Click to verify

netsh wlan show profile "WIFI-NAME-PROFILE" key=clear | findstr “Key Content” then netsh wlan show profile "WIFI-NAME-PROFILE" key=clear | findstr "Key Content". ================================== netsh wlan show profiles > wifiprofiles.txt then for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @if "%j" NEQ "" (echo SSID: %j & netsh wlan show profile name=%j key=clear | findstr "Key Content") & echo. ================================== @echo off setlocal enabledelayedexpansion for /f "tokens=2 delims=:" %%a in ('netsh wlan show profile ^| findstr ":"') do (set "ssid=%%~a" call :getpwd "%%ssid:~1%%") echo. echo Press any key to exit... pause > nul exit :getpwd set "ssid=%*" for /f "tokens=2 delims=:" %%i in ('netsh wlan show profile name^="%ssid:"=%" key^=clear ^| findstr /C:"Key Content"') do (echo SSID: %ssid% PASS: %%i) To find wifi password using cmd windows is good option. We appreciate all contributors who share knowledge and expertise with us. If you find any issue or have suggestion for improvement, please submit pull request or open issue. In today's digital world, wifi connection is very important. Whether at home, in office or out in public, staying connected become necessity. But, if you forget your wifi password it can be frustrating. Fortunately, if you using windows computer, you can easily recover your wifi password using cmd. Before we start finding wifi password, it's good to understand what is command prompt. Command prompt also known as cmd is a command-line interpreter in windows operating system. It allow user to execute various commands to perform specific task. This can include file management or network troubleshooting. Why use cmd to find wifi passwords? There are many reasons why you should use cmd to find wifi password. First, executing command is faster than navigate through several window and dialogue in graphical user interface. Second, cmd give you precise control over what you want to do or find without cluttering your screen with unnecessary information. Third, cmd can be used for various task beyond just finding wifi password. No additional software required, because cmd is built into windows operating system. But, before we start, make sure you meet some pre-requisites. First, you should using windows os. Second, you need to have administrative rights on your computer. And third, device must be connected to wifi network before. Now, let's start step by step guide to find wifi password with cmd. Step one, open command prompt. Press win + r and type cmd. Then press enter. Next, right click on cmd icon and select run as administrator. Step two, view all wifi profiles. In command prompt window, type netsh wlan show profiles and press enter. This will display list of all wifi networks your computer has connected to. Step three, find password of specific profile. Identify profile name from list retrieved in previous step. Then use following command: netsh wlan show profile name="profileName" key=clear. Replace "profileName" with actual name of profile you want to query. Step four, locate password in output. After executing above command, you will see various details about selected wifi profile. Look for line titled "key content" under security settings section. This line display your wifi password.netsh wlan show profile name="HomeNetwork" key=clear Security settings ----------------------------- Key Content : yourWiFiPassword Troubleshooting Common Issues Update Drivers →Fix Your PC → While the method described is straightforward, you might run into some common issues: Issue 1: No Wireless Networks Found If no wireless networks are displayed when you run netsh wlan show profiles, consider the following: Ensure your WiFi adapter is enabled. Connect your device to a WiFi network and try again. Issue 2: Access Denied If you receive an "Access Denied" error: Ensure you are running CMD as an administrator. Check your user permissions. Issue 3: Missing Key Content If the "Key Content" field is absent in the output: The command might not be run correctly; ensure you've used the correct profile name. The WiFi network may be misconfigured or doesn't have a password set. Additional CMD Commands Related to WiFi Beyond simply recovering passwords, CMD can also be used to perform other network-related tasks. Here are a few useful commands: 1. Check Current WiFi Connection To find out the current WiFi network you're connected to, type: netsh wlan show interfaces This will show details about the active WiFi connection, including its name, signal strength, and more. 2. Disconnect from WiFi Network If you wish to disconnect from a network, use: netsh wlan