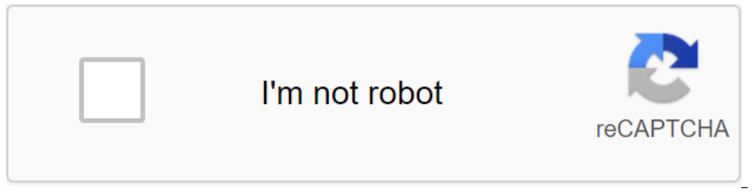

Continue

Certified ethical hacker notes pdf

Go to the contents It's a small (and I hope) useful crib for CEH V9 certification. 1. Introduction to the Ethical Basics of Hacking There are three main stages of the pen test: preparing an assessment of the conclusion What is the methodology of hacking? Intelligence cleaning tracks Black Box testing, the ethical hacker has absolutely no knowledge of TOE. It is designed to simulate an external, unknown attacker, taking the most time to complete. Testing the white box, pen testers have a full knowledge of the network, system and infrastructure they are targeting. The grey testing box is also known as partial knowledge testing. What distinguishes this from testing the black box is the estimated level of increased privileges that the tester has. While black box testing is usually conducted at network administration level, testing of a gray box only assumes that the attacker is an insider. Types of EC Council attacks broadly define four categories of attack types: Operating system attacks Generally, these attacks are aimed at a common error that many people make when installing operating systems - accepting and exiting all defaults. Things like administrator accounts without passwords, all ports remain open, and guest accounts (the list can go on forever) are examples of settings that the installer can forget. Attacks at the application level these are attacks on the actual application programming codes. While most people are very knowledgeable about protecting their OS and network, it's amazing how often they discount applications running on their OS and network. Many applications on the network are not checked for vulnerabilities within their creation and, as such, have many vulnerabilities built into them. Online apps are a goldmine for most hackers. Squeezing wrap the attack code These attacks take advantage of the built-in code and scripts the most finished applications come with. These scripts and code fragments are designed to simplify installation and administration, but can lead to vulnerabilities if not managed properly. Wrong Attacks These attacks use systems that are not intentionally or accidentally configured appropriately to ensure security. An asset is an object of economic value owned by an organization or an individual. Identifying assets in the world of risk analysis is the first and most important step. A threat is any agent, circumstance or situation that may cause harm or loss to an IT asset. Vulnerability is any weakness, such as software flaws or logical design, that can be exploited by the threat of harm to an asset. 18 U.S.C No. 1029 Basically, the law gives the U.S. government the power to prosecute criminals who use fake devices or use them. In short, the division criminalizes the misuse of any amount of credentials, including pass words, PINs, tokens credit card numbers, and the like. 18 U.S.C No. 1030 This law prosecutes criminals who use computers to access or misrepresent themselves as someone else. It's all about covering committing a crime using a computer or performing hacking activities without prior permission. Порты и протоколы Номера портов варьируются от 0 до 65 535 и разделены на три различные группы: Хорошо известно: 0-1023 Зарегистрировано: 1024-49151 Динамика: 49152-65535 Некоторые из наиболее важных известных портовых номеров, которые следует помнить: FTP (20/21) Telnet (23) SMTP (25) DNS (53/TCP - Зона Переводы 53/UDP - Запросы) Kerberos - 88 POP3 (110) NetBIOS (137-139) SNMP (161 - Управление /162 - Ловушки) LDAP - 389 CIFS/SMB Акции - 445 RADIUS/Diameter - 1812/1813 ISO/OSI слоев Применение - Презентация данных - Data Session - Data Transport - сегмент сети - пакет данных -кадры Физические - байты Все народы, кажется, нуждаются в обработке данных - мнемоническая фраза, чтобы помнить слои. PASSWORDs EC-Council rules for passwords: Password should not contain any part of a username. For example, the password KevinR0ck$! won't work on the CEH exam because you can clearly see my name there. The password must have at least eight characters. Eight is fine. Nine is better. Seven? Not very good. The password must contain symbols of at least three of the four main components of complexity, i.e. special characters (such as $), upper-register letters, lower-case letters, and numbers. U$e8Ch@rs all four, while use8chars only uses two. LM Hashing - 7 spaces hashed and AAD3B435B51404EE Attack Types Four main types of attack are defined in CEH. A passive online attack basically amounts to sniffing wires in the hope of either intercepting a password in clear text or attempting to play or a person in the middle of a (MITM) attack. active online, occurs when an attacker starts just trying passwords, guessing them, due to the lack of a better word in an offline attack occur when a hacker steals a copy of