CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 4
Security Architectures

Identity and Access Management

Chapter 12

Outline

- Security Issues Associated with Context-Based Authentication
- Security Issues Associated with Identities
- Security Issues Associated with Identity Repositories
- Security Issues Associated with Federation and Single Sign-On
- Exploits
- Quiz

Security Issues Associated with Context-Based Authentication

- **Security Issues Associated with Context-Based Authentication**
  - **Aims to improve both security and usability by giving context to login events**
    - **Example: a user may only have to input a dual factor authentication code if they sign in from a new device.**
      - **Gives some of the security benefits of 2 factor but users are able to log in quickly from their normal devices**
  - **For each parameter at least 2 events must occur**
    - **Catalog user information**
    - **Comparing and validating user data to accepted logins**
  - **Process must be fast and at the same time minimize the number of false positives and false negatives.**

Security Issues Associated with Context-Based Authentication

- **Time**
  - **Sometimes it makes sense that a user will only have access to certain systems at certain times, such as during business hours**
  - **Time should be closely tied to location when considering authentication in the following:**
    - **Time zones may mean that a travelling employee may be working when the rest of the company is not**
    - **Login attempts from distant locations at similar times should be treated as suspicious**
  - **Dual factor authentication often uses time in the form of a code that changes over time**

Security Issues Associated with Context-Based Authentication

- **Location**
  - **Often used to secure data by limiting login attempts to known and secure locations**
  - **Falls into two categories**
    - **Network Based Location**
      - **Uses the IP address to determine the location of the user/attacker attempting to login**
      - **Vulnerable to spoofed IP addresses**
    - **Device Based Location**
      - **Uses GPS or cell towers to determine the location of the device being used to login**
      - **Apps on "Jailbroken" or "rooted" devices can manipulate the location data on the device and make it appear to be wherever an attacker desires**

Security Issues Associated with Context-Based Authentication

- **Frequency**
  - **Since computers can operate much faster than humans it is often easy to tell when a computer is performing functions that should be done by a human**
    - **Login attempts that are coming too fast to possibly be done by a human are a red flag**

Security Issues Associated with Context-Based Authentication

- **Behavioral**
  - **Used after the login**
  - **Known as “active authentication”**
  - **This method learns the behavior of users and uses their distinctive method of interacting with the computer as a “digital fingerprint” to ensure that the same user is still in control of the session**

Interactive Exercise: 1

What are four ways that Context-Based Authentication is used?	
Which Context-Based Authentication watches to see if certain functions are being performed by a computer or a person?	
How does the Behavioral Context-Based Authentication method work?	
What does Context-Based Authentication Aim to improve?	

Interactive Exercise Answer: 1

What are four ways that Context-Based Authentication is used?	- Time - Behavior - Location - Frequency
Which Context-Based Authentication watches to see if certain functions are being performed by a computer or a person?	Frequency is what is used to measure this. Humans cannot input, interpret, and iterate anywhere near the speed that a machine can. It is obvious when a machine is performing actions that a human should be doing.
How does the Behavioral Context-Based Authentication method work?	Learns the behavior of users and uses their distinctive method of interacting with the computer as a "digital fingerprint" to ensure that the same user is still in control.
What does Context-Based Authentication Aim to improve?	Aims to improve both security and usability by giving context to login events. For example, a user may only have to input a dual factor authentication code if they sign in from a new device.

Security Issues Associated with Identities

- **Security Issues Associated with Identities**
  - **A digital identity is a distinct representation of a real-world subject within a digital environment**
    - **One individual will have many digital identities because they are on many different systems e.g. work, Twitter, Facebook… etc.**
  - **Authenticating identities requires complex mechanisms that may be exploited.**
  - **Identity Management (IDM) becomes ever more important as companies become more decentralized.**
  - **Cloud based systems allow users to access systems from any location but makes the process of IDM even more challenging**