disconnect 3. Connect to a WiFi Network If you know the SSID (name) and password of a WiFi network, you can connect using: netsh wlan connect name="ProfileName" 4. Delete a WiFi Profile If you want to remove a WiFi profile from your device, you can use: netsh wlan delete profile name="ProfileName" Security Considerations Using CMD to retrieve WiFi passwords is generally safe, especially on personal devices. However, it's crucial to maintain the security of your device: Keep Your Computer Secure: Always run updates and use antivirus software. Be Careful Using Public WiFi: When connected to public networks, be cautious of security threats. Change Default Passwords: If you are using a common router or modem, always change the default password to avoid unauthorized access. Conclusion Update Drivers →Fix Your PC → Finding your WiFi password using CMD is an efficient and straightforward process that everyone should know. By employing the Command Prompt, you gain quick access to essential network settings and can maintain better control over your computer's connections. With the steps outlined in this guide, you should now feel confident retrieving WiFi passwords whenever necessary. As technology continues to evolve, knowing how to navigate tools like Command Prompt is invaluable. Whether you're a tech enthusiast, a casual user, or someone who often deals with network issues, mastering CMD will undoubtedly enhance your problem-solving skills and technical know-how. In the future, always remember to save your passwords securely and consider using a password manager to keep track of your various logins, including WiFi passwords. Being proactive about password management not only saves time but also helps maintain your digital security. Wlan means wifi lan.Reference (WiFi Pentesting) — First convert wlan0 (managed mode) to wlan0mon (monitor mode) by using the below cmds. Inorder to go back. Looking for WiFi's Look for network packets using airodump. You can get BSSID/MAC Add via the above cmd. Press CTRL + C and get the BSSID of a private WiFi (like OnePlus). Copy it as it will be needed for EAPOL or 4 way handshake. Capturing 4 Way Handshake Now open 2 terminals. In the first one, use cmd while saving it in a ".cap" file (below is hack1 file). It uses the wirelessLooking forward to seein everyone at the meeting tomorow and discussin our strategies in detail. We need to check for connecting stations and shows their MACs. Notice that no channels are mentioned. This is done to know the channels used by AP (Access Points) in the second terminal. Simultaneously, in the second terminal write the aireplay cmd to deauth clients. This will show what channels does the AP use. Now add those channels to the cmd in the first terminal as shown. This captures WPA Handshake in the first terminal precisely 4 messages. Now do 'ls' to find hack1–01.cap file. Open it using cmd below. In wireshark set filter to "eapol" (for getting handshakes). As mentioned above, 4 msgs will be captured b/w the new connection to the wifi and the wifi itself. Here phone MAC was 66:9a: (and so on) and wifi MAC was ea:75: (and so on). Message 1 of 4 description - Message 2 of 4 description - Message 3 of 4 description - Message 4 of 4 description - Cracking WiFi Password We need to crack WPA Key Data. Since all "hack1–01" files are in "root" user, we need to move it to /home/kali. We can find the password of the wifi by this below cmd. If its in wordlist rockyou.txt then it will be cracked else not. (2) Fern WiFi cracker We can also use a tool named Fern WiFi Cracker. Fern works for LNMIIT WiFi also (Just need a better wordlist in order to get password via bruteforce/dictionary attack). can be used to create psk. (3) Wifite and Hashcat Using Wifite to crack password. We need to put below cmd. They when asked to select target, select any from the identified. Now convert '.cap' to '.hccapx' via hashcat-utils/cap2hccapx Hashcat Wiki — in windows with cmd provided. (4) Hashcat, hcxdumptool and hcxpcapngtool Use the following cmd on terminal in-order/sequence. sudo systemctl stop NetworkManager.servicesudo systemctl stop wpa_supplicant.servicesudo hcxdumptool -i wlan0 — nmea_pcapng dumpfile.pcapngsudo systemctl start wpa_supplicant.servicesudo systemctl start NetworkManager.servicehcxpcapngtool -o hash.hc22000 -E essidlist dumpfile.pcapnghashcat -m 22000 hash.hc22000 wordlist.txt Now this creates a file by the name of '2023...(some digits).....