Module in

ITP831 NETWORKING 2

Catanduanes State University

CICT

Disclaimer

This learning material is used in compliance with the flexible teaching-learning approach espoused by CHED in response to the pandemic that has globally affected educational institutions. Authors and publishers of the contents are well acknowledged. As such the college and its faculty do not claim ownership of all sourced information. This learning material will solely be used for instructional purposes not for commercialization.

College of Information and Communications Technology

MODULE 1 – Security Essentials

Learning Outcomes

At the end of the lesson the students shall be able to:

1. identify policies and best practices in network security.
2. configure various security measures
3. demonstrate how to secure a network

Key Terms

Hacker
Data breach
Vulnerability
Exploit
Social engineering
Authentication

Lesson 1.1 - Network Risk Management

As networks have turn out to be more geographically distributed and heterogeneous, the risk of their misuse has also increased. The threat of an outsider gaining access to an organization's network by using the Internet, and then taking or destroying data, is happening.

1.1.1 - Security Risks

Categories of Hackers

1. White Hat Hacker sometimes called ethical hackers

   These IT security experts are hired by organizations to assess their security and risks. Their goal is to identify security vulnerabilities of all kinds so the organization can make changes to increase their security. The extent of their efforts is usually clearly defined in a written contract before they begin their testing, and their activities are limited by existing laws and restrictions. At no point is private data compromised outside of that trusted relationship.
2. Black Hat Hacker

   These groups or individuals use their skills to bypass security systems to cause damage, steal data, or compromise privacy. They're not concerned with legal restrictions, and are intent on achieving personal gain or executing a personal agenda against an individual or an organization. Some black hat hackers and groups are also available for hire to serve someone else's agenda.
3. Gray Hat Hacker

   These hackers abide by a code of ethics all their own. Although they might engage in illegal activity, their intent is to educate and assist. For example, a computer hobbyist who hacks a local business's weak Wi-Fi password, and then reports that weakness to the business owners without damaging or stealing the company's data, has engaged in gray hat hacking. Gray hats are vulnerable to legal prosecution, and therefore often go to a great deal of effort to remain anonymous.

People Risks

By some estimates, human errors, ignorance, and omissions cause more than half of all security breaches sustained by networks. Human error accounts for so many security breaches because taking advantage of people is often an easy way to circumvent network security. End-user awareness and training can be a monumental task that requires regular attention and due diligence.

Common types of social engineering include the following:

- **Phishing** - An electronic communication that appears to come from a legitimate person or organization and requests access or authentication information.
- **Baiting -** A malware-infected file, such as a free music download, or device, such as a USB flash drive, is seemingly left unguarded for someone to take and attempt to use on their own computer.
- **Quid Pro Quo -** A gift or service is offered in exchange for private information or "temporary" access to the user's computer system. This tactic is surprisingly effective with employees who have not been adequately trained to detect social engineering attempts.
- **Tailgating** - A person posing as an employee or a delivery or service provider follows an authorized employee into a restricted area.

Technology Risks

Technology risks inherent in all seven layers of the OSI model.

The following risks are inherent in network hardware and design:

a. Spoofing Attack - MAC addresses can be impersonated in an attack called spoofing. Other types of spoofing attacks involve impersonating IP addresses. IP address spoofing can result in DoS (denial of service) attacks or modified DNS messages.
b. DoS (denial of service) attack - this attack occurs when a legitimate user is unable to access normal network resources, such as a web server, because of an attacker's intervention. Most often, this type of attack is achieved by flooding a system with so many requests for services that it cannot respond to any of them, as a result, all data transmissions are disrupted.

   DoS subtypes

   - DDoS (distributed DoS) attack - a DoS attack comes from one or a few sources owned by the attacker, DDoS attacks are orchestrated through many sources. The traffic spike caused by so many attackers is much more difficult to defend against than an attack from a single source. Effective firewalls can greatly reduce the chances of a computer being drafted into illegal botnets.

- DRDoS (distributed reflection DoS) attack - it is a DDoS attack bounced off of uninfected computers, called reflectors, before being directed at the target. This is achieved by spoofing the source IP address in the attack to make it look like all the requests for response are being sent by the target, then all the reflectors send their responses to the target, thereby flooding the target with traffic.
- Amplified DRDoS attack - A DRDoS attack can be amplified when conducted using small, simple requests that trigger very large responses from the target.
- PDoS (permanent DoS) attack - it damages a device's firmware beyond repair. This is called "bricking" the device because it effectively turns the device into a brick. PDoS attacks usually target routers or switches.
- friendly DoS attack - An unintentional DoS attack, or friendly attack, is not done with malicious intent.

