WIFI

Wi-Fi Protected Setup (WPS) is a non-proprietary and optional push-button configuration specification that is considered a security vulnerability and should not be used in the enterprise. It is commonly attacked either online or offline against the PIN generated by the Wireless Access Point (WAP) entered on the device.
According to the Wi-Fi Alliance, Protected Management Frames offers protection for unicast and multicast management action frames. Unicast management action frames are protected from both eavesdropping and forging, and multicast management action frames are protected from forging. They augment privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks.

IOT

Zigbee is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs.
The Internet of Things or IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people. These objects are enabled with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human--to-computer interaction. An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments..

IEEE802.1X

There are three components in the 802.1X architecture: supplicant (or client), network authorization device (NAD) or Authenticator, and authentication server. The client is the NAD and the server is usually a RADIUS or TACACS/TACACS+ server. The supplicant is a combination of the endpoint attempting to get on the network and the software agent running on the device.

NETCAT

Netcat is the Swiss army knife of networking tools and it can be run standalone or in an exploit kit. The most common cracking uses for Netcat are setting up reverse and bind shells, piping and redirecting network traffic, port listening, debugging programs and scripts and banner grabbing by making a raw connection to an FTP or Web server.

AWS

At AWS, Security groups (SGs) are tied to an instance whereas Network Access Control Lists ACLs are tied to the subnet. While NACLs allow or deny traffic before it reaches an SG, the SG controls the traffic flow to and from the instance.
The AWS Key Management System (KMS). It supports asymmetric keys. You can create, manage, and use public/private key pairs to protect your application data using the new APIs via the AWS SDK.

CLOUD

Auto-scaling is the cloud platform’s capacity to react to the live traffic load on the application/workload by spinning up or down server instances on an ad-hoc basis. This ability to auto scale allows the provider to add or remove additional computing power to the instance cluster based on the demand and thus ensure the consistent handling of the traffic and optimize costs.

AZURE

To create or delete management locks, you must have access to Microsoft.Authorization/ *or Microsoft.Authorization/locks/* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions.
An Availability Zone (AZ) is a high-availability offering that protects applications and data from data center failures. AZs are unique physical locations within an Azure region. Each zone is made up of one or more data centers equipped with independent power, cooling, and networking. To ensure resiliency, each enabled region has a minimum of three separate zones. The physical separation of Availability Zones within a region protects applications and data in the event of data center failures.
Office 365 uses Azure Active Directory (Azure AD), a cloud-based user identity and authentication service that is included with your Office 365 subscription, to manage identities and authentication for Office 365. In fact, any person with an existing Microsoft email account has an instance of Azure AD just waiting for activation.
Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet. IaaS quickly scales up and down with demand, letting you pay only for what you use. It helps you avoid the expense and complexity of buying and managing your own physical servers and other datacenter infrastructure. Each resource is offered as a separate service component, and you only need to rent a particular one for as long as you need it.

MAQUINA VIRTUAL

Xen, Red Hat, KVM, VMware, and Hyper-V are examples of hypervisors. A hypervisor is software that creates and runs virtual machines or VMs. The hypervisor creates an abstraction of underlying hardware and the VMs that use its resources are guests. A hypervisor is sometimes also called a Virtual Machine Manager (VMM).
A hypervisor is the software that generates and controls a virtual infrastructure allowing multiple OSs to run on a single physical machine my managing the finite resources of the system running the hypervisor called the “host” and the virtual machines running on the host called “guests”.
Containers isolate applications from each other on a shared OS. Containerized applications run on top of a container host that in turn runs on the OS (Linux or Windows). Containers therefore have a significantly smaller footprint than virtual machine (VM) images. Containerization is an approach to software development in which an application or service, its dependencies, and its configuration are packaged together as a container image.

IAM

Identity and Access Management (IAM) ensures that users are who they say they are (authentication) and that they can access the applications and resources they have permission to use (authorization). IAM solutions include single sign-on (SSO), multi-factor authentication (MFA) and access management, as well as directory for securely storing identity and profile data and data governance to ensure that only needed and relevant data is shared.

CIS CONTROLS

Center for Internet Security (CIS) is a forward-thinking nonprofit that harnesses the power of a global IT community to safeguard public and private organizations against cyber threats. Following are the foundational controls defined by CIS.
Foundational CIS Controls:
• Email and Web Browser Protections
• Malware Defenses
• Limitation and Control of Network Ports, Protocols and Services
• Data Recovery Capabilities
• Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

CIS CONTROLS (cont)

• Boundary Defense
• Data Protection
• Controlled Access Based on the Need to Know
• Wireless Access Control
• Account Monitoring and Control

The CIS 20 organizational controls are as follows:

• Implement a Security Awareness and Training Program,
• Application Software Security,
• Incident Response and Management, and
• Penetration Tests and Red Team Exercises.