-wlan0.pcapng' instead of dumpfile.pcapng. Hence we do a cat cmd as shown below. After this now drag-drop dumpfile.pcapng to Windows and then write the below cmd in windows instead of Kali since Kali in VM doesn't have the power/memory to execute. Since windows has a GPU, execute the following cmd there in Command Prompt. Evil-Twin Attack using Airgeddon We will explore the ominous world of Evil Twin attacks and understand how to safeguard ourselves using the powerful tool, Airgeddon. Follow these step-by-step instructions, accompanied by screenshots, to fortify your defenses against this menacing security threat. To exploit a Wi-Fi network with a connected client, the attacker requires a Wi-Fi card with a VIA-supported chipset, a requirement is to inject a malicious packet into the network. To start run the following cmd - Now select an interface (its always/mostly wlan0). Change the mode to Monitor Mode. After that select the attack you wish to do. Here we wish to do an Evil Twin attack. Select 9 option now It starts scanning WiFi. Now, Configure Captive Portal Set up a Captive Portal for your Evil Twin network to capture login credentials from unsuspecting users. Now choose and select a target. Start the Attack Airgeddon will configure the Evil Twin attack and begin broadcasting the malicious network. Wait for unsuspecting users to connect.We should be careful when connecting to Wi-Fi networks, especially in public or unfamiliar environments. A rogue access point with a similar network name can trick clients into entering their passwords, giving attackers unauthorized access. To test if a wireless network is secure, we can use aireplay-ng commands. First, set up an airmon mode using the command `airmon-ng check freq`. This will scan for available channels and report any potential issues. Here is how to get the password for the Wi-Fi network called "Gravity" using the Command Prompt. Step 3: Type in the right commandNow, type `netsh wlan show profile name="Gravity" key=clear` and press enter. This will display a bunch of information about that Wi-Fi network, including its settings and your saved password.This command shows you all the details of the "Gravity" network, like its Profile info, Connect settings, Security settings, and even Cost settings for that specific network profile.Using CMD Step 4: Find Your Password Scroll through these results until you find an entry called "Key Content", and next to it will be your Wi-Fi password for "Gravity".Wi-Fi password via CMDNow that we have the password, we can connect our device to this network easily. Easy Way to Find Your Wi-Fi Password Via Network Settings MethodStep 1: Open Network SettingsFirst, get connected to your Wi-Fi network , then right-click on the [Network] icon in the taskbar and select [Network and Internet settings].Check Wi-Fi PasswordStep 2: Choose Advance SettingsNext, scroll down and click on [Advanced network settings].Network & InternetUnder Related settings, choose [More network adapter options].Network and Internet SettingsStep 4: Select WiFi Option Pick your connected Wi-Fi network, then pick [View status of this connection].Network ConnectionStep 5: Select Wireless Properties In the Status window, tap on [Wireless Properties].Wireless PropertiesStep 6: Click on Security TabNow go to the [Security] tab and check the box for [Show characters], Your password will be visible in the Network security key field. How It WorksWhen you connect to a Wi-Fi network, Windows doesn't just save your password like a sticky note. Instead, it uses secure methods to store your password safely within its registry in an encrypted format. Both the CMD and GUI methods securely retrieve this information, eliminating threats from third-party tools. Here's what happens behind the scenes:1. Where Does Windows Store Wi-Fi PasswordsYour saved Wi-Fi passwords are kept safe in a digital vault called the Windows Registry. Think of it like a big file cabinet where Windows stores system info, including network details. Encryption: Your passwords are encrypted (scrambled code) so they can't be read by hackers or bad programs. Access Restrictions: Only administrators (like you, the owner) can access these passwords.2. How Do CMD and Network Settings Get the Password?Both methods access the same encrypted information but in different ways:For CMD (Command Prompt):The `netsh wlan` command is like a master key that decrypts your password from the registry.When you type `key=clear`, Windows shows your password in plain text for a moment.For Network Settings (GUI):The graphical interface (Network & Internet settings) uses a tool called Network Configuration Manager to get the same encrypted password.Unchecking [Show characters] encrypts your password again, like how phones hide text when entering a password.3. Here's How Encryption WorksWindows applies a method called