c. DNS poisoning, or DNS spoofing - this is altering DNS records on a DNS server, which is an attacker can redirect Internet traffic from a legitimate web server to a phishing website.
d. ARP poisoning—this is when attackers use faked ARP replies to alter ARP tables in the network. ARP vulnerabilities contribute to the feasibility of several other exploits, including DoS (denial-of-service) attacks, MitM (man-in-the-middle) attacks, which is described next, and MAC flooding. MAC flooding involves overloading a switch with ARP replies.
e. MitM (man-in-the-middle) attack—this attack relies on intercepted transmissions and can take several forms. In all these forms, a person redirects and captures secure transmissions as they occur.
f. rogue DHCP server—Default trust relationships between one network device and another might allow a hacker to access the entire network because of a single flaw. DHCP messages should be monitored by a security feature on switches called DHCP snooping, in which any switch ports connected to clients are not allowed to transmit DHCP messages that should only come from a trusted DHCP server.
g. deauth (deauthentication) attack—in this attack, the attacker sends these faked deauthentication frames to the AP, the client, or both (or as a broadcast to the whole wireless network) to trigger the deauthentication process and knock one or more clients off the wireless network. This is essentially a Wi-Fi DoS attack in that valid users are prevented from having normal access to the network.
h. Insecure Protocols and Services—Certain TCP/IP protocols are inherently insecure.
i. Back doors - Software might contain back doors, which are security flaws that allow unauthorized users to gain access to the system.

Malware Risks

Malware (short for malicious software) refers to any program or piece of code designed to intrude upon or harm a system or its resources.

Types of Malware

- Virus - program that replicates itself with the intent to infect more computers, either through network connections when it piggybacks on other files or through the exchange of external storage devices. A virus might damage files or systems, or it might simply annoy users by flashing messages or pictures on the screen.
- Trojan horse (or Trojan) - program that disguises itself as something useful but harms your system; named after the famous wooden horse in which soldiers were hidden. Because Trojan horses do not replicate themselves, they are not considered viruses.
- Worm - program that runs independently of other software and travels between computers and across networks. They may be transmitted by any type of file transfer, including email attachments. Worms do not alter other programs in the same way that viruses do, but they can carry viruses.
- Bot (short for robot) - process that runs automatically, without requiring a person to start or stop it. Bots can be beneficial or malicious. Especially when used for ill intent, it does not require user interaction to run or propagate itself. Instead, it connects to a central server (called a command-and-control server, or C&C server) which then commands an entire botnet of similarly infected devices. Bots can be used to damage or destroy a computer's data or system files, issue objectionable content, launch DoS attacks, or open back doors for further infestation.
- Ransomware - program that locks a user's data or computer system until a ransom is paid. In most cases, the infection encrypts data on the computer, and can also encrypt data on backup devices, removable storage devices, and even cloud storage accounts connected to the computer, such as Dropbox or OneDrive. Currently, the only mostly reliable defense is to make manual backups of data on a regular basis and disconnect the backup media from the computer between backups.

Some Characteristics of a Malware

- Encryption - some malware is encrypted to prevent detection. Most antimalware software searches files for a recognizable string of characters that identify the virus. However, encryption can prevent the anti-malware program's attempts to detect it.
- Stealth - some malware disguises itself as legitimate programs or replaces part of a legitimate program's code with destructive code.
- Polymorphism - Polymorphic malware changes its characteristics (such as the arrangement of bytes, size, and internal instructions) every time it's transferred to a new system, making it harder to identify.
- Time dependence - some malware is programmed to activate on a particular date. This type of malware can remain dormant and harmless until its activation date arrives. Time-dependent malware can include logic

bombs, or programs designed to start when certain conditions are met. (Logic bombs can also activate when other types of conditions, such as a specific change to a file, are met, and they are not always malicious.)

1.1.2 - Security Assessment

In examining network security risks, consider the effect that a loss or breach of data, applications, or access would have on your network. The more serious the potential consequences, the more attention you need to pay to security. Every organization should assess its security risks by conducting a posture assessment, which is a thorough examination of each aspect of the network to determine how it might be compromised. The more devastating a threat's effects and the more likely it is to happen, the more rigorously your security measures should address it. Posture assessments should be performed at least annually and preferably quarterly. They should also be performed after making any significant changes to the network.

Scanning Tools

To ensure that your security efforts are thorough, it helps to think like a hacker. During a posture assessment, for example, you might use some of the same methods a hacker uses to identify cracks in your security architecture.

Three types of attack simulations:

1. vulnerability scanning, or vulnerability assessment
   - This technique is used to identify vulnerabilities in a network. It's often performed by a company's own staff and does not attempt to exploit any vulnerabilities.
   - Vulnerability scanning might also be the first step in other attack simulations or in a real attack.
   - During attack simulations, there are two types of vulnerability scans:
     - ✓ Authenticated - In this case, the attacker is given the same access to the network as a trusted user would have, such as an employee or an intruder who has somehow hacked into a user's account.
     - ✓ Unauthenticated - In this case, the attacker begins on the perimeter of the network, looking for vulnerabilities that do not require trusted user privileges.

