Ethical Hacking

Study online at https://quizlet.com/_975u80

1.	**Which of these port designations could not be a result of running nmap as follows: nmap 172.18.0.75.** **A. 21/tcp open ftp** **B. 53/tcp closed domain** **C. 445/tcp open microsoft-ds** **D. 8080/tcp filtered http-proxy**	B. 53/tcp closed domain (CHECK) D. 8080/tcp based on https://wiki.onap.org/display/DW/Nmap "Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port."
2.	**Which of these would function the same with either a SOCKS 4a or SOCKS 5 proxy?** **A. DNS requests.** **B. Communication with a host based on an AAAA DNS record.** **C. nmap -A** **D. Https requests using wget.**	C. nmap -A (A, based on https://security.stackexchange.com/questions/134658/difference-between-socks5-and-socks4-p <- review says nmap -A
3.	**What distinguishes the CheckRa1n jailbreak from previous iPhone jailbreaks?** **A. The jailbreak is completely untethered.** **B. It is not necessary to unlock the phone to execute this jailbreak.** **C. The jailbreak is not dependent on the OS version.** **D. It is the first jailbreak distributed by Pangu.**	C. The jailbreak is not dependent on the OS version.
4.	**Which of these things has caused whois records to be of less utility in open-source intelligence?** **A. The ruling on DNS zone transfer by the court of North Dakota.** **B. A change of ownership of IANA.** **C. Enacting the GDPR.** **D. The Tallinn Manual concerning cyber warfare.**	C. Enacting the GDPR https://www.zdnet.com/article/icann-makes-last-minute-gdpr-requirements/

5.	**Which of these is most likely to employ a small collection of passwords likeFall2019?** **A. A spearphishing attack.** **B. A brute-force password cracking attack.** **C. A password spraying attack.** **D. A dictionary attack on the password hashes of a company's top-level executives.**	C. A password spraying attack.
6.	**Why does sslstrip need ipforward set to true in /proc/sys/net/ipv4/?** **A. So that https packets will reach their destinations.** **B. To insure that http packets (that should not be stripped) reach their destinations.** **C. This is not actually a requirement of sslstrip.** **D. To make sure packets not relevant to the sslstrip process get to their intended desti-nations.**	D. To make sure packets not relevant to the sslstrip process get to their intended desti-nations.
7.	**What is the primary benefit that Shodan provides to penetration testers?** **A. It allows one to determine available services without actually querying the host.** **B. It identifies out-of-date software versions.** **C. It lets one run checks against services to determine their vulnerabilities.** **D. It uses masscan on private networks, yielding faster service discovery than nmap.**	A. It allows one to determine available services without actually querying the host.
8.	**1. Which of these files is most likely to contain database credentials?** **A. global.asa** **B. groups.xml** **C. .htaccess** **D. robots.txt**	global.asa (Really check)
9.	**What is the netmask of the network associated with host 128.227.224.196 having 16,382 hosts?** **A. 255.255.63.0**	C. 255.255.192.0

B. 255.255.128.0
C. 255.255.192.0
D. 255.255.255.0

10.	**Which of these tools can be used to help fierce use active scanning to find hosts whose name-sare not in the default dictionary and whose addresses are in private IP address ranges?** **A. nmap** **B. amass** **C. Cewl** **D. NES**	C. Cewl
11.	**What reconnaissance is necessary if one wants to mount an effective attack with a USB rubber-ducky?** **A. Identify the VID/PID of the hardware in use at the site you will be visiting to avoidneedless popup messages.** **B. Verify that only Windows devices are installed because Duckscript requires it.** **C. Find the baud rate of the serial keyboard port.** **D. Know the SMB patch level of the server under attack**	A. Identify the VID/PID of the hardware in use at the site you will be visiting to avoidneed-less popup messages.
12.	**11. Which of these might be associated with a SuperCookie?** **A. A website using HSTS.** **B. XSS associated with a CSRF attack.** **C. A secure, rotating token to support multifac-tor authentication.** **D. SQL mitigation techniques.**	A. A website using HSTS.
13.	**Which of these flags is most likely to be modified when forwarding a TCP packet?** **A. Flags** **B. Checksum** **C. Source Port** **D. Sequence Number**	C. Source Port