a password file (remember our discussion on the SAM file before?) and runs the effort of hacking on a separate system. non-electronic and social engineering. side-hijacking. The idea is to steal the cookies exchanged between the two systems and the ferret, which can be used as a playback style attack of physical human security based on the attacks dumpster diving impersonation Technical support shoulder surfing Tailgating and piggybacking computer phishing attacks. Three main categories of physical safety measures: Physical measures include anything you can touch, taste, smell, or get shocked. For example, lighting, locks, fences, and guards with Tasers are all physical measures. The technical measures are a little more com-plicated. These measures, taken with technology in mind, to protect clearly on Level. For example, for example and permissions may not come across as physical-ical measures, but if you think of them in the context of smart cards and bio-metrics, it's easy to see how they should become technical measures for physical safety. Operational measures are the policies and procedures you have created to ensure the security of an operation. 2. Trace and intelligence for ECCouncil Vulnerability Research is part of the intelligence. The difference in definition between intelligence and footprint: For many, intelligence is a more general, excessive term for gathering information about targets, while trail-ing is more effort to map out, at a high level, what the landscape looks like. They are interchangeable terms in the language of CEH, but if you just remember that the trail is part of the intelligence. DNS uses port 53; Search names usually use UDP, while transfer zones use TCP. DNS: SRV-Service records the name of the host and the port number of servers that provide certain services, such as the directory server. SOA - Start Of Authority This record identifies the primary name server for the zone. The SOA record contains the host name of the server responsible for all DNS entries in the namespace, as well as the main domain properties. PTR - IP Address Map pointer in the host's name (with the condition of reverse DNS search). You don't necessarily need a PTR record for every record in your DNS name space, but they're usually associated with email server records. NS - Name Server This entry identifies the name servers in your namespace. These servers are the ones that respond to your customers' requests to resolve names. MX-Mail Exchange This record identifies your email servers in your domain. CNAME - Canonical Name This record provides domain name aliases in your zone. For example, one IP address may have an FTP service and a web service. CNAME records can be used to list both in DNS for you. A - Address This entry displays the IP address in the owner's name, and is most commonly used for DNS searches. DNS Footprinting Tools: whois, nslookup, dig 3. Network scanning Seven common types of scanning for port scanning: TCP Connect passes through a full connection (three-part handshake) at all ports. The easiest to detect, but perhaps the most reliable. Open ports will respond to SYN/ACK, closed ports with RST/ACK. SYN, known as semi open scanning. Only SYN packages are sent to ports (no three-part handshake ever ends). Open ports will be met by SYN/ACK, closed ports with RST/ACK. FIN scans run the link setting in the opposite direction, sending a package with a set of FIN flags. Closed ports will respond to RST, while open ports will not respond at all. XMAS Christmas scan is named so because the package is sent with multiple flags (FIN, URG and PSH). ports will meet RST, while open ports will not respond to all ACK used mainly for Unix/Linux-based systems. Open ports will send RST, closed ports, unanswered IDLE uses a fake IP address to get port responses during scanning. Designed for stealth, this scan uses the SYN flag and tracks responses, as with syn scan. NULL is almost the opposite of XMAS scanning. NULL scans send packages without a set of flags. The answers will vary depending on the OS and version, but null scans are designed for Unix/Linux machines. Military set is the process by which the attacker dials a set of specified phone numbers - Calli is looking for an open modem. The MAC address that is burned on NIC actually consists of two sections. The first half of the address, 3 bytes (24 bits), is known as an organizational unique identifier and is used to identify the card manufacturer. The second half is a unique number burned in at the production to ensure no two cards on any subnet will have the same address. MAC Spoofing Set the NIC mac address at the same value as another MAC Flooding Overwhelm a CAM (reference memory content) of the switch table so that it is smearing in ARP Poisoning Inject mode incorrect information in the ARP caches of two or more endpoints. The ICMP Internet Governance