2. penetration testing
   - This attack simulation uses various tools to find network vulnerabilities, as in vulnerability scanning, and then attempts to exploit those vulnerabilities.

3. red team-blue team exercise
   - During this exercise, the red team conducts the attack, and the blue team attempts to defend the network.
   - Usually the red team is a hired attacker, such as a consultant or security organization, and the blue team is the company's own IT, security, and other staff.
   - In some cases, the blue team has no warning of the impending attack in order to better evaluate day-to-day defenses.

- The red team relies heavily on social engineering to attempt to access the company’s private data, accounts, or systems without getting caught.
- The company’s detection and response to the attack is the primary focus, rather than the technical vulnerabilities of the network itself.

Scanning tools provide a simple and reliable way to discover crucial information about your network, including, but not limited to, the following:

- Every available host
- Services, including applications and versions, running on every host
- Operating systems running on every host
- Open, closed, and filtered ports on every host • Existence, type, placement, and configuration of firewalls
- Software configurations
- Unencrypted, sensitive data

Three popular scanning tools

1. Nmap - The scanning tool Nmap and its GUI version Zenmap are designed to scan large networks quickly and provide information about a network and its hosts. Nmap began as a simple port scanner, which is an application that searches a device for open ports indicating which insecure service might be used to craft an attack.

2. Nessus - Developed by Tenable Security (tenable.com), Nessus performs even more sophisticated vulnerability scans than Nmap. Among other things, Nessus can identify unencrypted, sensitive data, such as credit card numbers, saved on your network’s hosts. The program can run on your network or from off-site servers continuously maintained and updated by the developer.

3. Metasploit - This popular penetration testing tool combines known scanning and exploit techniques to explore potentially new attack routes.

Honeypots and Honeynets

Honeypot, or a decoy system is purposely vulnerable and filled with what appears to be sensitive (though false) content, such as financial data. To lure hackers, the system might be given an enticing name, such as one that indicates a name server or a storage location for confidential data. Once hackers access the honeypot, a network administrator can use monitoring software and logs to track the intruder’s moves. In this way, the network administrator might learn about new vulnerabilities that must be addressed on his real networked hosts. To fool hackers and gain useful information, honeypots cannot appear too blatantly insecure, and tracking mechanisms must be hidden. In addition, a honeypot must be isolated from secure systems to prevent a savvy hacker from using it as an intermediate host for other attacks. In more elaborate setups, several honeypots might be connected to form a honeynet. Honeypot software options include KFSensor (keyfocus.net), Canary (canary.tools), and Honeyd (honeyd.org).

1.1.3 - Physical Security

Physical access to all a network's critical components must be restricted and controlled. Preventative measures such as locked doors can make it more difficult for unauthorized people to get into these areas. However, it is also important to have good detection measures in place for those times when someone is able to breach a secured perimeter.

Prevention Methods

Security policy defines who has access to the computer room, locking the locations of networking equipment is necessary to keep unauthorized individuals out.

Door access controls

- keypad or cipher lock - Electronic keypads, also called cipher locks, are physical or electronic locks that require a code to open the door, which can reduce the inherent risk of lost keys.
- key fob—A key fob provides remote control over locks and security systems.To reduce the number of devices you need to carry, many lock types allow you to use a key fob app installed on a smartphone.
- access badge - Most companies require employees to have some kind of ID badge that identifies the person by name and perhaps includes a photo, title, and other information.
- proximity card - Some badges, are actually proximity cards (also called prox cards), which do not require direct contact with a proximity reader in order to be detected. In fact, a reader can be concealed inside a wall or other enclosure and requires very little maintenance. With a typical range of about 5–10 cm, the card can be detected even while it is still inside a wallet or purse, or it can be incorporated or duplicated in a key fob.
- biometrics—A more expensive physical security solution involves biorecognition access, in which a device scans an individual's unique physical characteristics, called biometrics, such as the color patterns in her iris or the geometry of her hand, to verify her identity.

Detection Methods

Methods of detecting physical intrusions and other kinds of events:

- motion detection - Motion detection technology, which triggers an alarm when it detects movement within its field of view, has been around for a long time. The latest motion detectors can discern between different types of motion, such as small animals, blowing plants, or walking humans, to reduce false alarms. Motion sensors might be configured to record date and time of motion detection, or trigger lights, alarms, or video cameras.
- video surveillance - Many IT departments use video surveillance systems, called CCTV (closed-circuit TV), to monitor activity in secured data rooms. IP cameras can be placed in data centers, computer rooms, data rooms, and data storage areas, as well as facility entrances. The cameras might run continuously, or they might be

equipped with motion detectors to start recording when movement occurs within their viewing area. The video footage generated from these cameras is contained within a secure segment of the network, and is usually saved for a period of time in case it's needed later in a security breach investigation or prosecution.

