ethical hacking quizzes

Study online at https://quizlet.com/_asvs2m

1. **According to SySS, which of these should you do if you want to carry out ethical penetration tests?**

   Notify your client of any risks or potential negative outcomes that might arise as a result of testing.

2. **Which of these potential parts of a penetration test report is of most value to a customer?**

   The executive summary that identifies the company's security posture and discusses how to improve it.

3. **In the Florida Computer Crimes Act, which of these terms is undefined?**

   Authorization

4. **What is the point of the General Data Protection Regulation?**

   To ensure that the personal data of users of computer services is not disclosed without permission.

5. **Which of these commands must be implemented as a shell builtin in order to exhibit the right behavior?**

   cd

6. **What work is likely based, in part, on Johnny Long's Google Hacking for Penetration Testers?**

   The document Untangling the Web: a Guide to Internet Research.

7. **What key element of James Comey's comments about his instagram account at the National Security Alliance Dinner led to Ashley Feinberg identifying his twitter account?**

   He said he had about nine followers, all relatives or close friends.

8. **Which of these could be the netmask for the network whose IP address is 255.255.64.0?**

   255.255.192.0

9.	**What does a dig request for record type AXFR achieve?**	Zone transfer if its supported.
10.	**What kind of dns lookup does fierce use in order to get a name server that won't provide zone transfer to reveal a host name that's not in the fierce wordlist?**	Reverse lookup.
11.	**Which of these is not a layer in the OSI networking model?**	Protocol
12.	**If, in starting a TCP connection, host X sends a SYN packet to host Y with sequence number A, what will be true of a correct response by host Y?**	It will have SYN and ACK set and the sequence number will be chosen randomly.
13.	**What is the number of bits in UDP port?**	16
14.	**What do the last 3 octets of a MAC address identify?**	The specific device ID.
15.	**How does nmap determine that a port is closed?**	It gets a RST response to a SYN packet
16.	**What organization is responsible for issuing internet RFCs?**	The IETF.
17.	**How does ASLR help preserve program control-flow integrity**	It makes it hard to identify the addresses of values written in the stack.
18.	**When do you set a payload in the metasploit framework?**	After you use an exploit.
19.	**Which of these malware artifacts did not use the vulnerability identified in MS08-067?**	Eternal Blue.

20.	**What register is used to hold the base- or frame-pointer in the X64 architecture**	rbp.
21.	**If I see a file with permissions -rwxrwxr-x+, which of these statements must be true?**	The file has an access control list (ACL).
22.	**Which of these is true about the RockYou password breach?**	The passwords were stored in plain text.
23.	**Which of these is most likely to keep a penetration tester from being able to guess passwords through SMB on a particular machine?**	Closing ports 139 and 445 with the machine's local firewall.
24.	**What did I report as the most common length for a password in the Have I Been Pwned password list?**	9
25.	**The Zack Attack can also be described as an**	NTLM relay attack.
26.	**Which of these was not a vulnerability of LDAP(S) session signing?**	The relayer could use its NetBIOS computer name in relayed messages.
27.	**If you want to get a Kerberos server long term key, which type of encryption should be enforced?**	RC4
28.	**How can an attacker exploit the following unquoted service path?** **C:\Program Files\Printer Software\EpsonDriver.exe**	By doing what either of the other two answers says. (By storing Program.exe in "C:\". By storing Printer.exe in C:\Program Files".)
29.		