DPAPI (Data Protection API) to encrypt your Wi-Fi password.Here's an analogy:When you enter your password, Windows mixes it into a secret code using a special key linked to your user account.To read it again, Windows uses that same key to decode the code which only happens when YOU ask for it through CMD or Settings.netsh wlan show profile or navigate through the Network & Internet settings can be used to retrieve Wi-Fi credentials in just a few clicks ================================== iwconfig or ip link show command list available interfaces airmon-ng check kill kill annoying processes airmon-ng start wlan0 monitor mode iwconfig wlan0 mode monitor iwlist wlan0 scan | grep "^BSS\|SSID\|WSP\|Authentication\|WPS\|WPA" scan available wifis Hijacker & NexMon can be used to enable Monitor And Injection On Android EAPHammer can be used to run airgeddon with docker wifiphisher can be used for Evil Twin, KARMA, and Known Beacons attacksdeauthentication using Aireplay-ng is a tactic that can persistently disrupt network connections, alarming in its simplicity, with significant implications for network security. Disassociation Packets ---------- Similar to deauthentication packets, disassociation packets serve to sever the connection between a device and an access point. The primary distinction lies in their usage scenarios; while APs emit deauthentication packets to remove rogue devices explicitly from the network, disassociation packets are typically sent when the AP is undergoing a shutdown, restart, or relocating, necessitating the disconnection of all connected nodes. mk4 Mode: b - Beacon Flooding ---------- This attack sends beacon frames to show fake APs at clients. This can sometimes crash network scanners and even drivers! Parameters like "-a" use non-printable characters in generated SSIDs and create SSIDs that break the 32-byte limit. All parameters are optional, and you could load ESSIDs from a file. mk4 Mode: a - Authentication Denial-Service ---------- Sending authentication frames to all accessible APs within range can overload these APs, especially when numerous clients are involved. This intense traffic can lead to system instability, causing some APs to freeze or even reset. Parameters like "-a" send random data from random clients to try the DoS. mk4 Mode: p - SSID Probing and Bruteforcing ---------- Probing Access Points checks if a SSID is properly revealed and confirms the AP's range. This technique, coupled with bruteforcing hidden SSIDs with or without a wordlist, helps in identifying and accessing concealed networks. Parameters like "-t" of a TKIP AP are required. mk4 Mode: m - Michael Countermeasures ---------- Sending random or duplicate packets to different QoS queues can trigger Michael Countermeasures on TKIP APs, leading to a one-minute AP shutdown. This method is an efficient DoS attack tactic. Parameters like "-t" of a TKIP AP are required. mk4 Mode: e - EAPOL Start and Logoff Packet Injection ---------- Flooding an AP with EAPOL Start frames creates fake sessions, overwhelming the AP and blocking legitimate clients. Alternatively, injecting fake EAPOL Logoff messages forcibly disconnects clients, both methods effectively disrupt network service. Parameters like "-l" are used. mk4 Mode: s - Attacks for IEEE 802.11s mesh networks ---------- Various attacks on link management and routing in mesh networks. Parameters are not specified. mk4 Mode: w - WIDS Confusion ---------- This mode is not described in the article. ================================== Attackers can exploit multiple vulnerabilities in Intrusion Detection and Prevention Systems to create confusion and potential system abuse. One such vulnerability is the Zero_Chaos' WIDS exploit, which authenticates clients from a WDS to foreign APs, causing the WIDS to malfunction. Another attack involves manipulating WPS (Wi-Fi Protected Setup) passwords using tools like Reaver and Bully, exploiting weaknesses in the PIN validation process. The WPS Pixie Dust attack takes advantage of nonces used by some Access Points, allowing attackers to easily crack the WPS PIN. Additionally, a Null PIN vulnerability can grant access to poorly designed systems. ================================== To use airgeddon, start by testing your custom PIN using keys 5 and 6. If you have a valid PIN, perform the Pixie Dust attack at keys 7 and 8. Key 13 allows you to test a NULL PIN, while keys 11 and 12 can recollect and generate possible PINs related to the selected AP from available databases. For WEP protection, which is largely obsolete today, use keys 9 and 10 to test every possible PIN. However, airgeddon also offers a "WEP in One" attack option