Security Issues Associated with Identities

- **Personnel**
  - **People are the most important part of any business but are also the greatest weakness in security**
  - **A IDM solution must be able to gather the necessary information to quickly determine a person's identity**
  - **Human error accounts for the majority of cases of unauthorized access**
    - **Phishing scams**
    - **Sharing passwords**
    - **Losing devices**
  - **Training users on best practices in securing their credentials is one of the most important factors in keeping a system secure**

Security Issues Associated with Identities

- **Endpoints**
  - **Endpoint authentication, also known as device authentication, must allow endpoints to quickly verify that the device it is communicating with is who it says it is**
  - **Common methods of endpoint verification include keys or tokens generated by the endpoint and presented to the network**
  - **Endpoints are at high risk for abuse regarding authentication because it is easy to spoof or replay endpoint data**

Security Issues Associated with Identities

- **Servers**
  - **Servers often use public key certificates defined by the S.509 standard. These certificates are issued by a trusted Certificate Authority (CA) which is required to verify the identity of the requesting organization**
    - **The process makes it difficult for an impostor to be issued a certificate though it is possible for a certificate to be stolen**
    - **If an attacker inserts themselves into the chain and presents a fake certificate browsers will warn the user but the user may ignore the warning**
    - **This method only verifies the server and not the user**

Security Issues Associated with Identities

- **Mutual verification such as Kerberos is often a better choice than certificates**
  - **The Kerberos authentication protocol which is found in nearly all operating systems has three components**

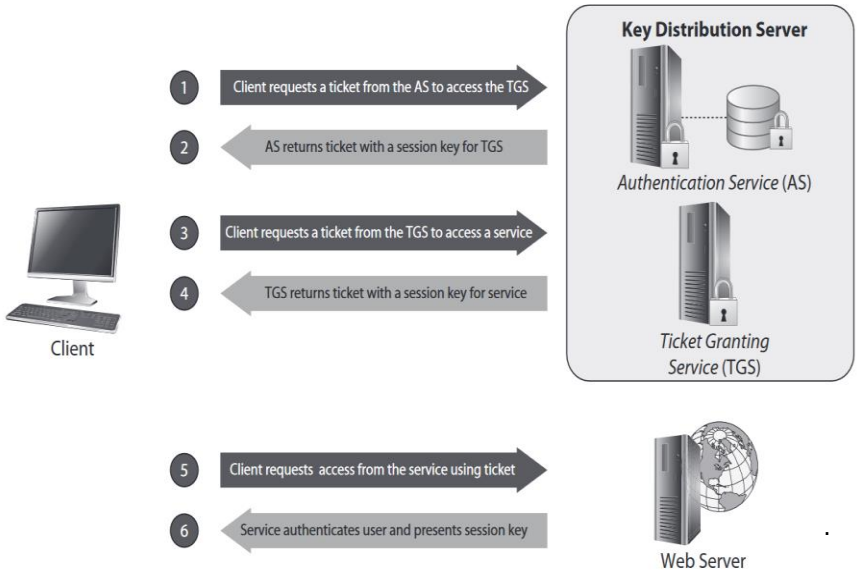


Figure 12-1 Relationship between the three "heads" of the Kerberos protocol

- **Authentication Service (AS)**
  - » **used to verify client identity**
- **Ticket Granting Server (TGS)**
  - » **distributes tickets to verified clients**
- **Key Distribution Center (KDC)**
  - » **controls the use of keys in a system; AS and TGS are housed within this system**

Security Issues Associated with Identities

- **Kerberos Authentication**
  - Client requests services, in plaintext, on behalf of user
  - AS verifies client and generates a secret key (K_{cAS}) by hashing user's password; sends back two messages
    - » Message A: encrypted client/TGS session key (K_{cT})
      AS→ Client: $\{K_{cT}\}K_{cAS}$
    - » Message B: Ticket-Granting-Ticket (TGT, includes the client ID, client network address, ticket validity period(P), and K_{cT}) encrypted using the secret key of TGS (symmetric key with AS and TGS, K_{AST})
      AS→ Client: $\{clientName, clientNA, P, K_{cT}\}K_{AST}$
  - Assuming user has entered correct password, the client will decrypt message A