- tamper detection - Many devices that need protection can't be kept within a secure area. For example, utility meters, parking meters, entry doors, ATMs, network cables, and even security cameras are potential targets. Tamper detection sensors on these devices can detect physical penetration, temperature extremes, input voltage variations, input frequency variations, or certain kinds of radiation. This might trigger defensive measures such as an alarm or shutdown, or it might activate a video camera or other security system.
- asset tracking - Asset tracking tags can be used to monitor the movement and condition of equipment, inventory, and people. Whether a simple barcode or a wireless-enabled transmitter, such as the RFID, asset tracking enables constant or periodic collection of information. This data is then reported to a central management application for monitoring, logging, and reporting. As wireless technologies have improved, these asset tracking systems have grown beyond Wi-Fi-dependent systems, which tend to be expensive and require frequent battery replacement for each asset being tracked. Today, these systems often use Bluetooth, RFID (such as NFC), cellular, and GPS wireless technologies.

As with other security measures, the most important way to ensure physical security is to plan for it. You can begin your planning by asking questions related to physical security checks in your security audit. Consider the following questions:

- Which rooms contain critical systems or data and must be secured?
- Through what means might intruders gain access to the facility, computer room, data room, network closet, or data storage areas (including doors, windows, adjacent rooms, ceilings, large vents, temporary walls, hallways, and so on)?
- How and to what extent are authorized personnel granted entry? Do they undergo background or reference checks? Is their need for access clearly justified? Are their hours of access restricted? Who ensures that lost keys or ID badges are reported?
- Are employees instructed on how to ensure security after entering or leaving secured areas (for example, by not propping open doors)?
- Are authentication methods (such as ID badges) difficult to forge or circumvent?
- Do supervisors or security personnel make periodic physical security checks?
- Are all combinations, codes, or other access means to computer facilities protected at all times, and are these combinations changed frequently?
- What is the plan for documenting and responding to physical security breaches?

Lesson 1.2 - Security in Network Design

1.2.1 - Network Security Devices

Most of the network devices now a days are designed with security features and even those devices that primarily serve non-security purposes, are equipped with significant security features and abilities. Proxy servers and ACLs on network devices are examples of non-security devices with security features, while firewalls and IDS/IPS systems are the network's specialized security devices. Combinations of multiple options for network security results in layered security and provides more protection than any one type of device or security.

Proxy Servers

According to West, J. et.al, a proxy server, or proxy, acts as an intermediary between the external and internal networks, screening all incoming and outgoing traffic. Proxy servers manage security at the Application layer of the OSI model. Although proxy servers only provide low-grade security relative to other security devices, they can help prevent an attack on internal network resources such as web servers and web clients.

A proxy server represents a private network to another network (usually the Internet). Although a proxy server appears to the outside world as an internal network server, in reality it is merely another filtering device for the internal LAN. One of its most important functions is preventing the outside world from discovering addresses on the internal network.

For example, suppose your LAN uses a proxy server, and you want to send an email message from your workstation inside the LAN to a colleague via the Internet. The following steps describe the process:

Step 1: Your message goes to the proxy server. Depending on the configuration of your network, you might or might not have to log on separately to the proxy server first.

Step 2: The proxy server repackages the data frames that make up the message so that, rather than your workstation's IP address being the source, the proxy server inserts its own IP address as the source.

Step 3: The proxy server passes your repackaged data to a packet-filtering firewall.

Step 4: The firewall verifies that the source IP address in your packets is valid (that it came from the proxy server) and then sends your message to the Internet.

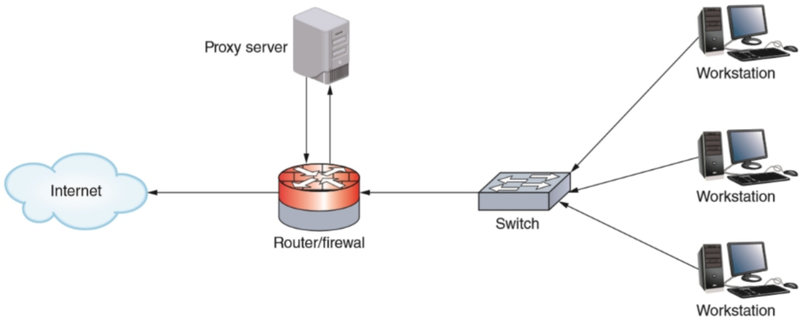


Figure 1.2 – 1 - Proxy server is used to connect to the Internet

ACLs (Access Control Lists) on Network Devices

A router's main function is to examine packets and determine where to direct them based on their Network layer addressing information.