that can crack this type of protection. Modern routers often include an optional Robust Security Network (RSN) field in the first EAPOL frame during association, which includes the PMKID. The PMKID is created using known data and can be used to crack WPA/WPA2 PSK passphrases. Hashcat revealed a new attack method in 2018 that only requires one packet and doesn't need clients to be connected to the target AP. To gather this information, you can use airmon-ng check kill, followed by airmon-ng start wlan0 and cloning hcxdumptool from GitHub. Then, run the tool and save the resulting PMKIDs to a capture file. Convert the capture to hashcat/john format using hcxtools and crack it with rockyou.txt. Additionally, you can use eaphammer to capture PMKIDs or transform handshakes to hashcat/john format using cap2hccapx and john. However, some handshakes captured with hcxdumptool may not be crackable, even with the correct password, so it's recommended to capture handshakes via traditional methods whenever possible. To attack WPA/WPA2 networks, you can monitor network traffic on a specific channel and BSSID using airodump-ng, hoping to capture a handshake. Momentarily disconnecting a client from the network can force re-authentication, increasing the chance of capturing a handshake.Looking forward to seeing everyone at the meeting tomorrow and discussing our strategies. ================================== Once in airodump-ng appears some handshake information this means that the handshake was captured and you can stop listening. #Cracking the Handshake with Aircrack-NG Check if handshake in file aircrack aircrack-ng psk-01.cap #Search your bssid/essid and check if any handshake was capture tshark tshark -r psk-01.cap -n -Y eapol #Username Capture Reading Looking like even using one of the most secure authentication methods, PEAP-EAP-TLS, it is possible to capture the username sent in EAP protocol. To do so, you can capture an authentication communication and filter the packets by eapol. #EAP Authentication Methods In enterprise WiFi setups, you'll encounter various authentication methods, each providing different security levels and management features. Some common methods include: 6A:FE:3B:73:18:FB -58 19 0 0 1 195 WPA2 CCMP MGT NameOfMyWifi EAP-GTC (Generic Token Card): This method supports hardware tokens and one-time passwords within EAP-PEAP. EAP-MD5 (Message Digest 5): Involves sending the MD5 hash of the password from the client. It's not recommended due to vulnerability to dictionary attacks, lack of server authentication, and inability to generate session-specific WEP keys. EAP-TLS (Transport Layer Security): Utilizes both client-side and server-side certificates for authentication and can dynamically generate user-based and session-based WEP keys for securing communications. EAP-TTLS (Tunneled Transport Layer Security): Provides mutual authentication through an encrypted tunnel, along with a method to derive dynamic, per-user, per-session WEP keys. It requires only server-side certificates, with clients using credentials. PEAP (Protected Extensible Authentication Protocol): Functions similarly to EAP by creating a TLS tunnel for protected communication. It allows the use of weaker authentication protocols on top of EAP due to the protection offered by the tunnel. PEAP-MSCHAPv2: Often referred to as PEAP, it combines the vulnerable MSCHAPv2 challenge/response mechanism with a protective TLS tunnel. #Protecting User Anonymity Identity hiding is supported by both EAP-PEAP and EAP-TTLS. In the context of a WiFi network, an EAP-Identity request is typically initiated by the access point (AP) during the association process. To ensure the protection of user anonymity, the response from the EAP client on the user's device contains only the essential information required for the initial RADIUS server to process the request.The utilization of pseudonymous identifiers is a common practice in RADIUS server configurations, often employing the user identifier "anonymous" for simplicity and convenience. In this setup, the initial RADIUS server acts as either an EAP-PEAP or EAP-TTLS server, managing the server-side protocol functionality. Wi-Fi networks often utilize ESSIDs and PNLs to streamline connections, but a lack of authentication to APs leaves them vulnerable. ================================== Stations store the wireless network's ESSID in their Preferred Network List (PNL) with configuration details. The PNL enables automatic connections to known networks, enhancing user experience through streamlined connection processes. Passive scanning APs broadcast beacon frames announcing their presence and