	Which of these commands will allow you to communicate with a web server on the host targetmachine.com?	nc targetmachine.com 80
30.	**If I am in a meterpreter session and issue the following command portfwd add -l 8000 -p 445 -r 172.30.0.96 which of these things can I do?**	Connect to the service provided on port 445 by 172.30.0.96 by connecting to localhost port 8000.
31.	**Which of these is not an underlying approach to malware detection?**	Pessimistic detection.
32.	**Why might it be preferable to use a powershell payload rather than a native .exe file payload?**	The powershell payload need never be stored in the filesystem.
33.	**Which of these can be a security principal?**	A user account.
34.	**Which of these integrity levels is used by Internet Explorer in protected-mode?**	Low.
35.	**Where was the AES-encrypted Microsoft Local Administrator password stored for distribution (until some time after 2014)?**	In the SYSVOL directory on the domain controller.
36.	**What account executes sethc.exe when 5 successive shift key press event occur before login?**	NT AUTHORITY/System.
37.	**Which of these is not true about carrying a successful stealthy arpspoof campaign?**	We must be running a web server on port 80.
38.	**Which of these must be done in order to run SSLStrip?**	Enable IP forwarding.
39.	**Which of the following is true of HSTS super-cookies?**	They cannot be removed from a

		compliant browser by using any browser function available to the user.
40.	**Which of these is true of ssh?**	Any password sniffing attack requires the attacker to have the server public key.
41.	**Which of these steps to enable telnet service for a user is not necessary on a Windows host?**	Ensure that you have opened port 22 in the firewall.
42.	**What does WPAD do?**	Provides automatic configuration for Windows browsers.
43.	**Which of these Shadow Brokers exploits was not used by WannaCry?**	Extrabacon
44.	**Why did Linus Torvalds' remove the patch that addressed the problem underlying Dirty Cow in around 2007?**	It caused problems for IBM S390 machines.
45.	**Which of these is true of the popular exploitdb exploit for DirtyCOW?**	After using it, the system is unstable and may crash.
46.	**Which of these is a Linux kernel vulnerability?**	Linux eBPF privilege Escalation.
47.	**What is a canonical representation?**	One that is given by a formal rule
48.	**What is true of an idempotent command?**	Applying the command more than

		once will yield the same result.
49.	**Which of these methods of authentication is most often encountered in web applications?**	Form-based authentication.
50.	**Which of the following is not a reason to use a web proxy?**	To reduce the number of web hosts in the path between a client and server on the first download of a page.
51.	**Which of these types of authentication is susceptible to a MITM downgrade attack but not direct password capture?**	Digest Authentication
52.	**Which of these is the worst idea to use if you want to avoid CSRF attacks?**	Use POST requests over HTTPS rather than GET requests so their parameters cannot be sniffed.
53.	**Which of these is true of sqlmap**	If you want to use it for POST requests, you must provide a request template.
54.	**Which of these factors will not contribute to enabling server-side request forgery?**	A user may employ an out-of-date browser that does not support HSTS.
55.	**What method does the FMS WEP cracking approach use?**	It replays ARP packets repeated-

		ly to discover the shared key.
56.	**Which of these is not an element of AAA management protocols**	Attribution
57.	**Which of these will the Evil Twin attack perform?**	Client deauthorization to force reauthorization.
58.	**Which of these cannot be true of a communication that is readily accessible to the general public?**	It is communicated over channels reserved for satellite communications.
59.	**What can an iPhone user do to prevent interception of communications?**	Use an end-to-end encryption app like Signal.
60.	**What is the underlying cause of the Android Master Key vulnerability?**	Incompatible installation and execution PK zip methods.
61.	**Why is the checkm8 vulnerability more persistent than earlier jailbreaks?**	Because it is a boot ROM vulnerability independent of the OS version.
62.	**Which of these security measures is least likely to insure applications security.**	Employing code obfuscation to make app reverse engineering difficult.
63.	**If you want to MITM communications between an iPhone app and a server with a pinned certificate, which tool should you use?**	ssl-killswitch-2.

64.	**Which of these flaws allows one to downgrade the firmware on a TPLink smart bulb?**	Trusting client software to report the correct firmware version.
65.	**Which of these is not an action that can be taken on S3 objects:**	HEAD
66.	**Which of these is not a Neurolinguistic Programming though mode?**	Economic.
67.	**What parameter to the Powershell program will make it less likely for a Rubber Ducky attack to be noticed?**	-windowstyle hidden