Communications Protocol is a transportation protocol that creates message data that can be exchanged by network hosts to fix problems, report errors, and information. ICMP Headline Example: Type code Description 0 0 Echo Response 3 Appointments Unattainable 3 3 13 Administratively Prohibited 8 0 Echo Request 5 0 Redirect 11 0 Time Exceeded Don't Forget!! Type 3 Code 13 means administratively prohibited TCP: URG (Urgent) Headline flags When this flag is installed, it indicates that the data inside is sent out of the lane. ACK (Confirmation) This flag is installed as confirmation of SYN flags. This flag is installed on all segments after the original SYN flag. PSH (Push) This flag forces the delivery of data without worrying about any buffering. RST (Reboot) This flag causes the communication to be terminated (in both directions). SYN (synchronization) This flag is installed during the initial creation of the link. It points to the alignment of the parameters and sequence numbers. FIN (Finish) This flag means ordering close to communications. Response type: FIN Scan - No Answer - Open Port RST /ACK - Closed Port XMAS Scan - No Answer - Open Port RST / ACK - Closed Port NULL Scan - No Answer - Open Port RST /ACK - Close Port NMAP Nmap is a de facto tool for trail networks. It is able to find living hosts, access points, fingerprinting of operating systems and verification services. It also has возможности для уклонения от IDS. nmap <scan options=> <target>Wireshark фильтры отображения фильтры работают в основном как: proto.field оператора значение Анализ следующих примеров: tcp.flags - 0x29 ip.addr</target> </scan> </scan> 192.168.1 tcp.port eq 25 or icmp ip.src-192.168.0.0/16 and ip.dst'192.168.0.0/16 http.request.uri corresponds to login.html Tcpdump syntax: tcmdump (flags) interface 4. The SNMP simple network management protocol was designed to manage IP-enabled devices on the network. As a result, if it's used in the subnet, you can learn a lot of information from properly formatted SNMP queries. Later versions of SNMP make it a little more difficult, but a lot of systems out there still use protocol in version 1. 5. Hacking System 6. Malware Threats Trojans and other Windows attacks will automatically run everything that is found in Run, RunServices, RunOnce, and RunServicesOnce Virus Types: Boot sector virus is also known as a system virus,

this type of virus actually moves the boot sector to another location on the hard drive, forcing the virus code to be performed in the first place. It is almost impossible to get rid of them once you become infected. You can create a boot recording of an old school fdisk or mbr can do the trick for you, but it's not necessarily a walk in the park. RootKit A rootkit is a type of program often used to hide utilities in a compromised system. Usually works at the core or library level. It takes a reimage of the famous good media to remove. The Shell virus works just like the boot sector virus, this type of virus wraps itself around the app code by inserting its own code in front of the app. Every time the app is launched, the virus code works first. The multiparty virus tries to infect both the files and the download sector at the same time. This usually refers to a virus with multiple vectors. . A macrovirus commonly written with VBA (Visual Basic for applications), this type of virus infects template files created by Microsoft Office, usually Word and Excel. Melissa's virus was a prime example of that. Polymorphic code virus This virus mutates its code with a built-in polymorphic engine. These viruses are very difficult to find and remove because their signatures are constantly changing. Metamorphic virus This type of virus rewrites itself every time it infects a new file. DOS Types of Attacks: SYN Attack Hacker will send thousands and thousands of SYN packages to the machine with a false source IP address. The machine will try to answer SYN/ACK, but will be unsuccessful (because the address is false). Eventually, all the resources the machine is engaged in and it becomes a giant press paper. SYN Flood In this attack, the hacker sends thousands of SYN packages to the target, but never responds to any of the SYN/ACK return packages. Since there is a certain amount of time, the goal has to wait to get an answer to SYN/ACK, it will eventually bog down and run out of available connections. ICMP Floods Here, Attacker Sends ICMP Echo Packages to Target With (fake) source source The target continues to respond to an address that does not exist, and eventually reaches the limit of packages sent per second. The level of the application is a simple attack in which a hacker simply sends more legitimate traffic to a web application than he can handle, causing the system to collapse. Smurf Attacker sends a large number of pings to the subnet broadcast address, with the original IP forged to the target address. Then the entire subnet will start sending answers to target targets, draining resources. The fraggle attack is similar, but uses UDP for the same purpose. Ping death in ping death, attacker snippets ICMP message to send targets. When the fragments are collected, the ICMP package is larger than the maximum size and cuts the system. 