Security Issues Associated with Identities

- **Kerberos Authorization**
  - Client sends two messages to TGS:
    - » Message C: message B along with a requested service ID
      Client → TGS: $\{clientName, clientNA, P, K_{cT}\}K_{AST}$
    - » Message D: Authenticator (client ID and timestamp(T)), encrypted with session key established in message A
      Client → TGS: $\{clientName, T, servID\}K_{cT}$
  - TGS decrypts message B, getting K_{cT} and the client ID; uses K_{cT} to decrypt authenticator and compares client ID from message B and D; if they match, server sends two messages to client:
    - » Message E: Client-to-server ticket (client ID, client network address, validity period, and Client/Server Session Key (K_{cs})) encrypted using the service's secret key (symmetrical key with TGS and server(K_{Ts}))
      TGS → Client: $\{clientName, clientNA, P, K_{cs}\}K_{Ts}$
    - » Message F: K_{cs} encrypted with K_{cT}
      TGS→ Client: $\{K_{cs}\}K_{cT}$

Security Issues Associated with Identities

- **Kerberos Service Request**
  - The client has enough information to authenticate itself to the Service Server (SS). The client connects to the SS and sends the following two messages:
    - » Message E: the client-to-server ticket, encrypted using TGS's secret key with server
      Client → SS: $\{clientName, clientNA, P, K_{cs}\}K_{Ts}$
    - » Message G: a new Authenticator and is encrypted using Client/Server Session Key(K_{cs}))
      Client → SS: $\{clientName, T\}K_{cs}$
  - The SS decrypts the ticket (message E) using its secret key with TGS to retrieve K_{cs}; uses K_{cs} to decrypt authenticator and compares client ID from E and G; assuming a match, server sends a message to client to confirm identity and willingness to serve client:
    - » Message H: the timestamp in client's authenticator (T_c) plus 1, encrypted using K_{cs}
      SS → Client: $\{T_c+1\}K_{cs}$
  - The client decrypts the confirmation (message H) using K_{cs} and checks whether the timestamp is correct. If so, client can trust the server and can start issuing service requests; the server provides the requested services to client

Security Issues Associated with Identities

- **Kerberos has been in use for decades and is important to learn, but it does have some weaknesses**
  - **Since the KDC is critical to the integrity of the entire Kerberos system, failing to properly protect it from unauthorized access will expose the entire organization to significant risk**
  - **In order to be effective Kerberos must be supported by every node in the network**
  - **In order to properly authenticate all devices in a Kerberos system must have their clocks synchronized since timestamps are an important part of the authorization process**

Security Issues Associated with Identities

- **Services**
  - **Masquerading as services is an effective way to phish users into providing sensitive data and is very difficult to detect at a user level**
  - **Microsoft's .NET Framework has a feature called Service Identity and Authentication**
  - **The Windows Communication Foundation (WCF) ensures that the identity value of the requested service matches a preset value**

Security Issues Associated with Identities

- **Roles**
  - Permissions are often managed by the given roles of users where each role is given access to certain resources
  - Users may have access to resources that they are not even aware of
  - As the number of objects and users grows some users will be granted access to resources that they do not need to be able to access
  - Attackers will often attempt to determine which users have elevated permissions based off of their roles
  - Auditing roles is an important part of assessing permissions

Security Issues Associated with Identities

- **Applications**
  - **Web applications are accessible to the public and are therefore one of the easiest parts of a system to target**
  - **Software flaws in web applications can allow attackers to manipulate the input of an application to gain escalated privileges or access within the application or operating system**

Interactive Exercise: 2

What accounts for the majority of cases of unauthorized access?	
What is endpoint devices authentication vulnerable to?	
What are the three main components needed for Kerberos?	
How are services used to gain sensitive information about a company?	
In what way are web applications a security issue?	

