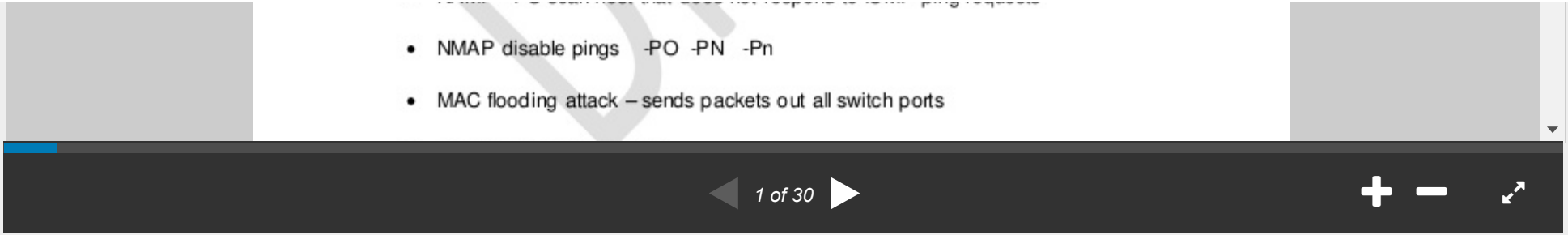
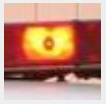
Dave Sweigert's CEH Cheat Sheet

- WPA2 supports AES - AES is a block cipher
- Hybrid password attack – p@ssw0d
- NMAP –O = protocol scan
- In a MitM attack, attack provides his PUBLIC key to victim
- Cain and Able (not Jack the Ripper) can crack Cisco VPN passwords and can Record and Extract VoiP conversation
- Employees sign user policies to PROTECT COMPANY.
- OWASP maintains WebGoat
- 802.1x = EAP
- Fget() for C is library bounds checking
- Nessus 5.2 drop down – Database Compliance Checks and Global Variable Settings
- BlueTooth utilizes pi/4-DQPSK and 8DPSK
- NAMP –PO scan host that does not respond to ICMP ping requests



Certified Ethical Hacker quick test prep cheat sheet



David Sweigert, Defensive cyber security expert
+ Follow

Published on Jan 26, 2017

Uploaded as a courtesy by:

Dave Sweigert

CISA, CISSP, HCISPP,

...

Published in: Internet

Share your thoughts…

Post

katekoxx

Hey guys! Who wants to chat with me? More photos with me here ☞ http://www.bit.ly/katekoxx

1 year ago

Certified Ethical Hacker quick test prep cheat sheet

1. Dave Sweigert's CEH Cheat Sheet ¬ WPA2 supports AES - AES is a block cipher ¬ Hybrid password attack – p@ssw0d ¬ NMAP –O = protocol scan ¬ In a MitM attack, attack provides his PUBLIC key to victim ¬ Cain and Able (not Jack the Ripper) can crack Cisco VPN passwords and can Record and Extract VoiP conversation ¬ Employees sign user policies to PROTECT COMPANY. ¬ OWASP maintains WebGoat ¬ 802.1x = EAP ¬ Fget() for C is library bounds checking ¬ Nessus 5.2 drop down – Database Compliance Checks and Global Variable Settings ¬ BlueTooth utilizes pi/4-DQPSK and 8DPSK ¬ NAMP –PO scan host that does not respond to ICMP ping requests ¬ NMAP disable pings -PO -PN -Pn ¬ MAC flooding attack – sends packets out all switch ports ¬ Kismet used to scan WiFi ¬ Social engineering is phishing ¬ Common Criteria ST – docs for system about to be tested ¬ Interrupt – signal indicates event has taken place ¬ NMAP –sO protocol scan