14.	**Which of these ports is most likely to alert an IDS if used as a handler port for a reverse-httpsmeterpreter shell?** **A. Port 80.** **B. Port 443.** **C. Port 1337.** **D. Port 3306.**	C. Port 1337.
15.	**Which of these is most likely to render an arp-spoof for MITM ineffective?** **A. Use of fully patched linux/windows operating systems.** **B. Use of a CISCO Catalyst switching system.** **C. Using resources from a cloud provider who uses layer-3 overlays and does not supportlayer 2 at all.** **D. Use of a Web Application Firewall (WAF).**	C. Using resources from a cloud provider who uses layer-3 overlays and does not support-layer 2 at all.
16.	**Why could your instructor not correctly implement a dirty sock vulnerability in an exercise?** **A. The debian version being used in the VM was not compatible with the dirty sockrepository.** **B. The kernel version employed did not exhibit the snapd vulnerability.** **C. Snapd requires internet access to reach a server.** **D. He's just not smart enough.**	C. Snapd requires internet access to reach a server.
17.	**Which of the following distinguishes the OSSTMM from the Flaw Hypothesis Model?** **A. The Flaw Hypothesis Model addresses legal/social issues to a much greater extentthan the OSSTMM.** **B. The OSSTMM preceded the Flaw Hypothesis model by at least 10 years.** **C. The OSSTMM addresses business risk, whereas the Flaw Hypothesis Model does not.** **D. The OSSTMM does not address cryptograph-**	C. The OSSTMM addresses business risk, whereas the Flaw Hypothesis Model does not.

	ic protections while the Flaw HypothesisModel does.	
18.	**Which of these properties of the program call stack in Intel machines made Aleph One's stacksmashing attacks possible?** **A. The stack stores local variables in lower addresses than the frame pointer.** **B. The frame pointer, while stored in the stack, can be overwritten to cause control totransfer to a different address.** **C. The program stack stores local data in lower addresses that the return address.** **D. The heap is stored in lower addresses than the stack.**	B. The frame pointer, while stored in the stack, can be overwritten to cause control to-transfer to a different address.
19.	**Which of these port designations could not be a result of running nmap as follows:** **nmap 172.18.0.75** **A. 25/tcp open ftp** **B. 53/tcp open domain** **C. 80/tcp open http** **D. 443/tcp open https**	A. 25/tcp open ftp
20.	**What is the primary reason for Nikto's effectiveness?** **A. Nikto is written in Python and uses a module that has been improved for the last 35 years.** **B. Nikto automates SQL injection and cross-site script vulnerability checks.** **C. Nikto's developers have included information from numerous web sites scanned in the past.** **D. Nikto uses the CUDA library to leverage the computational power and parallelism of GPUs.**	B. Nikto automates SQL injection and cross-site script vulnerability checks.
21.	**What is the primary difference between a SOCKS 4A proxy and a SOCKS 5 proxy?**	B. SOCKS5 adds support for UDP and ICMP,

	A. SOCKS5 supports the use of proxychains, but SOCKS4a does not. **B. SOCKS5 adds support for UDP and ICMP, which SOCKS4a ignores.** **C. SOCKS5 is implemented using HTML5.** **D. SOCKS4a is deprecated due to its reliance on jumbo packets.**	which SOCKS4a ignores.
22.	**What problem is addressed by using the Meterpreter's paranoid mode (as opposed to normal mode)?** **A. Communications will be encrypted using a custom public/private key pair.** **B. No bind connections will be allowed.** **C. Exfiltrated data will be encrypted using TLS.** **D. Only high-numbered ports will be used for communication.**	A. Communications will be encrypted using a custom public/private key pair.
23.	**Which of these methods is currently the most popular for iPhone jail-breaks?** **A. Running the Dirty Cow exploit to install Cydia Substrate.** **B. Using a hardware tethered jailbreak.** **C. Using a semi-tethered jailbreak.** **D. Using the Shadow Broker's Eternal Romance jailbreak.**	C. Using a semi-tethered jailbreak.
24.	**Which of these is completely unnecessary for a remote password spraying attack?** **A. Network connectivity.** **B. A copy of the /etc/passwd le.** **C. A candidate password list.** **D. An automated spraying tool or scripting language implementation plus ingenuity.**	C. A candidate password list. (check)
25.	**What kind of iptables rule does sslstrip require?** **A. A nat rule.** **B. A filter rule.** **C. A raw rule.** **D. A security rule.**	A. A nat rule.

26.	**What exploit can be used on a Bash Bunny that a Rubber Ducky will not support?** **A. Execution of Powershell code.** **B. USB HID device attacks on the keyboard.** **C. Simulation of an actual USB drive device.** **D. A Responder attack.**	A. Execution of Power-shell code.
27.	**Which of these is likely to make a cookie difficult to retrieve using BeEF?** **A. Using a SuperCookie.** **B. Enabling ad blocking in your browser.** **C. Using an HTTPOnly cookie.** **D. Setting your browser to use https everywhere.**	C. Using an HTTPOnly cookie.
28.	**Which of these isnotdone by hostapd-wpe?** **A. Use RADIUS to allow a client under attack to provide authentication credentials.** **B. Broadcast the SSID of the station under at-tack.** **C. Broadcast on the same channel as the station under attack.** **D. Arrange for a client under attack to connect to the WAN.**	D. Arrange for a client under attack to connect to the WAN.
29.	**Which of these compiler techniques isnotused to ensureCFI?** **A. Employing address space layout randomiza-tion.** **B. Enforcing non-executable stack pages.** **C. Unrolling loops to avoid jumps.** **D. Analysis of transfer-point equivalence class-es.**	C. Unrolling loops to avoid jumps.
30.	**Which large password collection was reported by your instructor to have a most likely pass-wordlength of 9 characters?** **A. The RockYou list.** **B. Troy Hunt's list.**	B. Troy Hunt's list.