A router's ACL (access control list), or access list, routers can also decline to forward certain packets depending on their content.

An ACL acts like a filter to instruct the router to permit or deny traffic according to one or more of the following variables:

- Network layer protocol (for example, IP or ICMP)
- Transport layer protocol (for example, TCP or UDP)
- Source IP address
- Destination IP address (which can restrict or allow certain websites)
- TCP or UDP port number

Each time a router receives a packet, it examines the packet and refers to its ACL to determine whether the packet meets criteria for permitting or denying travel on the network.

An access list is not automatically installed on a router. If you don't configure an ACL, the router allows all traffic through. Once you create an ACL and assign it to an interface, you have explicitly permitted or denied certain types of traffic.

Naturally, the more statements or tests a router must scan (in other words, the longer the ACL), the more time it takes a router to act, and, therefore, the slower the router's overall performance.

When troubleshooting a problematic connection between two hosts, or between some applications or ports on two hosts, consider that the problem might be a misconfigured ACL. Common errors include listing the ACL statements in the wrong order, using the wrong criteria when defining a rule, and constructing a rule incorrectly.

Firewalls

A firewall is a specialized device or software that selectively filters or blocks traffic between networks. A firewall protects a network by blocking certain traffic from traversing the firewall's position, similar to a bouncer checking IDs at the entrance to a private club. While firewalls include filtering from ACLs, they also offer a wide variety of other methods to evaluate, filter, and control network traffic. A firewall might be placed internally, residing between two interconnected private networks. More commonly, the firewall is placed on the edge of the private network, monitoring the connection between a private network and a public network (such as the Internet).

Some common criteria by which a packet-filtering firewall might accept or deny traffic include the following:

- Source and destination IP addresses
- Source and destination ports (for example, ports that supply TCP/UDP connections, FTP, Telnet, ARP, ICMP, and so on)
- Flags set in the TCP header (for example, SYN or ACK)
- Transmissions that use the UDP or ICMP protocols
- A packet's status as the first packet in a new data stream or a subsequent packet

- A packet's status as inbound to or outbound from your private network

For greater security, you can choose a firewall that performs more complex functions than simply filtering packets. Among the factors to consider when making your decision are the following:

- Does the firewall support encryption?
- Does the firewall support user authentication?
- Does the firewall allow you to manage it centrally and through a standard interface?
- How easily can you establish rules for access to and from the firewall?
- Does the firewall support filtering at the highest layers of the OSI model, not just at the Data Link and Transport layers?
- Does the firewall provide internal logging and auditing capabilities, such as IDS or IPS?
- Does the firewall protect the identity of your internal LAN's addresses from the outside world?
- Can the firewall monitor packets according to existing traffic streams?

A stateful firewall is able to inspect each incoming packet to determine whether it belongs to a currently active connection (called a stateful inspection) and is, therefore, a legitimate packet. A stateless firewall manages each incoming packet as a stand-alone entity without regard to currently active connections. Stateless firewalls are faster than stateful firewalls, but are not as sophisticated.

In response to the increasing complexity of threats against computing resources, vendors of firewalls and their related products continue to improve and innovate. One such innovation is **UTM (Unified Threat Management)**, which is a security strategy that combines multiple layers of security appliances and technologies into a single safety net. A UTM solution can provide a full spread of security services managed from a single point of control.

NGFW (Next Generation Firewalls) - a subset of UTM, also called Layer 7 firewalls, have some innovative features:

- application aware - Monitor and limit the traffic of specific applications, including the application's vendor and digital signature. This includes built-in Application Control features.
- user aware - Adapt to the class of a specific user or user group.
- context aware - Adapt to various applications, users, and devices.

This more granular control of configuration settings enables network administrators to fine-tune their security strategies to the specific needs of their companies. NGFWs are popular choices for larger enterprises that need to customize their security policies.

IDS (Intrusion Detection System)

An IDS (intrusion detection system) is a stand-alone device, an application, or a built-in feature running on a workstation, server, switch, router, or firewall. It monitors network traffic, generating alerts about suspicious activity. Whereas a router's ACL or a firewall acts like a bouncer at a private club who checks everyone's ID and ensures that only club members enter through the door, an IDS is generally installed to provide security monitoring inside the network, similar to security personnel sitting in a private room monitoring closed-circuit cameras in the club and alerting other security personnel when they see suspicious activity. These days, IDS most commonly exists as an embedded feature in UTM solutions or NGFWs.