Interactive Exercise Answer: 2

What accounts for the majority of cases of unauthorized access?	Human error is what accounts for the majority of unauthorized access . Examples - Phishing scams - Sharing passwords - Losing devices
What is endpoint devices authentication vulnerable to?	Endpoints are particularly vulnerable to abuse regarding authentication because it's easy to spoof or replay endpoint data.
What are the three main components needed for Kerberos?	- Authentication Service (AS) Used to verify client identity - Ticket Granting Server (TGS) Distributes tickets to verified clients - Key Distribution Center (KDC) Controls the use of keys in a system; AS and TGS are housed within this system
How are services used to gain sensitive information about a company?	They simulate a service to effectively phish users into providing sensitive data and is very difficult to detect at a user level.
In what way are web applications a security issue?	- Web applications are accessible to the public and are therefore one of the easiest parts of a system to target. - Software flaws in web applications can allow attackers to manipulate the input of an application to gain escalated privileges or access within the application or operating system.

Security Issues Associated with Identity Repositories

- **Security Issues Associated with Identity Repositories**
  - **An identity repository is any resource that stores the credentials necessary to validate a user's network access**
  - **Identity repositories are a rich target for attackers since modifying them can allow for adding or changing user attributes**

Security Issues Associated with Identity Repositories

- **Directory Services**
  - **A central repository for storing and managing information**
  - **Allows admins to provide management and security options at scale**
  - **Allows users to quickly locate network resources**
  - **Can store nearly any information about the network**
  - **Directory services need to be scalable and able to integrate well with various other services on the network.**

Security Issues Associated with Identity Repositories

- **Active Directory (AD)**
  - The directory service for Windows environments
  - AD allows organizations to centrally manage resources while providing network security policy
  - All systems, resources and services are considered objects with attributes associated with them
  - Many attackers will attempt to gain access to the AD domain controllers which would allow them complete control of all objects associated with the organization
  - 2 Types of defense plans are common for AD domain controllers
    - Using the principle of least privilege will make it more difficult for attackers to gain access to AD controllers
    - Enabling auditing functionality can allow for administrators to be aware of potential attacks by alerting them of attempts to access or change sensitive objects

Security Issues Associated with Identity Repositories

- **Lightweight Directory Access Protocol (LDAP)**
  - **LDAP provides a cross-platform open standard for maintaining directory services on a network**
  - **Users can query the LDAP server to get responses based on specifically formatted statements**
    - **Attackers may be able to format statements to provide information that is not normally authorized for the requester**
    - **It is possible that attackers may be able to get the LDAP server to execute arbitrary code**
    - **input sanitation is critical to prevent these abuses**

Security Issues Associated with Identity Repositories

- **Terminal Access Controller Access Control System Plus (TACACS+)**
  - **an authentication, authorization, and accounting (AAA) protocol that originated with Cisco in the 1990s that serves as an alternative to Kerberos**
  - **TACACS+ uses a client/server approach to determine a user's access level to anything on the network**
  - **At the time of the connection attempt, the user is compared against the user database, and the policy is then applied to that user**
  - **TACACS+ treats authentication, authorization, and accounting independently**

Security Issues Associated with Identity Repositories

- Utilizes TCP and encrypts both usernames and passwords during the authentication process
- TACACS+ was designed for device AAA but is commonly used for network AAA
- TACACS+ has several fundamental weaknesses
  - Most notably, TACACS+ is particularly vulnerable to replay attacks because every sequence number always starts with 1
  - TACACS+ sessions IDs are relatively short and the pool of IDs is small enough to be vulnerable to “birthday attacks”

Security Issues Associated with Identity Repositories

- **Remote Authentication Dial-In User Service (RADIUS)**
  - **An alternative AAA protocol to TACACS+ which uses UDP instead of TCP and encrypts only the passwords during authentication**
    - **The use of UDP instead of TCP means that reliability may suffer depending on network state**
      - **RADIUS is more vulnerable to forged packets because there is no confirmation of packet receipt**
      - **RADIUS allows for the use of "shared secret" across the network which means that a compromise anywhere can lead to the entire network becoming compromised more easily**
      - **RADIUS implementations may also be vulnerable to buffer overflow attacks which may lead to leaking of sensitive data or exploitation of arbitrary malicious code**

Interactive Exercise: 3

What are the two types of defence plans for Active Directory domain controllers?	
What are some of the functions of LDAP?	
What attacks is TACACS+ vulnerable to?	

