Authentication

Authentication Models

These include context-aware authentication, Single Sign-On authentication, and Federated Identity Management.

Context-Aware Authentication

The most common form of Context-aware authentication occurs by limiting the time or the day that the user is able to log on to a particular client or server. Another common use of this is to limit the geographic location that the user can log in from. For example, if you're a small company in the United States, you don't have any international employees, then you might be able to prevent any users from outside the United States from logging into your systems.

Single Sign-On authentication

Due to the large number of resources and websites that the average person accesses on a daily basis, many organizations are beginning to adopt an SSO environment. When adopted, the organization establishes a default user profile for each user, and then they link that profile to all of the different resources that that user is going to have to access. Now, under this type of system, the user is able to have a single long, strong password that they can memorize. This replaces the 30 or 40 different login credentials that the average user has. And since they let you memorize one, they can make it more complex and easier to learn. Additionally, if you're using multi-factor authentication, like we talked about in the last lesson, you now have a single strong dual factor or multi-factor authentication to use.

Federated Identity Management

The final model is called the Federated Identity Management or FIDM. Many organizations are now grouping together to create these Federations. Each organization that joins this Federation has agreed to a common set of standards and policies for the use of identification. This allows a Federated Identity to be created for that user. This identity can then be used across all of those different businesses that are part of the Federation, as well as all their systems. These Federations support

the provisioning and management of identification, authentication, and authorization. This can be done through two basic models, either Cross-Certification or Trusted Third-Party. The Cross Certification model is going to utilize a web of trust between these organizations. Now, that brings us to the second type, which is called a Trusted Third-Party Model. This is also known as a bridge model. This allows organizations to place their trust in a single third party. This third party, then, manages the verification and certification for all of the organizations within the Federation. This is more similar to the way a traditional certificate authority on the Internet is going to work. In this model, it's quite efficient even with a large number of organizations within the Federation, because everybody goes to that one trusted person to get their verification done.

SAML/OpenID

Security Assertion Markup Language, or SAML, is an attestation model that's built on top of XML, and it supports this federated identity management. SAML is used for the authentication and authorization between different systems, especially over the Internet using a Single Sign-On method. To perform this function, SAML is going to use an attestation ticket that's provided to the user being authenticated. Another possible solution that you might find is OpenID, which is an open standard decentralized protocol to authenticate users. OpenID allows the user to log into an identity provider and they can then utilize that same account across all of the cooperating websites. These cooperating websites are known as RP's or Relying Parties. One of the largest and most well-known OpenID identity providers is actually Google. Anytime you've gone to a website outside of Google, and you click that Google login button, you're using an OpenID system, to have Google authenticate you to that third-party website. OpenID is also much less difficult to implement than SAML. But SAML does perform these functions a lot more efficiently than OpenID. Which one you're using is really going to be up to you.

802.1x

802.1x is a standardized framework that's used for port-based authentication on both wired and wireless networks. Now, since 802.1x is just the framework, it's actually going to utilize other mechanisms to do the real authentication for us. For example, both the remote authentication dialling user service, known as RADIUS, and the terminal access controller access control system plus, or TACACS+, can both be utilised to conduct the authentication, using the 802.1x protocol. There are three roles that are required for an authentication to occur under 802.1x. The first is the supplicant, which is the device or user that's requesting access to the network, such as PC1 in this image. Then, there's an authenticator, which is the device through

which the supplicant is attempting to access the network. Normally, this is going to be something like a switch, a wireless access point, or a VPN concentrator. Finally, there's the authentication server, which is going to be the centralized device that performs the authentication, which is usually going to be your RADIUS or your TACACS+ server. Now, 802.1x is certainly something that should be considered in your network architecture as it's considered one of the best protections that you can add to your internal network connectivity to prevent rogue devices from gaining access to your organization's devices and connections.

EAP

802.1x also allows for us to encapsulate the extensible authentication protocol, or EAP, when we're using a wired or wireless connection. EAP is actually not a single protocol by itself, but a framework in a series of protocols that allows for numerous different mechanisms of authentication, including things like simple passwords, digital certificates, and public key infrastructure.

EAP-MD5 is a variant of the EAP and it utilizes simple passwords and the challenge handshake authentication process to provide remote access authentication. If you're using this method, you have to ensure that you're using long, strong, and complex passwords in order for you to maintain the security of your system. EAP-MD5 is a one-way authentication process and it's not going to provide mutual authentication.

