to the end user. For example, a user will use a password like "cowboys" or "godallas," but it should be advised to use a password like "%trEe987" or "123DoG$$" because those do not reflect the person's personal interests and therefore will not be easily guessed.

Issues such as minimum password length, password history, and password complexity come under administrative policies, not user policies. Those complexity requirements are still good recommendations. However, you should consider longer passwords, such as those 12 characters or longer. User policies dictate how the end user should behave.

However, no password is secure, no matter how long or how complex, if it is listed on a Post-it note stuck to the user's computer monitor. This may seem obvious, but it is not at all uncommon to go into an office and find a password either on the monitor or in the top drawer of the desk. Every janitor or anyone who simply passes by the office can get that password.

It is also common to find employees sharing passwords. For example, Bob is going to be out of town next week, so he gives Alice his password so that Alice can get into his system, check e-mail, and so on. The problem is that now two people have that password. And what happens if, during the week Bob is gone, Alice gets ill and decides she will share the password with Shelly so she can keep checking that system while Alice is out sick? It does not take long for a password to get to so many people that it is no longer useful at all from a security perspective.

Issues like minimum length of passwords, password age, password history are issues of administrative policies. System administrators can force these requirements. However, none of that will be particularly helpful if the users do not manage their passwords in a secure fashion.

All of this means you need explicit policies regarding how users secure their passwords. Those policies should specify:

- Passwords are never to be kept written down in any accessible place. The preference is that they not be written down at all, but if they are, they should be in a secure area such as a lock box.
- Passwords must never be shared with any person for any reason.
- If an employee believes his password has been compromised, he should immediately contact the IT department so that his password can be changed and so that logon attempts with the old password can be monitored and traced.

A recommendation is to choose a passphrase, something like ILikeCheeseBurgers, and then change the e's to 3's and use some capitalization. Perhaps add a symbol so it becomes #ILik3Ch33s3Burg3rs. This is a very secure password. It can be remembered and it has complexity and length.

The complexity requirements prevent dictionary attacks (using words from a dictionary) and guessing. However, you might be

wondering why a long password is so important. The reason has to do with how passwords are stored. In Windows when you select a password, that password is stored in hashed format in a SAM file. Remember that a hash cannot be undone. Therefore, when you log in, Windows will hash whatever you type in and compare it to what's in the SAM file. If they match, you are in.

Hashing passwords leads to the use of an interesting hacking technique called the rainbow table. A rainbow table contains all the possible hashes of all the key combinations that might have been used in a password, up to a given size. For example, all the single-character combinations are hashed, all the two-character combinations are hashed, and so on up to some finite limit (often 8 to 10 characters). If you get the SAM file then you can search the rainbow table for any matches. If you find a match, then the associated plaintext must be the password. Tools such as OphCrack boot into Linux and then run a rainbow table against the SAM file. However, larger rainbow tables are cumbersome. No current rainbow tables can handle passphrases of 20 characters or more.

9.1.2 Internet use Policy

Most organisations provide users with some sort of Internet access. There are several reasons for this. The most obvious reason is e-mail. However, that is hardly the only reason to have Internet access in a business. There is also the web, and even chat rooms. All of these can be used for legitimate purposes within any organisation but can also be serious security problems. Appropriate polices must be in place to govern the use of these technologies.

The web is a wonderful resource for a tremendous wealth of data. The Internet is also full with useful tutorials on various technologies. However, even nontechnology-related business interests can be served via the web. Here are a few examples of legitimate business uses of the web:

- Sales staff checking competitors websites to see what products or services they offer in what areas, perhaps even getting prices
- Creditors checking a business's AM Best or Standard and Poor's rating to see how their business financial rating is doing
- Business travellers checking weather conditions and getting prices for travel

Of course, other web activities are clearly not appropriate on a company's network:

- Using the web to search for a new job
- Any pornographic use
- Any use which violates local, state, or federal laws
- Use of the web to conduct employee's own business (i.e., an employee who is involved in another enterprise other than the company's business, such as eBay)

In addition, there are grey areas. Some activities might be acceptable to some organisations but not to others. Such activities might include:

- Online shopping during the employee's lunch or break time
- Reading news articles online during lunch or break time
- Viewing humorous websites

What one person might view as absurdly obvious might not be to another. It is critical that any organisation have very clear policies detailing specifically what is and what is not acceptable use of the web at work. Giving clear examples of what is acceptable use and what is not is important. You should also remember that most proxy servers and many firewalls could block certain websites. This will help prevent employees from misusing the company's web connection.