Basic CIS Controls:

• Inventory and Control of Hardware Assets
• Inventory and Control of Software Assets
• Continuous Vulnerability Management
• Controlled Use of Administrative Privileges
• Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
• Maintenance, Monitoring and Analysis of Audit Logs

NFC

NFC stands for “Near Field Communication” and, as the name implies, it enables short-range communication between compatible devices. This requires at least one transmitting device, and another to receive the signal. A range of devices can use the NFC standard and will be considered either passive or active. NFC is a mainstream wireless technology. Passive NFC devices include tags, and other small transmitters, that can send information to other NFC devices without the need for a power source of their own. Active devices are able to both send and receive data and can communicate with each other as well as with passive devices..

LOAD BALANCER

Network Load Balancer (NLB) distributes traffic based on network variables, such as IP address and destination ports. It is layer 4 (TCP) and below and is not designed to take into consideration anything at the application layer such as content type, cookie data, custom headers, user location, or the application behavior. Application Load Balancer (ALB) on the other hand distributes requests based on multiple variables, from the network layer to the application layer. ALB is full-featured Layer-7 load balancer, HTTP and HTTPS listeners only..

PHISHING

A whaling attack is a phishing variant that targets senior management in an attempt to steal sensitive data like financial information or personal employee information typically for malicious reasons.
Typosquatting (also known as URL hijacking), is a form of cybersquatting targeting people that mistype an intended website address into their web browser. Cybersquatters register domain names that are a slight variation of the target URL, which is usually a common spelling error. Typosquatting is a form of social engineering attack that tries to lure users into visiting malicious sites with URLs that are common misspellings of legitimate sites. These sites can cause significant damage to the reputation of organizations that are victimized by these attackers and harm users who are tricked into entering sensitive details into fake sites. For example, gooogle, facebooj..

RANSOMWARE

Since ransomware encrypts files instead of exfiltrating files, a rigorous backup and restore policy involving snapshots and disk imaging will eliminate most of the impact of the malware attack. Anti-ransomware solutions enable organizations to fight against ransomware.

RANSOMWARE

Since ransomware encrypts files instead of exfiltrating files, a rigorous backup and restore policy involving snapshots and disk imaging will eliminate most of the impact of the malware attack. Anti-ransomware solutions enable organizations to fight against ransomware.

DEFENSE IN DEPTH

The classification and labeling of all data assets is a combination of uniform protection and information-centric defense-in-depth. Vector-oriented defense in depth involves identifying all ingress and egress points and all probable threat agents and specific vectors.
The defense-in-depth approach is a layered approach to security. By providing various layers of security or security controls, for example, physical security, policies and procedures, firewalls at perimeter, IPS/IDS at DMZ, antiviruses and anti-malwares at host and network level, a network can be better protected against threats than deploying just one security control.
Defense in depth involves implementing multiple layers of security to defend property, facilities, systems, applications, and data. According to the SANS institute, there are four fundamental approaches to defense in depth, based on risk treatment: Uniform protection, Protected zoning, Information centric, and analyze threat vectors.
Honey tokens (aka Honey pots) are placed on systems in reasonable locations but not where the average end users would find them. A honeypot is a computer or computer system intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate valuable target system or Honeypots can also be used to gain information about how cybercriminals operate.

DEFENSE IN DEPTH (cont)

A honeypot is a computer or system intended to imitate the likely targets of cyberattacks. It can be used to detect attacks as well as deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate, getting logs of their operations. The basic principle behind them is simple i.e. to prepare something (honeypot) that would attract the attacker's interest and then wait for the attackers to show up.

Security expert John Strand and his team developed the Active Directory Active Defense (ADAD) security initiative using tools from his Active Defense Harbinger Distribution (ADHD).

The following are the three main attributes/mechanisms for active defense:

• Deception – The idea behind cyber deception follows the tactic of planting misinformation to deceive the attacker and take their focus away from the original target. Traps in the network, endpoints, and servers can be set up to reveal attackers or malicious insiders without them even knowing.

• Attribution – This is the process of tracking, identifying and laying blame on the perpetrator of a cyberattack or attempting a hacking exploit.

• Counterattack – This is considered to be the most efficient means of forcing the attacker to abandon offensive plans. Cyber counter attacks are sometimes used as a means of self-defense to slow down or even stop cyber attacks

An indicator of compromise (IoC) shows that there is an artifact or series of artifacts discovered on an endpoint indicating a breach with high confidence. IOCs artifacts enable information security professionals to detect intrusion attempts or other malicious activities.

An elite team can find things your automated response systems may miss. It can learn from incidents that have taken place, aggregating crowdsourced data, and providing response guidance when malicious activity is discovered. Having expert hunters working 24/7 on your behalf matches the ingenuity of determined attackers like no automated technology can.