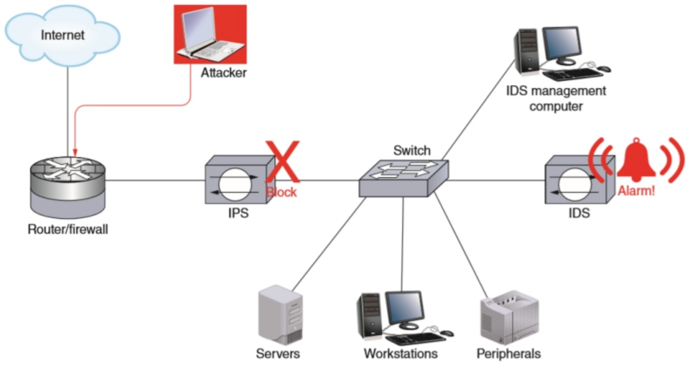


Figure 1.2 – 2 - An IDS detects traffic patterns, while an IPS can intercept traffic that might threaten a corporate network

An IDS uses two primary methods for detecting threats on the network:

- statistical anomaly detection - Compares network traffic samples to a predetermined baseline to detect anomalies beyond certain parameters
- signature-based detection - Looks for identifiable patterns, or signatures, of code that are known to indicate specific vulnerabilities, exploits, or other undesirable traffic on the organization’s network (such as games). To maintain effectiveness, these signatures must be regularly updated in a process called signature management. This also includes retiring irrelevant signatures and selecting the signatures most relevant to a specific network’s needs to most efficiently use memory and processing resources when scanning network traffic.

IPS (Intrusion Prevention System)

An IPS (intrusion prevention system) stands in-line between the attacker and the targeted network or host and can prevent traffic from reaching that network or host. If an IDS is like security personnel using closed-circuit cameras to monitor a private club, an IPS would be like security personnel walking around in the club available to escort unruly patrons to the exit door.

IPSes were originally designed as a more comprehensive traffic analysis and protection tool than firewalls. However, firewalls have evolved, and as a result, the differences between a firewall and an IPS have diminished. Because an IPS stands in-line with network traffic, it can stop that traffic. For example, if an IPS detects a hacker’s attempt to flood the network with traffic, it can prevent that traffic from proceeding to the network. Thereafter, the IPS might quarantine that malicious user based on the sending device’s IP address. At the same time, the IPS continues to allow valid traffic to pass.

Both an IDS and IPS can be placed inside a network or on the network perimeter.

SIEM (Security Information and Event Management)

SIEM (Security Information and Event Management) systems can be configured to evaluate all data stored in logs, looking for significant events that require attention from the IT staff according to predefined rules. When one of these rules is triggered, an alert is generated and logged by the system. If programmed to do so, a notification is then sent to IT personnel via email, text, or some other method.

The challenge is to find the right balance between sensitivity and workload. The network administrator can fine-tune a SIEM's rules for the specific needs of a particular network by defining which events should trigger which responses.

The SIEM system can also be configured to monitor particular indicators of anticipated problems or issues. These rules should be reevaluated periodically. Also, network technicians should review the raw data on a regular basis to ensure that no glaring indicators are being missed by existing rules.

Examples of SIEM software include AlienVault OSSIM (Open Source SIEM), IBM Security QRadar SIEM, SolarWinds Log & Event Manager, and Splunk ES (Enterprise Security).

1.2.2 - Switch Management

Switch Path Management

Network designed with redundancy of switches at critical stages makes the network fault tolerant. For example, if one switch suffers a power supply failure, traffic can reroute through a second switch. But potential problem with this kind of network has to do with traffic loops. To eliminate the possibility of this problem and other types of traffic loops, STP (Spanning Tree Protocol) was used.

STP (Spanning Tree Protocol):

- was developed by Radia Perlman at Digital Equipment Corporation in 1985 and then adopted by the IEEE in 1990.
- the first iteration of STP, defined in IEEE standard 802.1D, functions at the Data Link layer.
- it prevents traffic loops, also called switching loops, by calculating paths that avoid potential loops and by artificially blocking the links that would complete a loop.
- it can adapt to changes in the network. For instance, if a switch is removed, STP will recalculate the best loop-free data paths between the remaining switches.

Switch Port Security

Unused physical and virtual ports on switches and other network devices can be accessed and exploited by hackers and should be disabled until needed.

Shutdown command can be used in Cisco, Huawei, and Arista routers and switches. To enable them again, use the *no shutdown command* on Cisco or Arista devices, and use undo shutdown on Huawei devices. On a Juniper device, the corresponding commands are *disable and enable*, respectively. Another Cisco command (which is also used on Arista devices) to secure switch access ports is *switchport port-security* (or just port-security on Huawei switches). This is essentially a MAC filtering function that also protects against MAC flooding, which makes it a type of flood guard.