9.1.3 Email Attachments

Most business and even academic activity now occurs via e-mail. As we have discussed in several previous chapters, e-mail also happens to be the primary vehicle for virus distribution. This means that e-mail security is a significant issue for any network administrator.

Clearly you cannot simply ban all e-mail attachments. However, you can establish some guidelines for how to handle e-mail attachments. Users should open an attachment only if it meets the following criteria:

- It was expected (i.e., the user requested documents from some colleague or client).
- If it was not expected, it comes from a known source. If so, first contact that person and ask whether they sent the attachment. If so, open it.
- It appears to be a legitimate business document (that is, a spread sheet, a document, a presentation, etc.).

It should be noted that some people might find such criteria unrealistic. There is no question they are inconvenient. However, with the prevalence of viruses, often attached to e-mail, these measures are sensible. Many people choose not to go to this level to try to avoid viruses, and that may be your choice as well. Just bear in mind that millions of computers are infected with some sort of virus every single year.

No one should ever open an attachment that meets any of the following criteria:

- It comes from an unknown source.
- It is some active code or executable.
- It is an animation/movie.
- The e-mail itself does not appear legitimate. (It seems to tempt you to open the attachment rather than simply being a legitimate business communication that happens to have an attachment.)

If the end user has any doubt whatsoever, then should not open the e-mail. Rather, should contact someone in the IT department who

has been designated to handle security. That person can then either compare the e-mail subject line to known viruses or can simply come check out the e-mail personally. Then if it appears legitimate, the user can open the attachment.

9.1.4 Software Installation and Removal

This is one matter that does have an absolute answer. End users should not be allowed to install anything on their machine, including wall papers, screen savers, utilities etc. The best approach is to limit their administrative privileges so they cannot install anything. However, this should be coupled with a strong policy statement prohibiting the installation of anything on users' PCs. If they wish to install something, it should first be scanned by the IT department and approved.

This process might be cumbersome, but it is necessary. Some organisations go so far as to remove media drives (optical drive, USB, etc.) from end users' PCs so installations can occur only from files that the IT department has put on a network drive. This is usually a more extreme measure than most organisations will require, but it is an option you should be aware of.

9.1.5 Instant Messaging

Instant messaging is also widely used and abused by employees in companies and organisations. In some cases, instant messaging can be used for legitimate business purposes. However, it does pose a significant security risk. There have been viruses that propagated specifically via instant messaging. In one incident the virus would copy everyone on the user's buddy list with the contents of all conversations. Thus, a conversation the user thought was private was being broadcast to everyone with whom that user had messaged.

Instant messaging is also a threat from a purely informational security perspective. Without the traceability of an e-mail going through the corporate e-mail server, nothing stops an end user from instant messaging out trade secrets or other confidential information undetected. It is recommended that instant messaging simply be banned from all computers within an organisation. If you find your organisation absolutely must use it, then you must establish very strict guidelines for its use, including:

- Instant messaging may be used only for business communications, no personal conversations. Now this might be a bit difficult to enforce. More common rules, such as prohibiting personal web browsing, are also quite difficult to enforce. However, it is still a good idea to have those rules in place. Then if you find an employee violating them, you can refer to a company policy that prohibits such actions. However, you should be aware that in all likelihood you would not catch most violations of this rule.
- No confidential or private business information should be sent via instant messaging.

9.1.6 Desktop Configuration

Many users like to reconfigure their desktop. This means changing the background, screen saver, font size, resolution, and so on. Theoretically speaking, this should not be a security hazard. Simply changing a computer's background image cannot compromise the computer's security. However there are other issues involved.