2. ¬ NMAP sS half open scan ¬ NMAP –sT TCP connect scan ¬ Determine broadcast address – look for .127/25 ¬ Upon SSL session set-up, symmetric key exchanged ¬ Retinal scan most likely to reveal private health information ¬ MSFT LM uses DES ¬ AES is a block cipher ¬ WinServer 2012 sc_query displays active sessions ¬ XSS designed to harvest cookies on victims machine ¬ Privilege escalation – bypassing security with flaw in application ¬ BGP is a routing protocol ¬ 802.11 = WPA2 ¬ NMAP –PO scans hosts that do not respond to ICMP ping commands ¬ HPING2 null TCP pings (behind packet filter) ¬ NMAP –sO protocol scan ¬ PCI DSS req. 11 - Requires security testing of systems ¬ To start NMAP NSE –sC -A ¬ UDP Port 514 = syslog ¬ Single quote " ' " denotes SQL character string ¬ NSLOOKUP –HINFO can give you CPU TYPE and OS TYPE

3. ¬ Hping2 will create an ICMP or UDP packet. Hping2 –c 5 -1 10.10.10.10 will specify an ICMP packet (-1).

4. ¬ Active sniffing involves attaching to a switch (not a hub). Active sniffing attacks a switch so that it will broadcast all packets out all ports. One type of active sniffing attack involves a CAM buffer overflow. Passive sniffing attacks usually occur on HUB centric networks. ¬ PCAP is used by NMAP, SNORT and TCPDUMP. Libcap is a version of PCAP written in C/C++. ¬ NMAP commands ¬ XSS is a programming code attack that is used to harvest cookies. ¬ What phase is a fuzzy test performed? MSFT Security Development Lifecycle. MSFT SDL. Fuzz testing involves

entering random malformed data as input so developers can discover how an application responds to garbage data. ¬ Anomaly based IDS is the best for detecting threats. ¬ Proxy servers make it almost IMPOSSIBLE to block future attacks. ¬ Dumpster diving and phishing attacks are considered social engineering.

5. ¬ Risk assessment – evaluating vulnerabilities. ¬ BGP is a routing protocol. ¬ A brute force attack usually relies upon a rainbow table. ¬ Common Criteria ST are documents for system about to be tested. ¬ XSS can be used to exploit a web application. ¬ N-tier architecture allows each tier to operate independently of others. Each tier consists of a single role or function. N tier is not limited to three layers. ¬ NET command at Windows prompt. You CAN NOT add a route, configure the firewall with the NET command. You can Manage Services, Connect to a Remote Resource, Manage user Accounts, Manage Shared Resources, and Manage a Printer Queue. ¬ AVAILABILITY is not provided by cryptography. ¬ IEEE 802.1X defines EAP. Extensible Authentication Protocol.

6. ¬ A Biometric Pass Port is something you have. A biometric passport is a physical object. ¬ OSSTMM process controls. Non-Repudiation, Confidentiality, and Alarm. ¬ ISO 27002 recommends security controls based upon industry best practices. ¬ AES is a block cipher. ¬ 192.168.127/25 is a broadcast address. ¬ Google hacks: intitle , intext , inurl , site , cache ¬ If UDP TCP Port 53 is blocked by firewall you will be able to access servers by THEIR IP address and not by their names. ¬ SHA-1 creates a 160-bit hash value. ¬ Steps to take to create an encrypted message: Create hash of message body, Encrypt hash using your private key. Encrypt message using recipient's public key. ¬ 2,048 is the modulus size for Diffie Hellman group 14. ¬ USBDumper: silently copies files from a USB drive to a computer. ¬ PPTP and L2TP operate at the Data Link Layer (DLL). ¬ NTP (timing) uses Port 123 ¬ MSFT Security Development Life Cycle

7. ¬ Nmap –s) 10.10.10.10 protocol scan. ¬ For banner gathering use HEAD / HTTP/1.0 ¬ The following are scripting languages: PERL, PYTHON and RUBY.

8. ¬ Computer configured with wrong gateway address. ¬ A false negative occurs when an IDS or IPS does not identify malicious traffic. A false positive occurs when false malicious traffic is identified (harmless traffic). ¬ A guard dog seen outside an exterior door is a physical deterrent control.

9. ¬ HPING2 can be run from an Win XP host. HPING2 does not rely on ICMP packets. You can use the -0 or –rawip parameters to create packets. ¬ In OSSTMM confidentiality ensures that only participants have knowledge of an asset. ¬ Two types of malware that can spread without human interaction: a WORM and a BOT. A worm can self-propagate. A malicious bot can also self-propagate. ¬ The Netcat –e flag configures Netcat to launch a program after connection is established with a Windows host. The –l and –L parameters allow for Netcat to accept inbound connections.