An Indicator of Attack (IoA) is a unique construction of unknown attributes that are leveraged for a proactive approach to security. An IoA can consist of:

• Stealth behavior

• Persistence

• Code execution

• Command and Control

• Lateral movement

Indicators of Compromise (IOCs) are remnants, artifacts, and traces of a breach or attack on a system, network, application, or hosts. They can be precursors of a fully successful attack with all phases not being activated yet. Some practitioners call these indicators cyber observables or malware observances.

ATTACKS

Attribution as an active defense methodology that determines data about an attacker and their goals and targets. It is a valuable activity for incident response team members although it may be ineffective since source addresses are likely spoofed.

The attack back strategy involves information gathering, seek and disrupt, and seek and destroy actions yet is the most dangerous for the counter-attacker.

Pivoting is a technique of using an instance (aka 'plant' or 'foothold') to be moved around inside of a network. It leverages the first compromise to assist in vertical or horizontal (N/S or E/W) movement to aid in the compromise of other otherwise unreachable systems.

Cryptojacking is the unauthorized use of a personal device by cybercriminals to mine for cryptocurrency. Users can click on a malicious link in an email that loads cryptomining code on the computer or cloud based workloads. This is a common attack towards cloud platforms (public or private).

Many attackers use botnets to launch DDoS attacks.

ATTACKS (cont)

A botnet is a collection of compromised machines that the attacker can manipulate from a command and control (C2 or CnC) system to participate in a DDoS, send spam emails, and perform other illicit activities. Figure 4-3 shows how a botnet is used by an attacker to launch a DDoS attack. The figure illustrates, the attacker sending instructions to the C2 server; subsequently, the command and control server sending instructions to the bots within the botnet to launch the DDoS attack against the victim..

CRIPTOGRAFIA

Transport Layer Security (TLS) is a protocol that provides authentication, privacy, and data integrity between two Internet applications. It is the most widely deployed security protocol used today and is used for web browsers and other applications that require data to be securely exchanged over a network. TLS evolved from Netscape's Secure Sockets Layer (SSL) protocol and has superseded it for the most part.
Monitoring the file size assumes that a malicious version of an application would have a different file size than the original. However, attackers can also change the size of any given file. It is better to use attributes such as digital signatures and cryptographic hashes e.g. Message Digest algorithm 5 (MD5) or Secure Hash Algorithm 1 (SHA).
Key stretching attempts to make passwords based on one-way hashes much harder to compromise. It uses a key derivation process combined with a specialized function such as PBKDF2, bcrypt, or scrypt.
RSA is one of the original public-key cryptosystems and is still commonly used for secure data transmission. The acronym RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who published the algorithm in 1977.
With forward secrecy every TLS connection to the web server is individually protected. One of the biggest flaws of RSA is that it does not natively provide forward secrecy for TLS.
Technically speaking, a hash collision is a situation when the resultant hashes for two or more data input elements in a data set map to the same location in the hash table. A trustworthy hash function must be highly collision resistant. This is a known vulnerability of MD5.
Asymmetric encryption (also known as public key cryptography) uses two unique keys, a public key and a private key. The data is encrypted with the public key and only the matching private key can decrypt it. The private key is kept secret, whereas the public key can be given to anyone.
Message Digest 5 (MD5) algorithm is an example of a cryptographic hash function. The result of the hash is a fixed-length small string of data and is sometimes referred to as the digest, message digest, or simply the hash. Most software vendors publish the MD5 hash of the software package. This way the receiver of the software can run the same hash against the software and compare the results against the results the vendor published. If the hash generated matches the hash that was published, the software is intact from an integrity perspective.. Digital signatures are based on public key cryptography (asymmetric cryptography). The most common is RSA and provides integrity, origin authentication, and non-repudiation of transactions. To achieve confidentiality however, the digitally signed entity should be sent over a TLS or IPsec secure communication channel (essentially an encrypted transmission medium).
IPsec is an end-to-end security technology that allows two (or more) devices to communicate securely over a possibly unsecure medium. While the transport mode encrypts the data that is sent between peers, the tunnel mode encapsulates the entire packet and adds a new IP header.
TLS, SSL, and IPsec are various methods and protocols that can be used to protect data in transit. These protocols and secure data traversal mechanisms allow data payload and headers to be encrypted in such a way that an attacker cannot snoop into the data midway between sender and receiver. TLS is an improved version of SSL.
Transport Layer Security (TLS) is arguably the most important protocol for global communication and one of the most secure key exchange mechanisms that two parties can use is Elliptic Curve Diffie-Hellman Ephemeral.

