CompTIA Pentest+ (Attacks)

Study online at https://quizlet.com/_g034jo

Piggybacking	hacker gains access by following behind someone who is complicit example: someone holding a door open to be helpful
Tailgating	hacker gains access by following behind someone who isn't complicit or aware example: hacker walks through an opened door as it is closing
Lock Bypass	Pentester could jam a lock or bypass it by manipulating the locking function Stop a door from being shut fully by inserting a spacer or wedge * breaking a lock
Egress Sensor	Door will automatically unlock and open when a person approaches Sensors could be tricked to allow the door to be opened Some of these "fail open" when power is lost
Man-in-the-Middle	ARP spoofing Replay Relay SSL stripping Downgrade
ARP Spoofing	Attacker sends falsified ARP messages over the local area network Results in the attacker's MAC being associated with the IP of a valid computer
Replay Attack	Attack occurs when valid data is captured by an attacker and is repeated or delayed For example, they could capture a wireless authentication handshake and replay it to gain access to the wireless network as an authenticated client
Relay attack	Attack occurs when the attacker is able to become the man-in-the-middle and acts as a middle man in a communication session
SSL Stripping	Attack where a website's encryption is tricked into presenting the user with a HTTP connection instead of a HTTPS connection
Downgrade	Attack that attempts to have a client or server abandon a higher security mode to use a lower security mode TLS 1.2 is more secure than SSL 2.0 Ï Downgrade attack will cause session to attempt to establish an SSL 2.0 connection
Network Access Control (NAC) Bypass	NAC can prevent you from gaining access to the network NAC can often be bypassed by spoofing the MAC address of a VOIP device Ï Many VOIP devices don't support 802.1x Ï Their MAC addresses are often whitelisted for NAC
Virtual Local Area Network (VLAN) Hopping	VLANs are often used as logical separation Attack host on a different VLAN to gain access Double tagging the VLAN tag in 802.1Q Switch Spoofing Ï Attempt to auto negotiate with a targeted switch by setting your device to act as a switch Ï Switches get copies of all VLAN traffic and separate them based on tags
Evil Twin	Rogue access point that appears to be legitimate but is setup to eavesdrop on wireless communication
Karma Attack	(Evil Twin) Ï Karma Attacks Radio Machines Automatically

	Ï Devices listen for SSID requests and respond as if they Ï were the legitimate access point
Deauthentication (DeAuth) Attack	(Evil Twin) Type of denial of service that targets communication between a user and a wireless access point
Fragmentation Attack	Attacker exploits a network by using datagram fragmentation mechanisms against it A small amount of keying material is obtained from the packet then attempts to send ARP and/or LLC packets with known content to the access point (AP) If the packet is successfully echoed back by the AP then a larger amount of keying information can be obtained from the returned packet
Credential Harvesting	Attack that focuses on collecting usernames and passwords from its victims In wireless, this is usually performed by creating a fake Captive Portal ESPortalV2 can be used to setup a fake portal and redirect all WiFi devices connected to the portal for authentication
WPS Implementation Weakness	Wi-Fi Protected Setup (WPS) uses a push button configuration method to setup devices Uses an 8-digit WPS Pin to configure them Can be easily brute force attacked because the PIN is authenticated by breaking it in two Reaver and Bully are common attack tools
BlueJacking	ÏSending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs, or laptops
Bluesnarfing	Theft of information from a wireless device through a Bluetooth connection
RFID Cloning	Attacker captures the Radio Frequency (RF) signal from a badge or device and can copy it for reuse
Repeating	Used to capture the existing wireless signal and rebroadcast it to extend the range If not properly configured by the network administrators, this can be an attack vector
Fake Cellphone Towers	Used to capture the International Mobile Subscriber Identity (IMSI) number Can be used to create a man-in-the-middle
Deauthorization	forces connection for a device on the network, so a handshake can be created for Aircrack-ng using airreplay-ng
Parameter Pollution (Authorization)	HTTP parameters are modified in order to conduct a malicious attack
Insecure Direct Object Reference (Authorization)	Application provides direct access to an object based on the user-supplied input
Stored (persistent) XSS	Data provided by attacker is saved on server
Reflected XSS	Non-persistent, activated through link on site
DOM	o Document Object Model (DOM) is vulnerable o Victim's browser is exploited (client-side XSS)
CSRF/XSRF	Cross-Site Request Forgery
Cookie Manipulation	ÏDOM-based cookie manipulation that allows a script to write data into the value of a client-stored cookie
File Inclusion	Attack that includes a file into a targeted application by exploiting a dynamic file inclusion mechanism Usually occurs due to improper input validation by application File can be included