The first issue is where the background image comes from. Frequently end users download images from the Internet, creating an opportunity for getting a virus or Trojan horse, particularly one using a hidden extension (e.g., it appears to be a mypic.jpg but is really mypic.jpg.exe). There are also human resources/harassment issues if an employee uses a backdrop or screen saver that is offensive to other employees. Some organisations simply decide to prohibit any changes to the system configuration for this reason.

The second problem is technical. In order to give a user access to change screen savers, background images, and resolution, you must give rights that also allow to change other system settings you might not want changed. The graphical display options are not separated from all other configuration options. This means that allowing the user to change screen saver might open the door to alter other settings that would compromise security (such as the network card configuration or the Windows Internet connection firewall).

9.1.7 Bring Your Own Device (BYOD)

Bring Your Own Device (BYOD) has become a significant issue for most organisations. Most, if not all, of your employees will have their own smart phones, tablets, smart watches, etc. that they will most likely carry with them into the workplace. When they connect to your wireless network, this introduces a host of new security concerns. You have no idea what networks those devices previously connected to, what software was installed on them, or what data might be exfiltrated by these personal devices.

In highly secure environments, the answer may be to forbid personally owned devices. However, in many organisations, such a policy is impractical. A workaround for that is to have a Wi-Fi network that is dedicated to BYOD and is not connected to the company's main network. Another approach, although more technologically complex, is to detect the device on connection, and if it is not a company-issued device, significantly limit its access.

There are also alternatives to BYOD. For example, Choose Your Own Device (CYOD) is a policy wherein the company allows the employee to bring their own device, but only if that device is from a list of pre-approved devices. This gives the company some control over what the user is connecting to the company network.

COPE, or Company Owned and Provided Equipment, is another option. In this scenario, the company provides the device, and has complete control over it. However, this can become an issue when the employee uses a device for both personal and professional purposes, not to mention the expense of providing employees with devices and maintaining those devices.

Whatever approach you take, you must have some policy regarding personal devices. They are already ubiquitous and spreading even more. Just a few years ago, smart phones were really the only BYOD device. But today there are smart watches, smart luggage, etc., and it is difficult to predict what new devices might be coming in the future.