1.2.3 - AAA (Authentication, Authorization, and Accounting)

This is also known as triple-A that manages access control to a network and its resources

- Authorization - once a user has access to the network, the authorization process determines what the user can and cannot do with network resources. In other words, authorization asks the question, “What are you allowed to do?” Authorization restrictions affect Layer 2 segmentation, Layer 3 filtering, and Layer 7 entitlements. For example, what VLAN are you assigned to? What servers or databases can you access? What commands can you run on a device?
- Accounting - the accounting system logs users’ access and activities on the network. In other words, accounting asks, “What did you do?” The records that are kept in these logs are later audited, either internally or by an outside entity, to ensure compliance with existing organizational rules or external laws and requirements.

Authentication

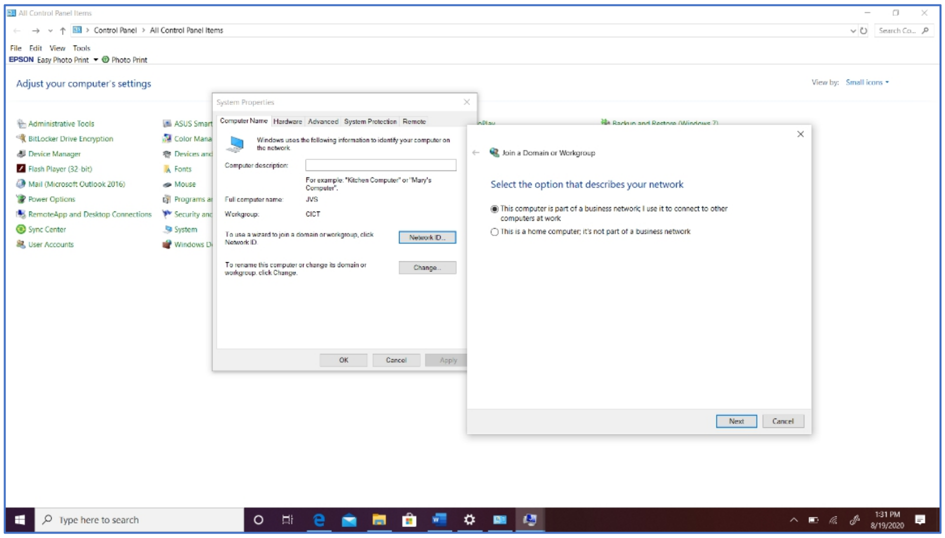
A user can be authenticated to the local device or to the network. Authentication asks the question, “Who are you?”

Local Authentication Local authentication processes are performed on the local device. Usernames and passwords are stored locally, which has both advantages and disadvantages:

- low security - Most end user devices are less secure than network servers. A hacker can attempt a brute force attack or other workarounds to access a single device. If those same credentials are used on other devices, then all these devices are compromised. Also, local authentication does not allow for remotely locking down a user account.
- convenience varies - For only a handful of devices, managing local accounts can be done a lot more easily than setting up a Windows domain, directory services, and all the supporting configurations. However, once you surpass about a dozen devices, the convenience of local authentication declines considerably.
- reliable backup access - In the case of a network failure or server failure, the only workable option is local authentication. For this reason, networking devices and servers should be configured with a local privileged account that is only used when authentication services on the network are unavailable, and of course this account should have very secure credentials.

With local authentication, every computer (workstation or server) on the network is responsible for securing its own resources. If several users need access to a file server, for example, each user must have a local user account on the file server. This local account and password must match the user account and password that the account holder used to sign in to Windows at his or her workstation.

In Windows, you can switch from local authentication to network authentication on the domain using the System Properties dialog box.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: JVS

Workgroup: CICT

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Select the option that describes your network

● This computer is part of a business network; I use it to connect to other computers at work

○ This is a home computer; it's not part of a business network

Figure 1.2 – 2 - Switch from local authentication to authentication on a Windows domain

Authentication restrictions that strengthen network security:

- time of day
- total time logged on
- source address
- unsuccessful logon attempts
- geographic location -