Interactive Exercise Answer: 3

What are the two types of defence plans for Active Directory domain controllers?	- Using the principle of least privilege will make it more difficult for attackers to gain access to AD controllers - Enabling auditing functionality to allow administrators to be aware of potential attacks by alerting them of attempts to access or change sensitive objects
What are some of the functions of LDAP?	- LDAP provides a cross-platform open standard for maintaining directory services on a network - Users can query the LDAP server to get responses based on specifically formatted statements
What attacks is TACACS+ vulnerable to?	- TACACS+ is particularly vulnerable to replay attacks because every sequence number always starts with one. - TACACS+ sessions IDs are relatively short and the pool of IDs is small enough to be vulnerable to “birthday attacks”

Security Issues Associated with Federation and Single Sign-On

- **Federated Identity is the concept of using a digital identity to gain access to various services across multiple organization**
  - **Example: Google allows you to log in once and access all of Google's various services (YouTube, Gmail, Google Drive, etc.)**
  - **Federated Identity authorizations are often implemented with Single Sign-On (SSO)**
    - **SSO allows a user to access multiple systems with a single set of credentials which streamlines the user experience**
    - **SSO also eases the job of admins who have to answer fewer calls about password problems**

Security Issues Associated with Federation and Single Sign-On

- Security Assertion Markup Language (SAML) is widely used to implement SSO
  - SAML communicates between a identity provider (IDP) and a service provider (SP)
    - When a user requests access to a service, the SP requests identity verification from the IDP
    - If the identity is verified then the IDP returns a token to the SP (in lieu of actual credentials)
    - The SP then makes a decision on a user's access based on the response from the IDP
- SSO platforms require a stronger focus on protecting user credentials and so multi-factor authentication becomes especially valuable

Security Issues Associated with Federation and Single Sign-On

Security Issues Associated with Federation and Single Sign-On

- Since the SSO authentication system is necessarily centralized, that system becomes a critical asset and therefore a target
- If the SSO authentication system is disabled or compromised then access to all associated services will be lost

Security Issues Associated with Federation and Single Sign-On

- **Manual vs. Automatic Provisioning/Deprovisioning**
  - **Provisioning is the coordination of efforts behind creating user accounts on a service and setting the appropriate roles and access associated with them**
  - **Auto provisioning allows the IDP to assert that the user should be allowed to hold an account with the SP**
    - **Requires great trust in the IDP and often occurs within a single organization's services such as Google**
  - **Not carefully controlling and consolidating accounts leads to an unnecessarily large attack surface.**

Security Issues Associated with Federation and Single Sign-On

- **Self-Service Password Reset**
  - **A self-sustaining network seeks to remove the need for administrator intervention whenever possible and one-time consuming role of administrators is dealing with problems like password resetting**
    - **This may not be a problem for a small network but as it grows it becomes a heavy time sink**
  - **Allowing users to reset their own passwords is a common process but may provide an opportunity for attackers**

Exploits

- **Impersonation**
  - **An authentication service is always just a machine and can only tell the difference between people by the information it has**
- **Man in the middle (MITM)**
  - **A MITM attack is where an attacker impersonates both a service and a client**
  - **By impersonating both, the attacker is able to gather credentials or record the traffic between the server and user or they can introduce falsified communications**

Exploits

- **Session Hijack**
  - An attacker using a valid user's session information to impersonate that user
  - Done by stealing the session from the user, by replaying the information to the server, or by predicting the session token information
- **Cross-site scripting (XSS)**
  - Malicious code injected into a website where user input data is not properly encoded or validated
  - Persistent XSS is when code is injected into the contents of a site and the attack runs when a user views the page
  - Non-Persistent is when the attack originates from off the site and is passed along, often in the form of a link