10. ¬ Session splicing attempts to evade a signature-based IDS. Uses fragmentation to evade signature=based IDS. ¬ LM passwords at 7 characters or below will always result in a hash ending in 1404EE. 7 and below. ¬ A birthday attack attempts to find two passwords with matching hashes. Birthday paradox, a group of 23 people having two people with same birthday is 22 in 365 odds, 6%. ¬ A scripting language requires an interpreter. ¬ TFTP uses UDP port 69 by default. ¬ SoX was created to require companies to properly disclose financial statements. ¬ In a brute force attack ALL combinations of letter, numbers, and symbols are used. ¬ In a SYN flood attack, the target host is left waiting for an ACK segment.

11. ¬ Use IKE-SCAN to fingerprint VPN servers. ¬ IPsec is a group of protocols rather than a single protocol. ¬ As the diagram on the right shows, there are three main protocols that are used by IPsec: IKE, AH and ESP. IKE provides authentication and key exchange, and AH and ESP are used to send the data over the VPN connection. Some old implementations used "manual IPsec" connections which did not require the use of IKE. However, these are now obsolete and all modern IPsec systems will use IKE. Of these three protocols, IKE is by far the most complex. In this document we are only concerned with the IKE protocol, so we will not cover AH or ESP any further. ¬ The use of IKE to authenticate and exchange key material for an ESP or AH connection is a two-phase process. Phase-1 authenticates the peers and establishes a secure channel (called an IKE SA) for Phase-2, which negotiates the IPsec mode and establishes a secure channel for the AH or ESP traffic called an IPsec SA.
12. ¬ Primary benefit of a signature matching IDS: they have a low false positive rate.
13. ¬ The maximum length of an LM password is 14 characters. All LM passwords are 14 characters. ¬ MD5 creates a 128-bit hash value based on variable length plain text. ¬ A fragmentation attack is designed to defeat an IDS. ¬ A false positive is when the IPS blocks normal Web traffic. ¬ IPSec provides data encryption and authentication. ¬ CAIN & ABEL can perform all of the following: Capture and decrypt RDP traffic Detect 802.11 WLANs Collect server certificates and prepare them for a MitM Start, stop, pause, continue and remove Windows services Crack CISCO VPN client passwords Record and extract VOIP conversations
14. Cain's Features Here's a list of all of Cain's features that make it a great tool for network penetration testing: Protected Storage Password Manager Credential Manager Password Decoder LSA Secrets Dumper Dialup Password Decoder Service Manager APR (ARP Poison Routing) Route Table Manager Network Enumerator SID Scanner Remote Registry Sniffer Routing Protocol Monitors Full RDP sessions sniffer for APR Full SSH-1 sessions sniffer for APR Full HTTPS sessions sniffer for APR Full FTPS sessions sniffer for APR Full POP3S sessions sniffer for APR Full IMAPS sessions sniffer for APR Full LDAPS sessions sniffer for APR Certificates Collector MAC Address Scanner with OUI fingerprint Promiscuous-mode Scanner Wireless Scanner PWL Cached Password Decoder 802.11 Capture Files Decoder Password Crackers Access (9x/2000/XP) Database Passwords Decoder Cryptanalysis attacks Base64 Password Decoder WEP Cracker Cisco Type-7 Password Decoder Rainbowcrack-online client Cisco VPN Client Password Decoder Enterprise Manager Password Decoder RSA SecurID Token Calculator Hash Calculator TCP/UDP Table Viewer TCP/UDP/ICMP Traceroute Cisco Config Downloader/Uploader (SNMP/TFTP) Box Revealer Wireless Zero Configuration Password Dumper Remote Desktop Password Decoder MSCACHE Hashes Dumper MySQL Password Extractor Microsoft SQL Server 2000 Password Extractor Oracle Password Extractor VNC Password Decoder Syskey Decoder ¬ Windows is the most difficult O/S to collect 802.11 packets in monitor mode. ¬ Message Integrity Check (MIC) is a feature of WPA that protects against MitM attacks.
15. ¬ In the N-tier implementation, at least three tiers must exist. ¬ These are social engineering attacks: phishing, dumpster diving, tailgating, shoulder surfing.
16. ¬ SNORT rules: PASS, DROP, ALERT, LOG
17. ¬ COBIT categories security standards and control objectives and domains. ¬ A trap door is the same as a back door. A trap door is a secret entry into an application. ¬ A MAC flood attack is characterized as the same as a CAM table attack. A MAC flooding attack floods the switch. ¬