Authorization

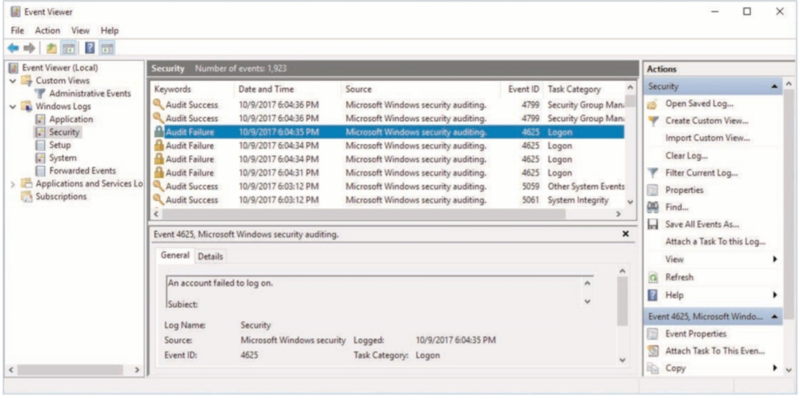
- User access to network resources falls into one of these two categories:
  1. the privilege or right to execute, install, and uninstall software,
  2. permission to read, modify, create, or delete data files and folders.
- The most popular authorization method is RBAC (role-based access control). With role-based access control, a network administrator receives from a user's supervisor
- The administrator is responsible for assigning the privileges and permissions necessary for the user to perform only these roles.
- Two other popular methods of access control in addition to RBAC are **DAC** and **MAC**. The least secure of these options is DAC (discretionary access control). This is where users decide for themselves who has access to that user's resources. The most restrictive is MAC (mandatory access control). In this case, resources are organized into hierarchical classifications, such as "confidential" or "top secret." Resources are also grouped into categories, perhaps by department. Users, then, are also classified and

categorized. If a user's classification and category matches those of a resource, then the user is given access.

Accounting

With a Linux or Macintosh NOS, most logs are generated as text files. These text files can get quite long and a network administrator is responsible for making sure they don't control server storage space. In addition, you can install a log file viewer to make it easier to monitor log files for interesting or suspicious events.

In Windows, you can use Event Viewer to view Windows logs. But before these logon events are logged, you must use Group Policy to turn on the feature.



Security Number of events: 1,923

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	10/9/2017 6:04:36 PM	Microsoft Windows security auditing.	4799	Security Group Man:
Audit Success	10/9/2017 6:04:36 PM	Microsoft Windows security auditing.	4799	Security Group Man:
Audit Failure	10/9/2017 6:04:35 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:34 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:34 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	10/9/2017 6:04:31 PM	Microsoft Windows security auditing.	4625	Logon
Audit Success	10/9/2017 6:03:12 PM	Microsoft Windows security auditing.	5059	Other System Events
Audit Success	10/9/2017 6:03:12 PM	Microsoft Windows security auditing.	5061	System Integrity

Event 4625, Microsoft Windows security auditing.

An account failed to log on.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 10/9/2017 6:04:35 PM
Event ID: 4625 Task Category: Logon

NAC (Network Access Control) Solutions

BYOD (bring your own device) environments, makes the network administrators have struggled with the need to balance network access with network security. These challenges have, in turn, sparked a variety of solutions. To help manage the complexity, a NAC (network access control) system takes authentication, authorization, and accounting to a new level.

A NAC system employs a set of rules, called network policies, which determine the level and type of access granted to a device when it joins a network. A popular NAC solution by Cisco includes Cisco firewalls, routers, switches, and ASA (Adaptive Security Appliance) devices that all collectively perform NAC functions. In addition, Microsoft offers NAP (Network Access Protection) software that functions as a NAC solution in Windows Server.

NAC systems authenticate and authorize devices by verifying that the device complies with predefined security benchmarks, such as whether the device has certain system settings, or whether it has specific applications installed. On some networks, software called an agent must be installed on the device before the device can be authenticated. The agent monitors the device's status regarding the security benchmarks to determine the device's compliance.

Two types of agents are commonly used:

- A **nonpersistent agent**, or dissolvable agent, remains on the device long enough to verify compliance and complete authentication, and then uninstalls. Devices might be required to periodically reinstall the agent to complete the authentication process again.

- A **persistent agent** is permanently installed on a device. This more robust program might provide additional security measures, such as remote wipe, virus scans, and mass messaging. Not all networks require agents.

Another option is Active Directory, which allows for agentless authentication, in which the user is authenticated to a domain. Active Directory then scans the device to determine compliance with NAC requirements.

Supplementary Learning Resources

http://dl.booktolearn.com/ebooks2/computer/networking/9781337569330_Network_Guide_to_Networks_8th_Edition_fe64.pdf

https://www.youtube.com/watch?v=4PPUvRj2PvM

REFERENCES

Krause, Jordan (2019). ***Mastering Windows Server 2019 Second Edition***,Packt Publishing, ISBN 97 8-1 -7 8980-453-9

Lowe, Doug(2018). ***Networking All-in-One For Dummies 7th Edition***,John Wiley & Sons, Inc.New Jersey,ISBN 978-1-119-47159-2

http://www.fao.org/3/a-au767e.pdf

https://www.geog.ox.ac.uk/research/technologies/projects/mesc/guide-to-monitoring-and-evaluation-v1-march2014.pdf

http://www.psc.gov.za/documents/docs/guidelines/PSC%206%20in%20one.pdf