Exploits

- **Privilege escalation**
  - **A malicious user gains normally denied access to another user's data**
  - **Can be done two ways:**
    - **Vertical privilege – gaining the privileges of a higher-privilege user (e.g. sys admin)**
      - **Example: through SQL injection an attacker who normally only has public user access and should not be able to access the system's database can interact with it at the permission level of the admin**
    - **horizontal privilege – the same user level but can access different data or functionality than the current user**

Exploits

- **Rootkits**
  - **One of the most challenging types of malware to combat**
  - **Seek to give root access and are very hard to detect**
  - **May exist at very low level within the system**
    - **In Device drivers**
    - **Within the kernel**
    - **Within the BIOS**
    - **Sometimes even built into hardware**

Interactive Exercise: 4

What are some features of Single Sign On (SSO)?	
What is the identity provider (IDP) main function?	
How does a man in the middle attack work?	
What are the two ways to do privilege escalation?	

Interactive Exercise Answer: 4

What are some features of Single Sign On (SSO)?	- SSO allows a user to access multiple systems with a single set of credentials which streamlines the user experience - SSO also eases the job of admins who have to answer fewer calls about password problems
What is the identity provider (IDP) main function?	It verifies the identity of a user who is trying to use a service from a service provider (SP)
How does a man in the middle attack work?	A man in the middle attack is where an attacker impersonates both a service and client. By impersonating both, the attacker is able to gather sensitive information or is able to introduce falsified information
What are the two ways to do privilege escalation?	- Vertical privilege – gaining the privileges of a higher-privilege user - horizontal privilege – the same user level, but can access different data or functionality than the current user

Quiz

Chapter 12

Question #1

- **Which of the following would not be a consideration in context-based authentication?**
  - **A. The one-time passcode used for authentication was incorrect.**
  - **B. The login attempt occurred outside of regular working hours.**
  - **C. The transaction was initiated from a foreign country.**
  - **D. The commands should have been manually entered, but they were issued faster than any human could type.**

Answer #1

- **A**
  - **One-time passwords are not context sensitive, which means they wouldn't fall into this type of authentication.**
  - **The other options allude to issues of time, location, and behavior, all of which can play roles in context-based authentication.**

Question #2

- **In order to mitigate the security risks that your staff can pose to identity management, you would consider doing all the following except which one?**
  - **A. Remind users never to share credentials with anyone else.**
  - **B. Provide a demonstration of how their online identities can be stolen.**
  - **C. Force complex passwords that must change every two months.**
  - **D. Disable hyperlinks in e-mail messages.**

Answer #2

- **C**
  - **Complex and changing passwords may help improve security in many ways, but they will probably also increase the risk imposed by personnel to identity management because users are likely to adopt bad password practices such as writing them down or using variations of previous passwords.**

Question #3

- You are investigating an incident in which a user account in the accounting department appears to have deleted a critical marketing spreadsheet in a shared folder. Each department has its own VLAN and no other files appear to have been affected. The employee owning that user account claims to not know about this. What is the likeliest explanation?
  - A workstation in the accounting department was probably comprised.
  - The VLANs are not properly segmented.
  - The roles associated with the account may have been inappropriate.
  - The file server was likely compromised.

Answer #3

- C
  - The likeliest among the given choices is that the user account had access to the shared folder and the user inadvertently deleted the file.
  - Given that only one file was deleted, it is unlikely that this would indicate a compromise, and even if the VLANs were incorrectly implemented, that should not have allowed that user account to delete the file.