CERTIFICATE

The following information is found in a typical X.509 certificate:
• Serial Number: Used to uniquely identify the certificate
• Subject: The person, or entity identified
• Signature Algorithm: The algorithm used to create the signature
• Signature: The actual signature to verify that it came from the issuer
• Issuer: The entity that verified the information and issued the certificate
• Valid-From: The date the certificate is first valid from
• Valid-To: The expiration date
• Key-Usage: Purpose of the public key, for example, certificate signing
• Public Key: The key used to encrypt information (The private key is kept secret as it is used to decrypt information, and once made public or leaked, the key-pair is unsafe to use.)
• Thumbprint Algorithm: The algorithm used to hash the public key certificate
• Thumbprint: The hash itself, used as an abbreviated form of the public key certificate
The CA follows one of these validation processes: Domain Validated (DV), which is the most common, Organization Validated (OV), and Extended Validation (EV) which shows the green padlock. Upon validation, the CA issues the certificate and all intermediary certificates needed to chain to its root.

FALSO POSITIVO

True positives: The security control, such as an IPS sensor, acted as a consequence of malicious activity. This represents normal and optimal operation. True negatives: The security control has not acted, because there was no malicious activity. This represents normal and optimal operation. False positives: The security control acted as a consequence of non-malicious activity. This represents an error, generally caused by too tight of proactive controls. False negatives: The security control has not acted, even though there was malicious activity. This represents an error, generally caused by too relaxed proactive controls (which permit more than just minimal legitimate traffic) or too specific reactive controls.. False negatives is the term used to describe a network intrusion device's inability to detect true security events under certain circumstances—in other words, a malicious activity that is not detected by the security device. The broad term false positive describes a situation in which a security device triggers an alarm, but no malicious activity or actual attack is taking place. In other words, false positives are false alarms.

POLICIES

An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet. Many businesses and educational facilities require that employees or students sign an acceptable use policy before being granted network access.

Guidelines are recommendations to users when specific standards do not apply. They are designed to streamline certain processes according to established best practices. Policies on the other hand are mandatory processes.

Policies must be followed whereas guidelines are recommendations that may be followed.

A written information security policy is the keystone of an Information Security Program. The policy should mirror the organization's mission, goals, and objectives based on how executive management positions and prioritizes security.

SCANNER

Some examples of popular vulnerability scanners include the following:

- Nessus from Tenable
- Retina from Beyond Trust
- Nexpose from Rapid7
- AppScan from IBM
- Nmap
- SAINT

IPV4 X IPV6

The IP header is a total of 32 bits. The version field is 4 bits. The version field is the first header field in an IP packet.

Time-to-live (TTL) - designates the number of hops a packet can take before it reaches its destination - is a value in an Internet Protocol (IP) datagram that tells a network router whether or not the packet has been in the network too long and should be discarded. In IPv6 the TTL field in each packet has been renamed the hop limit.

IPv4 Address Resolution Protocol (ARP) was replaced by the ICMPv6 Neighbor Discovery Protocol (NDP) in IP version 6. One of the functions of the IPv6 NDP is to resolve network layer (IP) addresses to link layer (for example, Ethernet) addresses. The Secure Neighbor Discovery (SEND) Protocol prevents an attacker who has access to the broadcast segment from abusing NDP or ARP to trick hosts into sending the attacker traffic destined for someone else, a technique known as ARP poisoning.

ARP (Address Resolution Protocol) converts an internet protocol (IP) address to its corresponding physical network address. IP networks, including those that run on Ethernet and Wi-Fi, require ARP to function properly.

Fragmentation is used to break up a datagram into smaller packets for a neighbor router that supports a smaller max transmission unit (MTU). This is accomplished using fields in the IP header.

The Traffic Class field indicates class or priority of IPv6 packet which is similar to Service Field in IPv4 packet. It helps routers to handle the traffic based on priority of the packet. If congestion occurs on router then packets with least priority will be discarded. As of now only 4-bits are being used (and remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.

Encapsulating Security Payload EH is similar in format and use to the IPv4 ESP header defined in RFC2406. All information following the Encapsulating Security Header (ESH) is encrypted and for that reason, it is inaccessible to intermediary network devices. The ESH can be followed by an additional Destination Options EH and the upper layer datagram.

TCP

TCP (Transmission Control Protocol) is a layer 4 protocol. TCP works with the Internet Protocol (IP) at layer 4 of the OSI model. It is connection-oriented, ordered and should be used if your service needs a reliable transmission of datagrams. TCP is meant to provide error-free data transmission as it handles retransmission of dropped or garbled packets and acknowledges all packets that arrive. TCP provides multiplexing, demultiplexing, and error detection. TCP is connection-oriented because before one application process can begin to send data to another, the two must first establish a "handshake" with each other. UDP is connectionless, TTL is Time To Live – it is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Real-Time Protocol (RTP) is based on UDP and is connectionless as it is used for transmission of real time voice and/or video packets.. TCP (Transmission Control Protocol) is a layer 4 protocol and a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP) at layer 4 of the OSI model. It is connection-oriented, ordered and should be used if your service needs a reliable transmission of datagrams. TCP is meant to provide error-free data transmission as it handles retransmission of dropped or garbled packets and acknowledges all packets that arrive..