features, including the ESSID unless broadcasting is disabled. Stations listen for these frames if they match an entry in the station's PNL. Attackers can exploit a device's PNL by mimicking a known network's ESSID, tricking it into connecting to a rogue AP. Active probing involves stations sending probe requests to discover nearby APs and their characteristics. Directed probe requests target specific ESIDs, detecting if a particular network is within range even if it's hidden. AP creation with redirection involves creating an AP and redirecting its traffic to an interface connected to the Internet. ---------- To create an AP, using ifconfig -a confirms the wlan interface is present. DHCP & DNS management can be achieved using apt-get install dnsmasq, configuring a file /etc/dnsmasq.conf with settings like dhcp-authoritative and server=8.8.8.8. IPs and routes are set using ifconfig wlan0 up 192.168.1.1 netmask 255.255.255.0 route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1, then starting dnsmasq. ---------- Evil twin attacks exploit the way WiFi clients recognize networks by using the network name (ESSID) without authenticating with the base station. Key points include difficulty in differentiation, client roaming and connection manipulation, and challenges in execution. Attackers can lure devices to disconnect from their current base station and connect to a rogue one by offering a stronger signal or disrupting the legitimate access point. ---------- Redirection and forwarding are achieved using iptables with MASQUERADE settings. A configuration file hostapd.conf is created for setting wireless network parameters like ssid, channel, and macaddr_acl. ---------- To mitigate evil twin attacks, devices must recognize the authenticity of networks beyond just ESSID matching. Regular security updates, monitoring network activity, and verifying authentication mechanisms can help prevent attacks.The art of creating evil twins has become a necessary skill for those who wish to test the security of wireless networks. By duplicating and manipulating access points, attackers can gain valuable insight into the network's defenses. ================================== In order to create an evil twin, one must first choose an airbase-ng or eaphammer tool. Airbase-ng is used to create a basic evil twin with limited capabilities, while eaphammer offers more advanced features such as WPA authentication and captive portals. Using eaphammer, you can create an evil twin using the "captive-portal" option. A very basic Open Evil Twin (no routing capabilities) can be created with the command: airbase-ng -a 00:09:5B:6F:64:1E --essid "Elroy" -c 1 wlan0mon Alternatively, you can use eaphammer to create an evil twin using the "captive-portal" option. The interface should not be in monitor mode when using this tool. One thing to note is that if the real access point is WPA protected, devices will not automatically connect to the open evil twin. However, you can try to do a Denial of Service (DoS) attack on the real AP and hope that the user connects to your open evil twin manually. Alternatively, you can DoS the real AP and use a WPA Evil Twin to capture the handshake. WPA/WPA2 Evil Twin Creating an evil twin using WPA/2 requires knowledge of the password used by the client device. If this information is not available, the connection will not be completed. Using eaphammer, you can create a WPA/EAP authentication Evil Twin using the command: ./eaphammer -i wlan0 -e exampleCorp -c 11 --creds --auth wpa-psk --wpa-passphrase "mywifipassword" Enterprise Evil Twin Creating an Enterprise Evil Twin requires knowledge of the network's configuration and authentication settings. This can be achieved using hostapd-wpe. Using hostapd-wpe, you can automate the generation of configurations using a Python script from a GitHub repository. The script takes parameters such as the victim device, PrivateSSID, channel, and user files. To intercept traffic, modify the hostapd-wpe configuration by changing the key exchange method from Diffie-Hellman (DH) to RSA. This can be done by editing the dh_file parameter in the /etc/hostapd-wpe/certs/dh file to point to a modified version of the RSA key. The Same Area: A Common Ground for Rogue Access Points ================================== You can use several of these best cmd commands for hacking to perform various tasks. Simply type in your desired command on the command prompt and execute it. ================================== lookin forward to seein everyone at teh meetin tomorow and discusin our strategis!!! leavin a coment bewe if yu want tu add enny comand tu teh liste!!! leev a coment bewe!!!!!!