EAP-TLS is a form of EAP that's going to use public key infrastructure, with a digital certificate being installed on both the client and the server, as the method of authentication. This makes it immune to password-based attacks, since neither side is going to use a password and instead, they're going to use digital certificates to identify themself. This is considered a form of mutual authentication between both devices, the client, and the server, because each one is going to authenticate with the other.

Another variant of this is called EAP-TTLS. This form is going to require a digital certificate on the server, but not on the client. Instead, the client is going to use a password for its authentication. This makes it more secure than the traditional EAP-MD5, which just uses passwords, but it is less secure than the EAP-TLS because that one removes the password vulnerability by using two-digit certificates.

Now, EAP-FAST, or EAP flexible authentication via secure tunneling, is our fourth variant of EAP. And this is going to use a protected access credential, instead of a certificate, to establish that mutual authentication between devices.

The fifth and final type of EAP is called PEAP, or protected EAP. This variant also supports mutual authentication by using server certificates and the Microsoft Active Directory databases for it to authenticate a password from the client.

Now, in addition to all these cross platform variants of EAP, there's also a proprietary protocol from Cisco, called LEAP, or the lightweight EAP. But, for you to be able to use this in your organization, you have to be running a Cisco-based network and all of your clients have to support it.

LDAP/Kerberos

LDAP is the lightweight directory access protocol. This is a database that's used to centralize information about your clients and your objects on the network. LDAP is essentially a simplified version of X.500, which is a directory service, and it contains a hierarchical organization of the users, groups, servers, and systems inside your network. LDAP communicates over port 389 when it's doing it unencrypted. And if you decide to encrypt it using SSL or TLS, it's going to use port 636. Both of these are ports you should know for the Security+ exam. Now, while LDAP is considered cross platform, Microsoft created their own implementation of this, known as AD or Active Directory. This is yet another example of a single sign-on system. Now, Kerberos, on the other hand, is focused on authentication and authorization. This is performed through our Kerberos ticketing system in a Windows domain. Kerberos is an authentication protocol that provides for two-way or mutual authentication. When a user logs on to the domain, they first contact the domain controller which acts as the key distribution center, or KDC. This KDC has two basic functions, authentication and ticket granting. So, if your client is authenticated properly, the KDC will issue them a TGT, which is called a ticket-granting ticket. This ticket-granting ticket is then provided to the domain controller anytime that user wants to access a resource. And then the domain controller can provide that user with a service ticket or a session key to use, whichever one's appropriate for their needs. These tickets are presented to the resource and the access is then granted, because the resource always trusts the domain controller's provided tickets. If your domain controller is running Kerberos, it's going to have port 88 open so it can receive those inbound service login requests from the clients. Now, because Kerberos relies on the domain controller to serve as that key distribution center, this is a single point of failure in the domain. If the domain controller is down, ticket-granting services are also shut down. To prevent this, though, what most people will do is have a primary and a secondary active domain controller. That will give you this form of redundancy to ensure Kerberos is up and LDAP is still running.

Remote Desktop Services

RDP

RDP is a proprietary protocol that was developed by Microsoft to allow administrators and users to remotely connect to another computer and have a graphical user interface instead of the command line provided by tools like Secure Shell and Terminal Services. This allows the user to operate the computer as if they were simply sitting in front of a Windows Desktop. Now, remote desktop protocol provides native encryption as part of the design, but it doesn't provide for authentication. Therefore, you have to enable SSL or TLS for service authentication and require some kind of a digital certificate for increased security when RDP is being implemented within your network.

VNC

Virtual Network Computing or VNC. This is similar to RDP, but it's platform-independent. Where RDP works on Windows machines, VNC works on Linux, OSX, or Windows, making it cross platform and an easy way to get a graphical user interface that you can remotely connect to. VNC becomes a great solution for us to consider anytime you're using things that are just beyond the Windows domain. In order to use VNC or Virtual Network Computing, you have to have a VNC server set up on the machine that you want to access. You also have to have a VNC client on the machine you're going to access it from and the VNC protocol, known as the remote framebuffer, to communicate between the two. VNC or Virtual Network Computing, normally, is going to operate over port 5900 or 59 hundred and it should only be used internal to your own network. For connections outside of your enterprise network, it's much more secure to use VPN or an SSH connection first and then, tunnel VNC over that secure connection.