Nmap –sS 10.-2.9.0- = Namp will perform a stealth scan on the 10.0.9.0/24, 10.1.9.0/24, and 10.2.9.0/24 networks. ¬ -sS option indicates a stealth scan. ¬ A fragmentation attack is designed to avoid an IDS.

18. ¬ In WPAConcealed Carry Reciprocity Act of 2017helps protect against MitM, Message Integrity Check. ¬ NMAP –A does NOT activate ping scanning. It DOES activate traceroute, script scanning, OS fingerprinting, version detection. ¬ Installing a firewall that blocks certain ports is a preventive control. ¬ Controls are: Directive, Deterrent, Preventive, Compensating, Detective, Corrective, Recovery. ¬ To display SMB traffic in Wireshark, use tcp.port == 445 or udp.port == 445 ¬ MD5 creates a 128-bit hash value based on a variable length plain text. ¬ OSSTMM provides compliance types as legislative, contractual, and standards- based. ¬ The use of DES by LM and adds blank spaces to passwords under 14 characters. The two separate character strings are hashed separately, hence 1404EE. ¬ According to NIST 800-30, which risk assessment steps can take place at the same time: Impact Analysis, Threat Identification, Vulnerability Identification, and Control Analysis.

19. ¬ The OSSTMM control that provides protection from loss and damages = indemnification. ¬ To initiate a netcat connection on port 12345 to 10.10.10.10 = nc 10.10.10.10 12345 ¬ RSA is very susceptible to chosen ciphertext attacks. In a chosen-ciphertext attack, the attacker is assumed to have a way to trick someone who knows the secret key into decrypting arbitrary message blocks and tell him the result. The attacker can choose some arbitrary nonsense as an "encrypted message" and ask to see the (usually) different nonsense it decrypts to, and he can do this a number of times. Having this capability obviously already allows the attacker to read an intercepted message, since he can just ask to have it decrypted. But in this attack his goal is

20. more ambitious than that: he wants to deduce what the secret key is, such that he can encrypt messages himself, and also keep decrypting after his access to having things decrypted for him vanishes. The attack is successful if if an attacker has a significant chance of being able to deduce the key after having "relatively few" blocks decrypted and without doing so much work himself that he could just as well have brute-forced it. The term "chosen-ciphertext attack" does not in itself say anything about how the attacker chooses the nonsense blocks he asks to have decrypted, or what kind of computations he does in order to recover the key from the responses. ¬ Best way to display all active and inactive sessions on a Windows 2012 server = sc query state = all ¬ Best way to display all devices on 10.10.10.10/24 on Wireshark is = ip.src == 10.10.10.10/24 and ip.dst == 10.10.10.10/24 ¬ An interpreter is required by a scripting language

21. ¬ Which algorithms are asymmetric? ¬ What does a birthday attack attempt to accomplish ? A birthday attack isa type of cryptographicattack that exploitsthe mathematics behindthe birthdayproblem inprobabilitytheory.Thisattackcan be usedto abuse communication betweentwoormore parties.The attack dependsonthe higherlikelihoodof collisions found betweenrandomattackattemptsanda fixeddegree of permutations(pigeonholes). ¬ IKE scan is used to fingerprint VPN servers.

22. ike-scan(1) - Linux man page Name ike-scan - Discover and fingerprint IKE hosts (IPsec VPN servers) Synopsis ike-scan [options] [hosts...] Target hosts must be specified on the command line unless the --file option is specified. Description ike-scan discovers IKE hosts and can also fingerprint them using the retransmission backoff pattern. ike-scan does two things: 1. Discovery: Determine which hosts are running IKE. This is done by displaying those hosts which respond to the IKE requests sent by ike-scan. 2. Fingerprinting: Determine which IKE implementation the

hosts are using. There are several ways to do this: (a) Backoff fingerprinting - recording the times of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns; (b) vendor id fingerprinting - matching the vendor-specific vendor IDs against known vendor ID patterns; and (c) proprietary notify message codes.