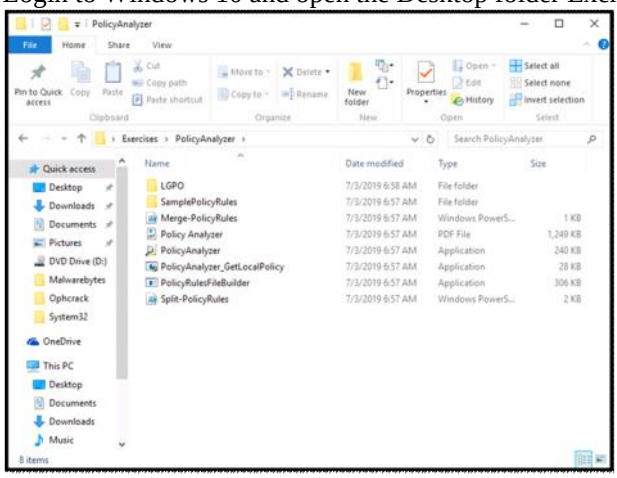
Guided Exercise: Analysing Policies

9.2 Guided Exercise: Analysing Policies

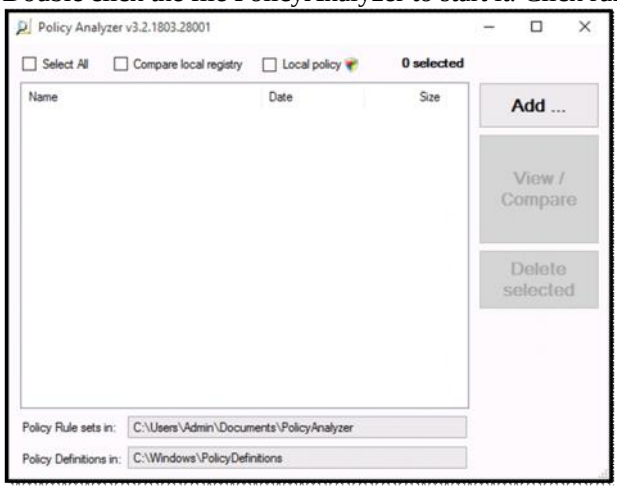
Resources	

Files	None
Machines	Windows 10

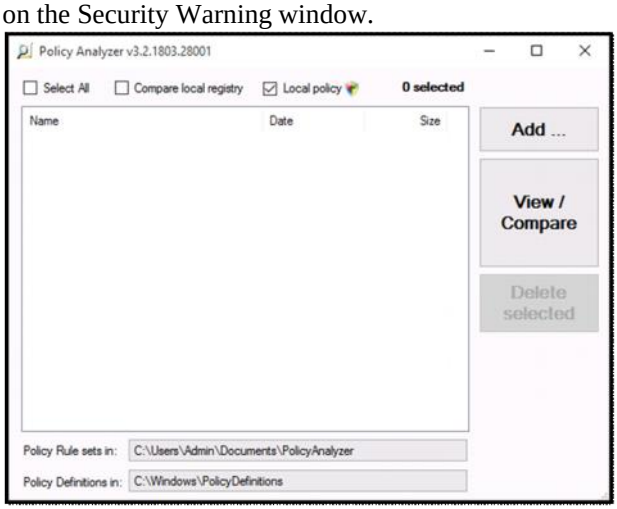
In this exercise you will use the PolicyAnalyser tool to analyse existing policies and provide recommendations.
Login to Windows 10 and open the Desktop folder Exercises -> PolicyAnalyzer.



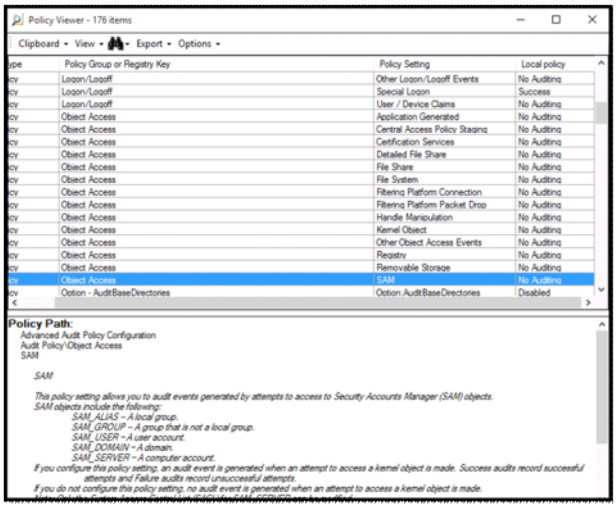
Double click the file PolicyAnalyzer to start it. Click run on the Security Warning window.



Check the box Local Policy and then click on View/Comapre button. Click Yes on the User Account Control Window and click Run on the Security Warning window.



Once the results are shown scroll till you find the Policy Setting for SAM. The Local policy says No Autiding. What will be your recommendation?



A recommendation will be to audit such object as the SAM file contains the password hashes for the Windows users.

System Administration Policies

9.3 System Administration Policies

In addition to determining policies for users, you must have some defined policies for system administrators. There must be a procedure for adding users, removing users, dealing with security issues, changing any system, and so on. There must also be procedures for handling any deviation.

9.3.1 New Employees

When a new employee is hired, the system administration policy must define specific steps to safeguard company security. New employees must be given access to the resources and applications their job functions require. The granting of that access must be documented (possibly in a log). It is also critical that each new employee receive a copy of the company's computer security/acceptable use policies and sign a document acknowledging receipt of such.

Before a new employee starts to work, the IT department (specifically network administration) should receive a written request from the business unit for which that person will be working. That request should specify exactly what resources this user will need and when will start. It should also have the signature of someone in the business unit with authority to approve such a request. Then, the person who is managing network administration or network security should approve and sign the request. After you have implemented the new user on the system with the appropriate rights, you can file a copy of the request.