Example of Local File Inclusion	../../uploads/malware.exe
Example of Remote File Inclusion	https://www.xyz.com/malware.exe
Verbose error handling	ÏErrors can display too much information Ï Great for debugging...horrible for security
Hard-coded credentials	ÏSource code of a web application has the username and password written into the code instead of using an inclusion file Ï Common issue for applications using PHP, databases, or WordPress
Race conditions	ÏFlaw that produces unexpected results when the timing of actions can impact other actions Ï Can occur when multithreaded operations are occurring on the same piece of data
Unauthorized use of function/unprotected API	ÏAllows anyone with network access to send your application a request Ï Designers should implement function-level access control
Example of Unauthorized use of function/unprotected API	http://example.com/app/getappinfo http://example.com/app/admin_getappinfo
Hidden elements	ÏHTML forms often use hidden elements o Fields using <INPUT TYPE=HIDDEN> Ï Could allow sensitive data to be stored in the DOM
Lack of code signing	ÏWithout code signing it is easy for an attacker to modify the code and it go unnoticed Ï Code signing ensures it is digitally signed, which uses a hash digest that is encrypted with a private key certificate to ensure changes have not occurred
SUID	Set-User Identification (SUID)
SGID	Set-Group Identification (SGID)
Sticky Bit	Used for shared folders like /tmp Allows users to create files, read, and execute files owned by other users Attack cannot remove files owned by others -t
Ret2libc	An attack technique that relies on overwriting the program stack to create a new stack frame that calls the system function Stands for "return to library call" 
Cpassword	Name of the attribute that stores the passwords in a Group Policy preference item Stored in the SYSVOL folder on the Domain Controllers in encrypted XML file Easily decrypted by any authenticated user in the domain, though
Clear Text Credentials in LDAP	If SSL is not enabled for LDAP, credentials are sent over the network in clear text Use the Insecure LDAP Bind script to check for this in PowerShell You receive a CSV file as output showing which accounts are vulnerable
Kerberoasting	Any domain user account that has a service principal name (SPN) set can have a service ticket (TGS) Ticket can be requested by any user in the domain and allows for offline cracking of the service account plaintext password

Credentials in LSASS	Local Security Authority Subsystem Service Process in Windows that enforces the security policy of the system Verifies users when logging on to a computer or server Performs password changes Creates access token (ie, Kerberos)
Unattended Installation	Clear text credentials of Preboot Execution Environment (PXE) could be captured using network sniffers
SAM Database	Security Account Manager is a database file that stores the user passwords in Windows as a LM hash or NTLM hash File is used to authenticate local users and remote users Passwords can be cracked offline if the SAM file is stolen
DLL Hijacking	Dynamic Link Library (DLL) provides a method for sharing code and allows a program to upgrade its functionality without requiring re-linking or re-compiling of the application Hijacking is a technique used to load a malicious DLL in the place of an accepted DLL
Exploitable Services	Attacker uses the way services normally operate to cause an unintended program to run
Sandbox Escape	Escape the vm to exploit the hardware
Cold Boot Attack	A side channel attack where an attacker has physical access to the system User is able to retrieve the encryption keys from a running operating system after using a cold reboot to restart the machine
JTAG Debug	JTAG is a standard for verifying designs and testing printed circuit boards Ï Diagnostic connection Port use for debugging, probing, and programming With breakpoints setup, the JTAG can be used to read registers from motherboard and read arbitrary memory locations
Serial Console	Many network devices still have serial console connections (routers and switches) If attacker can get physical access to the device then they can connect to the device over the serial port Lower security enabled (if any) on these ports
Situational Awareness	A shared common understanding of the network and its current security state
De-confliction	Determining if detected activity is a hacker or an authorized penetration tester
De-escalation	Decrease the severity, intensity, or magnitude of a security alert that is being reported
Stages	Communication often occurs as the assessment moves from one phase to another
Critical Findings	A vulnerability is found that causes significant risk to occur to the security of the network
Indicators of Prior Compromise	Attack signatures have been detected and the network has been previously hacked
Goal Reprioritization	Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state?
Communication Paths	How will the pentest team communicate with the organization? Ï Phone, text, chat, email, white paper, etc. Who at the organization can they contact? o CEO/CSO/CTO or System Admins