PACKET ANALYZERS

Wireshark and tcpdump are both examples of packet analyzers. Wireshark is a GUI-based free and open source packet analyzer. tcpdump is a CLI-based packet analyzer and is also free and open source (distributed under a BSD license). tcpdump, runs on Linux and Mac OS X systems. Tcpdump, written in C, is a data-network packet analyzer computer program that runs under a command line interface. It allows the user display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

RISK ASSESSMENT

ISO 31000:2009 involves risk management principles and guidelines. It offers principles, a framework, and a process for managing risk. It can be used by any organization regardless of its size, activity, or sector. The first phase will be to ascertain the purpose, context, and scope of the risk assessment and management program.

Vulnerability Management begins with assessment and prioritization of assets so that you can better determine the Return on Security Investment (ROSI). The next step is to start building the risk register (log or ledger) based on semi-quantitative or quantitative approach if one does not already exist.

Risk assessment can be done in two possible ways: quantitative and qualitative. Quantitative risk assessment involves dollar values and mathematical formulas and aims to determine tangible values. Qualitative risk assessment uses questioners and/or interviews.

The acronym RACI is as follows:

1. responsible,
2. accountable,
3. consulted, and

RISK ASSESSMENT (cont)

4. informed.
It is used for clarifying and defining roles and responsibilities typically in cross-functional projects and/or processes.
The term "risk transfer" is often used in place of risk sharing, although in practice the transfer of risk to an insurance or outsourcing company may result in loss if the company goes out of business.
Annualized Loss Expectancy (ALE) = Single Loss Expectancy ? Annualized Rate of Occurrence in classic quantitative analysis
An incident is an established negative occurrence that affects the state of data, network, application, or system. An incident can cause damage or loss, either directly (primary) or indirectly (secondary). All incidents are made up of events, but not all events are categorized as incidents.

Resposta à incidentes

Incident response lifecycle consists of six phases:
1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned
Business Continuity Planning (BCP) consists of Business Impact Analysis (BIA), Backups and Restoration, and Disaster Recovery Planning (DRP). The BIA is a key step in implementing the Continuity Planning controls in NIST SP 800 53 and in the contingency planning process overall.
Two of the important parameters that define a Business Continuity Disaster Recovery (BCDR) plan are the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These are defined as follows:
• RPO is the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan’s maximum allowable threshold or tolerance.
• RTO is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
•
Recovery time objective (RTO) is the maximum required amount of time allowed between an unforeseen failure or disaster and the resumption of regular operations and service levels. The RTO describes the point in time after a failure or disaster at which the consequences of the interruption become unacceptable. Recovery Time Objective (RPO) is the target time you set for the recovery of your IT and business activities after a disaster has struck. The goal here is to calculate how quickly you need to recover, which can then dictate the type or preparations you need to implement and the overall budget you should assign to business continuity.. A cold site is the least expensive disaster recovery option as there is practically nothing at the site except for electricity, HVAC, and utilities. It may have ethernet cable installed or may rely on a wireless network installation.

BACKUP

Incremental backups begin with a full backup. But once that initial full backup is taken, incremental backups only copy the parts of files that have changed since the previous backup. Once the incremental backup has run, it won't back up that file again until the next full backup, unless the file changes.
A differential backup is a data backup that copies all of the files that have changed since the last full backup was performed. This includes any data that has been created, updated or altered in any way and does not copy all of the data every time. The term differential backup is based on the concept that only data that is "different" is copied. An incremental backup is a backup type that only copies data that has been changed or created since the previous backup activity was conducted.
Snapshots and traditional backups essentially have a similar role. They both make copies of the data on your system which you can later restore. The first snapshot is a precise copy of the given virtual machine or data volume. Ensuing snapshots store data blocks (usually as object/blob storage) that have been changed or added in the meantime. It can perform versioning and fallback activities much faster than traditional backups.