9.3.2 Leaving Employees

When an employee leaves, it is critical to make sure all logins are terminated and all access to all systems is discontinued immediately. Unfortunately, this is an area of security that many organisations do not give enough attention to. It is imperative to have all of the former employee's access shut down on his last day of work. This includes physical access to the building. If a former employee has keys and is displeased, nothing can stop him from returning to steal or vandalize computer equipment. When an employee leaves the company, you should ensure that on his last day the following actions take place:

- All logon accounts to any server, VPN, network, or other resources are disabled.
- All keys to the facility are returned.
- All accounts for e-mail, Internet access, wireless Internet, cell phones, etc., are shut off.
- Any accounts for mainframe resources are cancelled.
- The employee's workstation hard drive is searched.

The last item might seem odd. However, if an employee was gathering data to take with him (proprietary company data) or conducting any other improper activities, you need to find out right away. If you do see any evidence of any such activity, you need to secure that workstation and keep it for evidence in any civil or criminal proceedings.

All of this might seem a bit extreme for some people. It is true that with the vast majority of exiting employees, you will have no issues of concern. However, if you do not make it a habit of securing an employee's access when he departs, you will eventually have an unfortunate situation that could have been easily avoided.

9.3.3 Change Requests

The nature of IT is change. Not only end users come and go, but requirements change frequently. Business units request access to different resources, server administrators upgrade software and hardware, application developers install new software, web developers change the website, and so on. Change is occurring all of the time. Therefore, it is important to have a change control process. This process not only makes the change run smoothly but also allows the IT security personnel to examine the change for any potential security problems before it is implemented. A change control request should go through the following steps:

- An appropriate manager within the business unit signs the request, signifying approval.
- The appropriate IT unit (database administration, network administrator, e-mail administrator, and so on) verifies that the request is one they can fulfil (from both a technological and a budgetary/business perspective).

- The IT security unit verifies that this change will not cause any security problems.
- The appropriate IT unit formulates a plan to implement the change and a plan to roll back the change in the event of some failure.
- The date and time for the change is scheduled, and all relevant parties are notified.

Your change control process might not be identical to this one; in fact, yours might be much more specific. However, the key to remember is that in order for your network to be secure, you simply cannot have changes happening without some process for examining their impact prior to implementing them.

Access Control

9.4 Access Control

An important area of security policies that usually generates some controversy in any organisation is access control. There is always a conflict between users' desire for unrestricted access to any data or resources on the network and the security administrator's desire to protect that data and resources. You cannot simply lock down every resource as completely as possible because that would block the users' access to those resources. Conversely, you cannot simply allow anyone and everyone complete access to everything.

It is worth keeping this acronym in mind when thinking about access control. Your goal is to make sure the data is accurate, confidential, and available only to authorised parties.

This is where the least privileges concept comes into play. The idea is simple. Each user, including IT personnel, gets the least access they can have to effectively do the job. Rather than asking the question "Why not give this person access to X?" you should ask "Why give this person access to X?" If you do not have a very good reason, then do not provide the access. This is one of the fundamentals of computer security. The more people who have access to any resource, the more likely some breach of security is to occur.

Clearly trade-offs between access and security must be made. One common example involves sales contact information. Clearly, a company's marketing department needs access to this data. However, what happens if competitors get all of your company's contact information? That information could allow them to begin targeting your current client list. This requires a trade-off between security and access. In this case, you would probably give sales people access only to the contacts that are within their territory. No one other than the sales manager should have complete access to all contacts.

QUIZ:

- 1.Always open email attachments coming from unknown sources.
- 2.Which of the following is the best reason users should be prohibited from installing software?
- 3.Which of the following should be recommended as acceptable e-mail attachments?
- 4.Instant messaging can be used not only for business communication but also for personall communication.
- 5.Which of the following is NOT an area user policies need to cover.
- 6.Which of the following is NOT an example of a user password policy?
- 7.1. Logon accounts, VPN, network and any other resources should NOT be disabled for leaving employees.
- 8.Passwords must always be shared with any person for any reason.
- 9.What should an employee do if she believes her password has been revealed to another party?
- 10.What is the best rule of thumb in access control?