7. Sniff 8. Social Engineering Types social engineers Insider Associates have limited authorized access, and escalate privileges from there. Insider Partners insiders by virtue of affiliation, they deceive the identity of the insider. Outsider Partners are nonтtrusted who use an access point that has been left open. Physical Safety 9. Denial of service 10. Session Hijacking 11. Hacking web servers web hacking This point-slash attack point (bypass catalog) is also known as a Unicode variant or unverified input attack. 12. Hacking Web Apps 13. The types of injectable attacks S'L Injection S'L: Union query Thought here is to use the UNION command to bring back the alliance of your target database with the one you created to steal data from it. Tautology is too complex a term used to describe the behavior of a database system when deciding whether a claim is true. Because custom documents and passwords are often compared, and the true measure allows you to gain access, if you cheat the database by providing what is already true (1 does, indeed equal to 1), then you can sneak past. Blind injection S'L This occurs when the attacker knows that the database is subject to injections, but error messages and screen returns are not returned to the attacker. Because there are a lot of guesses and trial and error, this attack takes a long time to take down. Error-based injections S'L It is not necessarily an attack as much as the method of listing. The goal is to intentionally enter poorly built operators to force the database to respond with table names and other information in their error messages. Buffer Attack Categories are as follows: Stack This idea comes from the basic premise that all program calls are stored in the stack and run in order. If you're affecting a buffer overflow stack, you might want to change the function pointer or variable to ensure that the code is running. The pile is also called overflow heaps, this attack uses memory on top an application that dynamically stands out while running. Because this memory typically contains these programs, you can force the app to rewrite function pointers. Nop Sani NOP Sleigh uses a machine instruction called a non-op. In an attack, the hacker sends a large number of NOP instructions to the buffer, snuupling the command code instructions at the end. Because this attack is so common, most IDS protect against it. Dangerous functions for overflowing the buffer The following functions are dangerous because they do not check the size of the destination buffers: receives () a strcat () printf () 14. Hacking Wireless Networks Wireless Network Hacking 802.11 Spec Distance Speed Freq 802.11a 30M 54Mbps 5Ghz 802.11b 100M 11Mbps 2.4Ghz 802.11g 100M 54Mb 54Mbps2.4Ghz 802.11n 125M 100Mbps 2.4Ghz, 5Ghz WEP uses RC4 for stream cipher with 24b vector initialization Key sizes 40b or 104b WPA uses RC4 for thread cipher, But supports longer keys. The 48-bit IV WPA/TKIP changes the IV with each frame and includes a key mixing WPA2 uses AES as a flow cipher and includes all TKIP functions; 48 bit IV. Rogue APs (evil twins) can also be used as a wrong attack association. 15. Hacking mobile Bluetooth attack platforms : Bluesmacking is simply a denial of service attack on the device. Bluejacking consists of sending unwanted messages to and from mobile devices. Bluesniffing is exactly what it sounds like, and finally. Bluescarfing is the actual theft of data from a mobile device. War driving is used to refer to, literally, driving around in a car, 35mph or less, looking for open access points. In the ethical field of hacking, it still points to the search for open WAP 16. Dodging IDS, Firewalls and Honeypots Snort Rule: Warning tcp ! HOME_NET any $HOME-NET 31337 (msg :BACKDOOR ATTEMPT-Backorifice) If you happen to come across a package from any address that is not my home network, using any original port intended for address in my home network at port 31337, alert me to BACKDOOR-ATTEMPT-Back-back orifice. The Port of Span is a port that reflects a false negative when IDS reports a particular stream as pure, but it's not 17. NIST Cloud Computing Reference Cloud Consumer - A person or organization that uses Cloud Provider Cloud Computing Services - Person or Organization providing cloud carrier- Intermediary services to provide communications and transportation services between cloud consumers and Cloud Auditor providers - a party to conduct an independent assessment of cloud services management and acceptance of the cloud broker, an organization that manages cloud services in terms of cloud services in terms of performance and delivery. 