WINDOWS

When deploying a Windows Server Update Services (WSUS) implementation, it is important to realize that a single server can handle more than 10,000 client systems.
A Windows network operating system domain controller is a server that handles network security, effectively functioning as the gatekeeper for user authentication and authorization. Domain controllers are especially important in Microsoft directory services terminology, and function as the primary mode for authenticating Windows user identities.
In order to have a domain implemented, you will need to configure a domain controller to centrally authenticate users who wants to connect and provides them the resources that they need. The domain controllers are also essential in adding an extra layer of security for the system beyond the normal usual security from individual computers in workgroups.
The user employs Remote Desktop Protocol (RDP) client software for this purpose, while the other computer must run RDP server software. This service should be disabled if not absolutely necessary as part of system hardening.
There are three Servicing Channels in Windows:
1. Semi Annual
2. Windows Insider, and
3. The Long-Term Channel.
Home edition users can defer quality (not feature) updates for up to 35 days.
According to Microsoft, BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline. Microsoft offers BitLocker as a built-in encryption with Windows OS.
BitLocker uses the Advanced Encryption Standard (AES) for protecting data at rest. BitLocker uses (AES) as its encryption algorithm with configurable key lengths of 128 or 256 bits. The default encryption setting is AES-128, but the options are configurable by using Group Policy.
The AGULP model goes as follows: Accounts > Global Groups > Universal Groups > Local Groups > Permissions and Rights.
The shared folder is made possible by the File and Print Sharing service and the SMB protocol. Share permissions are Full Control, Change, and Read.
The Registry Key structure (registry hive) is similar to folders. A single folder stores all the information and data related to that folder. In a Registry Key, the highest-level folder is a Hive (or Registry Hive). Also, if you further classify any information then you create sub-folders. The sub-folder in Windows Registry Key is classified as a Key and any folder under a sub-folder is called a Sub Key. The following figure gives an insight to the Windows Registry Hive.
Windows AppLocker is applicable to Windows 10 and Windows Server only. AppLocker helps reduce administrative overhead and helps reduce the organization's cost of managing computing resources by decreasing the number of Help Desk calls that result from users running unapproved apps.

WINDOWS (cont)

According to Microsoft, User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

Group Policy and Group Policy Objects is the strategy for centralized administration but works only in conjunction with Active Directory. Administrators can manage Group Policy using the Group Policy Management Console (GPMC).

Azure PowerShell modules can be installed by using PowerShellGet on Windows, macOS, and Linux platforms. PowerShell 7.x and later are the recommended versions of PowerShell for use with Azure PowerShell on all platforms.

According to Microsoft, PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. PowerShell is built on top of the .NET Common Language Runtime (CLR) and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation.

Windows Event Viewer displays the Windows event logs. This is the default application to view and navigate the logs, search and filter particular types of logs, export logs for analysis, and much more.

SOFTWARE COMPOSITION ANALYSIS

Before applying a security template using the SCA tool, you should always perform a full backup that includes the System State. There is no feature to revert back to a previous state or “undo” after applying the template.

Since there is no fallback or undo feature in the SCA tool, you should make a backup of the production server that includes the system state.

LINUX

You should always set the sticky bit on these directories so that only the owner can removed his own files, with the exception of the owner of the sticky bit directory (and the root user), who can delete all of the files in the directory. These directories are intended for storing temporary files that may be made by anyone.

You can add a new user in Linux using the command:

$ sudo useradd username

To maintain a record of which files belong to which user and to enforce some security, Linux uses the concept of ownership. Every file belongs to an owner—a user—and to a group. On Unix-like operating systems, the chown command changes ownership of files and directories in a filesystem.

The /dev directory holds device drivers; /usr is the primary read-only directory; /var contains log files, queues, and more; and /home has user home directories.

Bash is a Unix shell and command language written by Brian Fox for the GNU Project as a free software replacement for the Bourne shell. First released in 1989, it has been used as the default login shell for most Linux distributions and all releases of Apple's macOS prior to macOS Catalina.

Linux (and flavors of Unix) have following shells to offer:

• The Bourne Shell (sh): Developed at AT&T Bell Labs by Steve Bourne, the Bourne shell is regarded as the first UNIX shell ever. It is denoted as sh. It gained popularity due to its compact nature and high speeds of operation.

• The GNU Bourne-Again Shell (bash): More popularly known as the Bash shell, the GNU Bourne-Again shell was designed to be compatible with the Bourne shell.

• The C Shell (csh): The C shell was created at the University of California by Bill Joy. It is denoted as csh.

• The Korn Shell (ksh): The Korn shell was developed at AT&T Bell Labs by David Korn, to improve the Bourne shell. It is denoted as ksh.

LINUX (cont)