Question #4

- **Which of the following are features of the standard Kerberos authentication protocol? (Choose two.)**
  - **It uses asymmetric encryption for authentication.**
  - **It uses symmetric encryption for session security.**
  - **It requires use of AS, KDC, and TGS.**
  - **It requires use of AD, KDC, and GTS.**

Answer #4

- **B, C**
  - **Though some implementations of Kerberos support the optional use of asymmetric encryption, the standard does not.**
  - **Furthermore, sessions are always secured using symmetric encryption.**
  - **The key components of a Kerberos implementation are the Authentication Server (AS), the Key Distribution Center (KDC), the Ticket Granting Server (TGS), and the Service Servers (SS).**

Question #5

- **Which of the following statements is not true of Single Sign-On (SSO) solutions?**
  - **They decrease the impact of compromised credentials.**
  - **Identities are verified by a federated identity manager or identity provider (IDP).**
  - **They are widely implemented using the Security Assertion Markup Language (SAML).**
  - **They reduce the number of passwords users have to memorize.**

Answer #5

- **A**
  - **The main disadvantage of Single Sign-On (SSO) is that compromised credentials will affect multiple systems.**

Question #6

- **Which of the following exploits is likely to trigger a certificate warning on the victim's web browser if HTTPS is used in the connection?**
  - **Session hijacking**
  - **Cross-site scripting**
  - **Man-in-the-middle**
  - **SQL injection**

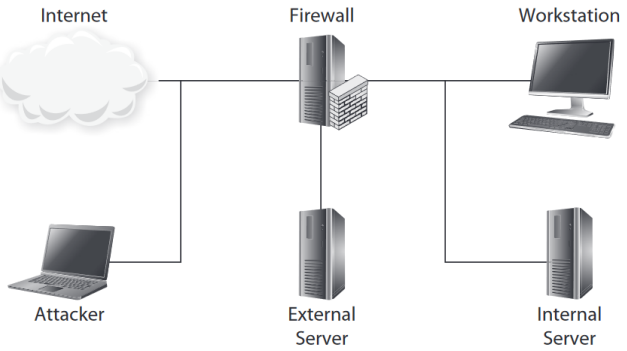
Answer #6

- **C**
  - **A man-in-the-middle attack involving an HTTPS connection will generate a certificate warning on the victim's browser unless the attacker has stolen the target server's private key, which is very rare.**
  - **None of the other exploits will normally generate such warnings.**

Question #7

You are investigating a series of potentially unrelated incidents affecting a small business. Four hosts were involved in these events and are illustrated in the simplified network diagram.

- **The internal server's logs recorded repeated login attempts to a domain administrator account from an external IP address suspected to be the attacker. These attempts were ultimately successful. The server is a domain controller implementing Kerberos. Which of the following is true?**
  - **All objects and subjects in the domain are compromised.**
  - **We only know that the internal server is compromised at this point.**
  - **Any TGTs for the user at the workstation are now invalid.**
  - **The external server will no longer be able to respond to requests from the workstation's user.**



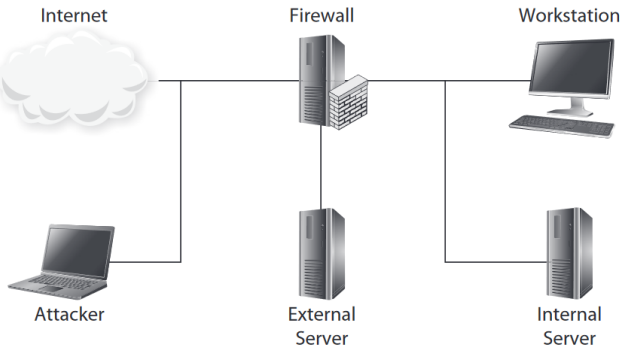
Answer #7

- **A**
  - **Because Kerberos centralizes secret keys and is implemented domain-wide, all secret keys should be considered compromised at this point since the attacker controls the Kerberos server.**

Question #8

You are investigating a series of potentially unrelated incidents affecting a small business. Four hosts were involved in these events and are illustrated in the simplified network diagram.