Remote Access

When implementing remote access to your network, you have to carefully select the method of network authentication. There are various options to choose from, including:

- PAP, the Password Authentication Protocol
- CHAP, the Challenge Handshake Authentication Protocol
- EAP, the Extensible Authentication Protocol

PAP

The first remote access authentication that was widely used is known as PAP, the Password Authentication Protocol. Now, PAP is a really old protocol and because of that, it was never built with security in mind. In fact, whenever they sent the username and passwords, those user credentials over the network during the authentication, it didn't even encrypt them. They were sent in plain text. This makes PAP an insecure choice for any modern network and you simply shouldn't use it.

CHAP

Well, because after PAP, came CHAP and with CHAP, it's an evolution to PAP, and it's the Challenge Handshake Authentication Protocol. This is going to solve the problem of sending credentials over the network in clear text. Instead, they're going to have the server send the client a string of random text called a challenge. This random text is then encrypted by the client using their password and this text is then sent back to the server. The server then unencrypts that text using the user's stored password and checks if the encrypted text matches the original text that it sent in the challenge. Using this method, the password is never sent across the network and the security can be achieved and ensure that we have it safe. Now, CHAP was popular for many years and Microsoft even created their own proprietary version called MS-CHAP. MS-CHAP provides stronger encryption keys and mutual authentication so, it was an improvement over standard CHAP.

EAP

Now, while the CHAP and MS-CHAP were used widely for many, many years, both of these have been overtaken by EAP, the Extensible Authentication Protocol, that we discussed earlier in this section.

VPN

Virtual private networks, or VPNs, allow end users to create a tunnel over an untrusted network like the Internet and remotely and securely connect back to our enterprise networks. These VPN connections provide a layer of encryption around that connection, creating this virtual and secure circuit between your end user's device and the VPN concentrator that terminates that connection back inside our enterprise networks. VPNs are commonly used by teleworkers and traveling employees so that they can remotely access the corporate resources, things like our intranets and our file servers.

VPNs rely on two different protocols when they're being operated. One is called the point-to-point tunneling protocol and the other one is the layer two tunneling protocol.

Client-to-Site VPN

This type of VPN is what we call a remote access VPN or a client-to-site VPN, because one person is connecting back to the larger site.

Site-to-Site VPN

Now, in addition to this, VPNs can also be used to connect two different sites together. So, instead of having to purchase a dedicated lease line between two offices, I can use the Internet as my transport path. For example, if a company has a small satellite office in Washington DC and wants to connect it back to their headquarters out in San Francisco, it could be less expensive to implement a site-to-site VPN instead of having to purchase a dedicated lease line that goes that 3,000 miles between those two cities. Now, when you're creating a site-to-site VPN connection, routers on both sides are going to be configured with an encryption key and this key's going to be used to encrypt all of the traffic between the sites to keep it safe from prying eyes and confidential as it goes over that untrusted and dirty Internet between the two locations.

VPN concentrator

For your organisation to allow VPN connections, though, you have to have a server sitting there and answering all of those requests for connection. If you don't want to have a dedicated server to do that, you can, instead, buy a hardware device known as a VPN concentrator. Now, a VPN concentrator can allow hundreds of simultaneous VPN connections from all of your remote workers to easily connect back into your company's intranet, and this frees up your server.

Split Tunnelling

One area of concern we have with VPNs is how do we ensure that clients aren't using split tunnelling? Well, when they're using split tunnelling, what this means is that a remote worker's device will use their own Internet connection for their web request, but they're going to use your VPN connection for all of their intranet requests like your file server request. Now, this is efficient from a bandwidth

perspective, because they don't have to send all of their requests over the VPN to your company and then out to the Internet and then back to the company and then back over the VPN to get to them. But by doing split tunnelling, you are allowing a security risk to occur. This is because your company now has an alternate path to the Internet because it can go from your file servers out to the remote worker's laptop and then out to the Internet, bypassing a lot of your network perimeter defences.

Radius/TACACS+

Radius

RADIUS is the Remote Authentication Dial-In User Service. It provides centralised administration of dial-up, VPN, and wireless authentication so that you can use that with both 802.1x and the Extensible Authentication Protocol, or EAP. RADIUS is a client/server protocol that runs over the seventh layer of the OSI model, the application layer. RADIUS is usually configured to be run on a separate server, but it can also be loaded up on a Windows server in smaller domain environments. RADIUS is used to authenticate users, authorise them to services, and account for their usage of those services. This is the typical AAA that we spoke about all the way back in section one of the course, Authentication, Authorization, and Accounting. RADIUS also utilises UDP for making its connections, making it fairly fast during its authentication to authorization functions. RADIUS commonly uses port 1812 for its authentication messages and port 1813 for its accounting messages. Some proprietary versions of RADIUS may also use ports 1645 and 1646, instead. Now, exam tip here, I would have these ports memorised as part of the things you need to know before test day because you may see some test questions on them.