• The Z Shell (zsh): The Z Shell or zsh is a sh shell extension that has all the features and more.
•
These are the traditional init runlevels:
• 0 - Halt the system,
• 1 - Single-user mode (for special administration),
• 2 - Local Multiuser with Networking but without network service (like NFS),
• 3 - Full Multiuser with Networking,
• 4 - Not Used,
• 5 - Full Multiuser with Networking and X Windows(GUI),
• 6 - Reboot.
iptables is an extremely flexible firewall utility built for Linux operating systems. iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on your system, iptables looks for a rule in its list to match it to. iptables almost always comes pre-installed on any Linux distribution and to update or install it, you can just retrieve the iptables package using the command: sudo apt-get install iptables
SELinux was first introduced in CentOS 4 and significantly enhanced in later CentOS releases. SELinux follows the model of least-privilege more closely. By default under a strict enforcing setting, everything is denied and then a series of exceptions policies are written that give each element of the system (a service, program or user) only the access required to function. SELinux has three basic modes of operation as follows:
1. Enforcing
2. Permissive
3. Disabled
Bastille is a hardening program that locks down a Linux, HP-UX, and MacOS operating system, proactively configuring the system for enhanced security and decreasing its susceptibility to compromisse. Bastille can also assess a system's current state of hardening and generate a granular report on each of the security settings with which it works.
The recommended method to perform this hardening feature is to edit the /etc/sysctrl.conf file. Remember this fact for the exam as well as setting this to prevent source routing and two-way spoofed communications.
Trusted Platform Module (TPM) offers hardware-based, security-related functions in the form of a secure crypto-processor chip that performs cryptographic operations. The chip includes several physical security mechanisms to make it tamper resistant, and malicious software is unable to tamper with the security functions of the TPM.
Ansible is an open-source automation tool, or platform, used for IT tasks such as configuration management, application deployment, intra--service orchestration, and provisioning.
Auditd is an access monitoring and accounting for Linux developed and maintained by RedHat. It was designed to integrate tightly with the kernel and look for interesting system calls. Also, likely because of this level of integration and detail, it is the default logger in SELinux.
Each Syslog message Priority also has a decimal Severity level indicator. Severity values MUST be in the range of 0 to 7 inclusive. Debug has the highest number 7, representing the lowest priority level.
Linux builds have a native stateful firewall called iptables. Append this rule to the input chain (-A INPUT) to view ingress traffic; look for TCP (-p tcp); if so, does it go to the destination SSH port (-dport ssh)? If yes, then permit the traffic (-j ACCEPT).

NTFS

Every NTFS (NT file system) file or folder has an owner assigned to it. As part of the discretionary access model (DACL), If a user is the owner of an object the only recourse for the administrator is to take ownership away from the user. Other objects include printers, AD containers, registry keys, processes, and threads.
It is vital to understand that NTFS (NT file system) permissions are always enforced, regardless of how the files are being accessed.
What happens if there is a conflict between an NTFS deny permission and an Allow permission when applied to a file? The user's final effective permission on the file will be deny since that always takes precedence.

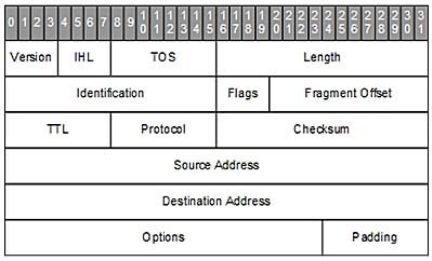
FORENSIC

A write-blocking is a tool is designed to avoid any write access to a hard disk when performing forensic investigations. It allows read-only access to a data storage device without compromising the integrity of the data. If used properly, it can deliver a high degree of confidence in the protection of the chain of custody.

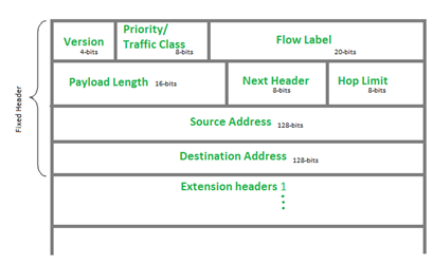
DNS

Domain Name System (DNS) uses TCP port 53 for connection-oriented tasks such as database replication and UDP port 53 for unreliable activities like queries to DNS servers.

IPV4 HEADER



IPV6 HEADER



PENTEST

White box penetration testing takes into account scenarios where almost all information is available to execute an attack. More often this type of pen testing produces very focused results. Black box approach is the opposite of white box, and the pen tester does not have any information about the system they are trying to breach. This is more accurate in simulating an external attack. Gray box, on the other hand, is halfway between a white box and a black box approach. In this approach, the pen tester has some information available, but not all..

NIST

The five key aspects of NIST Cyber Security Framework are:
1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

The five steps of the NIST Enterprise Security Architecture (ESA) are identify > protect > detect > respond > recover. Other activities of the “protect” phase are awareness training and information protection and procedures.

According to NIST, security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. Examples of operational controls would be configuration management, incident response, and system integrity.

Examples of deterrent controls would be signage, bollards, banners, guards, dogs, lighting, and visible video surveillance.

According to NIST Special Publication 800-61, a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An employee knowingly crashing the e-commerce server is an example of a computer security incident. The security administrator changing the permissions of a directory and an employee accessing a file do not relate to an incident. The intruder breaking into office premises does constitute a security incident, just not a computer security incident..

TCP

Assume Device A has completed its transmission and indicates this by sending a segment to Device B with the FIN bit set to 1. Device B will acknowledge the segment with an ACK. At this point in time, Device B will no longer accept data from Device A. Device B can continue to accept data from its application to transmit to Device A. If Device B does not have any more data to transmit, it will also terminate the connection by transmitting a segment to Device A with the FIN bit set to 1. Device A will then ACK that segment and terminates the connection..