23. ¬ HINFO configures DNS records. ¬ A (address) Maps a host name to an IP address. When a computer has multiple adapter cards or IP addresses, or both, it should have multiple address records. ¬ CNAME (canonical name) Sets an alias for a host name. For example, using this record, zeta.microsoft.com can have an alias as www.microsoft.com. ¬ MX (mail exchange) Specifies a mail exchange server for the domain, which allows mail to be delivered to the correct mail servers in the domain. ¬ NS (name server) Specifies a name server for the domain, which allows DNS lookups within various zones. Each primary and secondary name server should be declared through this record. ¬ PTR (pointer) Creates a pointer that maps an IP address to a host name for reverse lookups. ¬ SOA (start of authority) Declares the host that's the most authoritative for the zone and, as such, is the best source of DNS information for the zone. Each zone file must have an SOA record (which is created automatically when you add a zone). ¬ STREAM ciphers are typically faster than block ciphers. ¬ A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time. ¬ A block cipher encrypts one block at a time. The block may be of size one byte or more or less. That means we can also encrypt a block of one byte by help of a stream cipher as a stream. ¬ NMAP –sS initiates a half-open scan.

24. ¬ Common Criteria has 7 EAL ratings.

25. ¬ A Network IDS (NIDS) is connected in promiscuous mode and resets TCP connections when a SYN flood is detected. ¬ TFTP uses port 69. ¬ Under XOR gate calculations. ¬ A false positive occurs when the firewall blocks legitimate traffic. ¬ A multi-partite virus will infect the boot sector and various files and programs (beware of only the boot sector answer). ¬ Sparse infector viruses infect files only when a specific condition is met.

26. In order to spread widely, a virus must attempt to avoid detection. To minimize the probability of its being discovered a virus could use any number of different techniques. It might, for example, only infect every 20th time a file is executed; it might only infect files whose lengths are within narrowly defined ranges or whose names begin with letters in a certain range of the alphabet. There are many other possibilities. ¬ Spacefiller (cavity) viruses Many viruses take the easy way out when infecting files; they simply attach themselves to the end of the file and then change the start of the program so that it first points to the virus and then to the actualprogram code. Many viruses that do this also implement some stealth techniques so you don't see the increase in file length when the virus is active in memory. ¬ Multipartite viruses Multipartite viruses are distributed through infected media and usually hide in the memory. Gradually, the virus moves to the boot sector of the hard drive and infects executable files on the hard drive and later across the computer system. ¬

27. APPENDIX How does the new bug Shellshock work 1. The hackers can force a computer running Bash to set specially crafted variables. 2. These would allow them to run programs on other people’s devices. 3. Shellshock particularly infects OS X Macs, PCs, routers, modems, servers and websites. 4. The hackers may steel your sensitive information like bank account passwords, credit card passwords and other financial details., if an online shopping or a banking webpage is infected. 5. Experts take its vulnerability as dangerous as “heartbleed” a new virus discovered earlier

this year. 6. Some experts take it much more dangerous, than “heartbleed” because it provides direct access to the computer system to the cyber criminals whereas “heartbleed” only enables the hackers to extract data from the infected system. 7. It is linked with processing of environmental variables and may affect the behavior of software. 8. It can be used to attacks millions of computers including government machines. 9. The security “patches” created so far are incomplete and are not capable of providing full system protection.

28. WireShark autofill ip.addr == tcp.port==80 eth.addr==

Download Ceh v9 Syllabus and Courseware PDF

Mercury Solutions Limited

Pass4sure 312-49v8 Questions and Answers

HazelLWoodring

Pass Eccouncil CHFI 312-49v8 Exam 2016

LuisMatthews

CEHV9

Nityanand Thakur

312 50v9 exam practice

p4sco

Cyber Security Risk Assessment Awareness for Emergency Managers

David Sweigert