- **The workstation's user learns of the compromised server and immediately changes the domain account's password. Why will this be an ineffective response?**
  - **A. The password would also have to be changed at the external server.**
  - **B. Changing the password will prevent access to the external server.**
  - **C. The password was not compromised, so it need not be changed.**
  - **D. Changing the password will update the information on the compromised internal server, to which the attacker now has full access.**



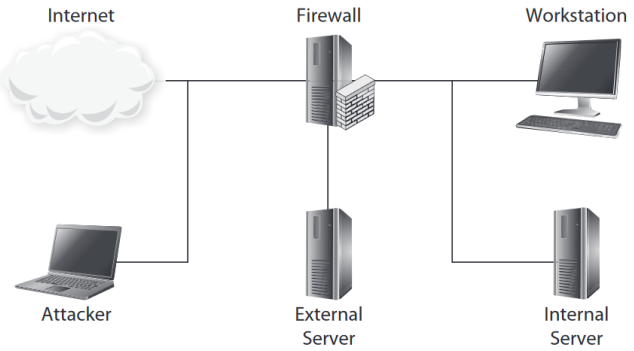
Answer #8

- **D**
  - **The main disadvantage of Kerberos is that it centralizes all the secret keys in the Key Distribution Center (KDC).**
  - **Any domain password changes and changes to the secret keys will be available to the attacker who now controls the server.**

Question #9

You are investigating a series of potentially unrelated incidents affecting a small business. Four hosts were involved in these events and are illustrated in the simplified network diagram.

- **The external server provides virtual private network (VPN) services for remote users. While examining NetFlow data at the firewall, you notice large flows on port 443 from the workstation to a remote user that are correlated to equally large flows on port 443 from the remote user to an external web server. What is likely happening?**
  - **A. The remote user is an attacker who compromised the VPN server, pivoted to the workstation, and is now exfiltrating data.**
  - **B. The remote user is the victim of a cross-site scripting attack.**
  - **C. The remote user is simply visiting the same site as the workstation's user and uploading similarly large files to it.**
  - **D. The remote user is an attacker who compromised the VPN server and is now conducting a man-in-the-middle attack.**



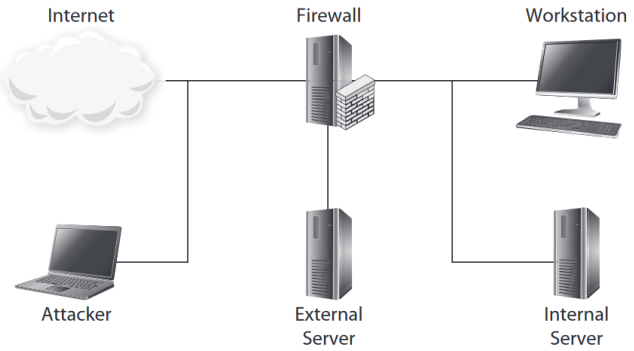
Answer #9

- **D**
  - **In a man-in-the-middle attack, traffic is commonly relayed through a malicious host to the legitimate endpoints.**
  - **It is easiest to conduct this type of attack from the local network, so it makes the most sense to conclude that the attacker leveraged compromised VPN credentials and is now intercepting all of the workstation's user traffic to and from the website.**

Question #10

You are investigating a series of potentially unrelated incidents affecting a small business. Four hosts were involved in these events and are illustrated in the simplified network diagram.

- **You decide to investigate the VPN server and connect to it over SSH. You use netstat to examine network connections, ps to look at running processes, and search to look for newly created suspicious files. You find nothing out of the ordinary. What can you conclude?**
  - **A. The VPN server appears to be secure and you should allow the remote user to connect again.**
  - **B. You should also look for new user accounts and check your log files before reaching any conclusions.**
  - **C. You can't reach any conclusions strictly from built-in tools because a rootkit could interfere with their outputs.**
  - **D. There must be a rootkit in play because you know the server was compromised**



Answer #10

- **C**
  - **Rootkits will prevent system tools from accurately reporting the state of a computer.**
  - **If these tools had reported evidence of compromise, you could conclude that an attack took place.**
  - **However, finding no evidence is no reason to conclude that there is no compromise**

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.