CIA TRIAD

Confidentiality, Integrity, and Availability (also known as the CIA triad) are the cornerstones of Information Security. This is a model created to define security policies for organizations and it has everything to do with secure storage, transmission, retrieval, execution, and any action dealing with security of information.
The Parkerian hexad is a group of six information security elements offered by Donn B. Parker in 1998. The hexad adds three additional attributes to the three classic security attributes of the CIA triad (confidentiality, integrity, availability). These elements are utility, authenticity, and possession (control).
Digital signatures provide peer authentication, integrity, and non-repudiation. They do not offer confidentiality services or availability between peers.
In the world of information security, integrity protects against unauthorized changes to data. Integrity can be implemented using various tools and mechanisms, for example, hashing algorithms.
The least privilege principle involves granting just the right amount of access to data, applications, and systems that are necessary for the job role and no more.

THREAT

Threat enumeration is defined as a process which establishes an active connection to the target hosts to discover potential attack vectors in the system, and the same can be used for further exploitation of the system. Enumeration is often considered as a critical phase in Penetration testing as the outcome of enumeration can be used directly for exploiting the system.
Enumeration is defined as a process that establishes an active connection to the target hosts to discover potential attack vectors in the system. Enumeration can be used for further exploitation of the system. Enumeration is used to gather: Usernames, group names, Hostnames, Network shares and services, IP tables and routing tables, SNMP and DNS details.

ACCESS CONTROLS

A mandatory access control (MAC) model, such a Bell-LaPadula and Biba, is a system of access control that assigns security labels or classifications to system resources and allows access only to principals with distinct levels of authorization or clearance. Mandatory Access Control (MAC) requires allocation of labels to provide resource access. The labels are, for example, Public, Confidential, Secret, and so on. The labels can be managed at organizational level.
When the owner of a file makes the decisions about who has rights or access privileges to it, the owner is using discretionary access control or DAC. The Nondiscretionary access control on the other hand has a fixed set of rules that exist to manage access.

FIREWALL/SIEM

A next generation firewall (NGFW) provides capabilities beyond that of a stateful network firewall. A stateful firewall is a network security device that filters incoming and outgoing network traffic based upon Internet Protocol (IP) port and IP addresses. By intelligently inspecting the payload of some packets, new connection requests can be associated with existing legitimate connections. An NGFW adds additional features such as application control, integrated intrusion prevention (IPS) and often more advanced threat prevention capabilities like sandboxing.. A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Ideally, a firewall should be placed at critical junctures in a network to provide segmentation between trusted and untrusted services or user access. Firewalls have been an integral part of security industry over the past 25 years.

A firewall is a software or hardware device that work as a filtration system for the data attempting to enter your computer or network. A firewall monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls are typically used to segment network to filter traffic from unsecure (untrusted) to secure (trusted) zones and vice-versa.

The intrusion prevention service (IPS) sensor is an inline, proactive, and preventative security control that can prevent the malicious payload from being delivered to the target. The IDS will take actions based on copies of the frame and is reactive.

A signature-based HIDS system is dependent entirely on availability (and timely updating) of signatures as it can only detect attacks that correspond to attack signatures present in its signature database. Hence, a signature-based HIDS system wouldn’t be able to appropriately identify any zero-day attacks.

Anomaly-based detection is form of intrusion detection that relies upon observing network occurrences and discerning anomalous traffic through heuristics and statistics measured against an established baseline of normal operations.

Endpoint Detection and Response (EDR) are tools that are mainly dedicated to detection and investigation of suspicious activities and indicators of compromise (IoCs) on hosts/endpoints. McAfee, Norton, and CrowdStrike are examples of EDR solutions.

A multi-phased logging analysis methodology would be Phase 1: Log Collection using tools like Kiwi and syslog ng; Phase 2: Log Storage using databases such as MySQL and PostgreSQL; Phase 3: Log Analysis using Splunk, grep, or LogParser; and Phase 4: Log Correlation and Alerting with tools like OSSEC (Open Source HIDS SECurity) and OSSIM (Open Source SIEM).

All given examples are Security Information and Event Management (SIEM) solutions. A SIEM solution receives data from different sources, including IPS devices, firewalls, NetFlow generating devices, servers, endpoints, and syslogs from infrastructure devices. It provides a central view of logging and related security activities across network.

SIEM has evolved from separate security event and security information monitoring. It is the primary centralized log correlation, aggregation, and normalization solution used in modern enterprises today. Common solutions would be SolarWinds Security Event Manager, ManageEngine EventLog, and Azure Sentinel.

Following are the most commonly used network security logging platforms:

• Kiwi Syslog – SolarWinds Kiwi Syslog Server is a syslog management tool. It can receive syslog messages and SNMP traps from network devices (routers, switches, firewalls, etc.), and Linux/Unix hosts

• syslog-ng – It is a free and open-source implementation of the syslog protocol for Unix and Unix-like systems

Syslog messages include time stamps, event messages, severity levels (0-7), host IP addresses, and diagnostics.

When using a SIEM system the Never Before Seen (NBS) analytics reporting is critical for identifying mew threats against systems.