TACACS+

Now, while RADIUS is a cross-platform standard, there is a proprietary protocol from Cisco called TACACS+ that we've mentioned before. This is the Terminal Access Controller Access Control System Plus which can perform the role of an authenticator in an 802.1x network. Now, it's up to you to determine which one is best for your organisation's needs. Personally, I've used RADIUS almost exclusively within my organisations. I've found that TACACS+ is a little bit slower to operate because it's relying on TCP instead of UDP, and operates over port 49. But TACACS+ does have some benefits. It gives you some additional security and

independently conducts its authentication, authorization, and accounting processes. TACACS+ supports all network protocols. But RADIUS, on the other hand, doesn't support the remote access protocol, NetBIOS Frame protocol, X.25 PAD connections, and some others.

Summary

802.1x

First, 802.1x is an IEEE standard that defines Port-Based Network Access Control or PNAC. 802.1x is a data link layer authentication technology that's used to connect devices to a wired or wireless LAN. Also, it defines the EAP protocol.

LDAP

Second, LDAP is the lightweight directory access protocol. It's an application layer protocol for accessing and modifying directory services data. Microsoft's Active Directory uses LDAP.

Kerberos

Third, Kerberos is an authentication protocol that's used in Windows to identify clients to a server using mutual authentication. In Windows, this in implemented through a series of tickets.

Remote Access Service

Fourth, Remote Access Services or RAS is a service that enables dial-up and VPN connections to occur from remote clients.

CHAP

Next, the Challenge Handshake Protocol or CHAP is an authentication scheme that's used for standard dial-up connections.

Radius

Next, RADIUS is a centralised administration system for dial-up, VPN, and wireless authentication. It's going to use 1812 and 1813 or ports 1645 and 1646 using UDP for its transport mechanism. RADIUS is used with 802.1x and EAP.

TACACS+

Finally, TACACS+. TACACS+ is a Cisco-proprietary remote authentication system that provides separate authentication and authorization functions using port 49 over a TCP connection. TACACS+ is similar to RADIUS, but it is not considered cross-platform.

Authentication Attacks

- Spoofing
- Man-in-the-middle
- Password spraying
- Credential stuffing
- Broken authentication

Spoofing

Now, when we talk about spoofing, this is a software-based attack where the goal is to assume the identity of a user, a process, an address, or other unique identifier. Spoofing is used a lot to try to bypass authentication and be able to present yourself as if you're somebody else.

Man-in-the-middle

Now, one of the things attackers love to try is the man-in-the-middle attack. Now, a man-in-the-middle attack, or MitM, is an attack where the attacker is going to sit between two communicating hosts and transparently captures, monitors, and relays the communications between those hosts. Now, we've talked about a man-in-the-middle before, but essentially, if you're on a wireless network, somebody could be sniffing the air, capturing those packets, and then being a man-in-the-middle. They can capture what's being said. Now, they put themselves directly in the middle of the communication, you might be connecting to them, and they would be connecting to the server and they're listening to everything you say.

Now, a variation on this is what's known as a man-in-the-browser. This is an MitB. This is an attack that intercepts the API calls between the browser process and its DLLs. And so, if you're attacking the network or between two clients or a client in the server, you're a man-in-the-middle. If you're using the browser to do it, you're a man-in-the-browser.

Password spraying

This is a brute force type of attack in which multiple user accounts are tested with a dictionary of common passwords.

Credential stuffing

Now, credential stuffing is another type of brute-force attack. In this one, they're going to try and take stolen user account names and passwords and test them against multiple websites. So, let's say there was a new story and there was a new data breach that happened and Facebook got hacked. And now, all of Facebook's usernames and passwords are known. So, everybody knows what the usernames are, which are emails and the passwords.

Broken authentication

Broken authentication is a software vulnerability where the authentication mechanisms allow the attacker to gain entry. Essentially, the coders did a really bad job. Now, when this happens, you can have bad things happen like displaying clear text credentials, using weak session tokens, or permitting brute-force login requests.