18. Cryptography symmetrical encryption - - to calculate the number of key pairs you will need N (N - 1) / 2, where N is the number of nodes in the network of symmetrical algorithms: DES block is a cipher that uses a 56-bit key (with 8 bits reserved for parity); Fixed locked size. A 3DES block cipher that uses a 168-bit key. 3DES (called triple DES) can use up to three keys in the multiple encryption method. AES (Advanced Encryption Standard) is a block cipher that uses key lengths of 128, 192 or 256 bits, and effectively replaces DES. IDEA (International Data Encryption Algorithm) is a block cipher that uses a 128-bit key. A two-fish block is a cipher that uses key size up to 256 bits. Blowfish Is a Fast Block cipher, largely replaced by AES, using a 64-bit block size and a key of 32 to 448 bits. RC (Rivest Cipher) includes several versions from RC2 to RC6. A block cipher that uses a variable key length of up to 2040 bits. The RC6, the latest version, uses 128-bit blocks, while the RC5 uses variable block sizes (32, 64 or 128). Asymmetric encryption As a rule: public key - encryption, private key - decryption. Asymmetrical Algorithms: Diffie-Hellman, designed for use as a key exchange protocol, Diffie-Hellman is used in Secure Sockets Layer (SSL) and IPSec encryption. Elliptic Curve Cryptosystem (ECC) uses dots on the elliptical curve, combined with logarithic problems, for encryption and signatures. Uses less computing power than other methods, making it a good choice for mobile devices. El Gamal is not based on factoring in a simple number, this method uses the solution of discrete logarithm problems for encryption and digital signatures. RSA Is an Algorithm that achieves strong encryption using two large simple numbers. Factoring these numbers creates key sizes of up to 4,096 bits. RSA can be used for encryption and digital signatures and is a modern de facto standard. Hash algorithms: MD5 (Message Digest Algorithm) produces a 128-bit hash output expressed as a 32-digit hexagonal. Sha-1, developed by the NSA (National Security Agency), SHA-1 produces a 160-bit product value, and was required by law for use in U.S. government applications. The SHA-2, developed by the NSA, actually contains four separate hash functions that produce outputs of 224, 256, 384 and 512 bits. Trust Models web trust, several organizations sign certificates for each other. a single system of authority has a CA at the top, which creates and issues certificates. Users trust each other based on ca itself. The hierarchical trust system also has a CA at the top (which is known as the CA root) but uses one or more intermediate CAs under it - known as (RAs) - to issue and manage certificates. Cryptographic Attacks: The known simple text attack In this attack, the hacker has both simple and relevant encryption messages - the more the better. Copies of the simple texst are scanned for repetitive sequences that then compared to cipher versions. Over time, and with effort, it can be used to decipher the key. Ciphertext-only attack In this attack, the hacker receives copies of several messages encrypted in the same way (with the same algorithm). Statistical analysis can be used to identify, ultimately, repetitive code that can be used to decode messages later. A replay of an attack is most often performed in the context of a man in the middle attack. The hacker repeats part of the cryptographic exchange in the hope of deceiving the system into creating a communication channel. The attacker really doesn't need to know the actual data (such as the password) being exchanged, he just has to get the right time in copying and then play a bit of flow. Session tokens can be used in communication to combat this attack. A digital certificate is an electronic file that is used to verify a user's identity, ensuring a waiver throughout the system. This determines the certificate format. The most common version is 1. The serial number is quite self-evident, the serial number is used for unambiguous identification of the certificate itself. Subject Whoever or what is currently defined by the certificate. The ID algorithm (or signature algorithm) shows the algorithm that was used to create a digital signature. The issuer shows the entity that verifies the authenticity of the certificate. The issuer is the one who creates the certificates. Valid from and valid for these fields show the date of the certificate well through. Key exhibitions use for what purpose the certificate was created. The public key of the subject's copy of the subject's public key is included in the digital certificate. Additional fields These fields include a unique issuer ID, an alternative subject name and extension. Extensions. certified ethical hacker notes pdf. certified ethical hacker course notes