C. Crackstation's human password list.
D. The Ashley Madison password list.

31. **Which of these is a reason to use themigrate-command in the meterpreter?**
A. To pivot to another host.
B. To increase the likelihood that your session will persist longer.
C. To elevate your privilege to that of another process's user.
D. To get access to a filesystem mounted by another process.

B. To increase the likelihood that your session will persist longer.

32. **Why does KrackAttack require the use of a different channel from the targeted station?**
A. So it can set up a clone of the station with the same MAC and communicate withtarget clients.
B. To keep the bandwidth on the station's channel low because of the high number ofduplicated packets.
C. To increase the likelihood of capturing connections from clients who use randomchannel assignments.
D. This isn't really something that KrackAttack does.

A. So it can set up a clone of the station with the same MAC and communicate withtarget clients.

33. **Which flag(s)musthave value 1 in the second Packet of a TCP four-way disconnect?**
A. SYN.
B. SYN and RST.
C. ACK.
D. ACK and FIN.

C. ACK.

34. **What method of encoding is used by Veil's Powershell payload scripts?**
A. Base64
B. ASE
C. XOR
D. Shikata Ga Nai

A. Base64

35.	**Which of these DNS record types will not help you in identifying the IP address associatedwith a hostname?** **A. A.** **B. CNAME.** **C. SRV.** **D. AAAA.**	C. SRV.
36.	**Which of these is required in order to arrange ssh MITM?** **A. Arp spoof must be carried out.** **B. The server public key must be captured.** **C. The user must either not notice or ignore the server fingerprint mismatch.** **D. A previous ssh login session must be sniffed.**	C. The user must either not notice or ignore the server fingerprint mismatch.
37.	**Does moving to LTE mean that cell phone communications are now secure?** **A. They are presumed to be secure as no problems with DIAMETER have been identi-fied.** **B. No, because SS7 still applies to all LTE calls exchanged between international carriers.** **C. No, as evidenced by Tobias Engels' demonstration of call-forwarding at CCC.** **D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.**	D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.
38.	**Which of these is not true concerning sslstrip?** **A. IP forwarding must be set to true.** **B. You must arpspoof the gateway's address to the target and the target's address tothe gateway.** **C. You must set an iptable rule that will forward connections on port 80 to the sslstripprogram.** **D. You must have the sslstrip executable running in order to downgrade https URLs tohttp in web pages delivered to the target.**	D. You must have the sslstrip executable running in order to downgrade https URLs tohttp in web pages delivered to the target.
39.	**Which of these isnottrue of IAM?** **A. Services can act freely once a group is as-**	B. Policies can be applied to other services.

signed.
B. Policies can be applied to other services.
C. Roles can be applied to other services.
D. Users must interact with the console, SDK, or CLI.

40. **Which of these is the type of cross-site scripting injection that would be used in an attackmounted by inserting a script tag into comments posted on a blog page?**
A. DOM.
B. Persistent.
C. Viral.
D. Reflected.

B. Persistent.

41. **Which of these is least likely to succeed against a Linux host?**
A. Dirty Sock
B. Dirty Cow
C. Spectre
D. Extrabacon

D. Extrabacon

42. **How is phishing typically used in the active phase of a penetration testing engagement?**
A. To increase employee awareness of security.
B. To shame employees who will click on anything.
C. To get information about desktop software used by employees.
D. To get a user to execute code that will provide a foothold into the network.

D. To get a user to execute code that will provide a foothold into the network.

43. **What name did a Russian security company give to the source of the exploits released by the-ShadowBrokers?**
A. The NSA
B. Edward Snowden
C. Kaspersky Labs
D. The Equation Group

D. The Equation Group

44.	**What is the traditional source of information about the operation of LSASS functions?** **A. undocumented.ntinternals.net.** **B. The mimikatz source code.** **C.Windows Internals, by Mark Russinovich.** **D. The source code.**	A. undocumented.ntinternals.net.
45.	**What can be done to best protect passwords against a rainbow table attack?** **A. Employ the hash function multiple times in generating a password hash.** **B. Use a salt of reasonably large size.** **C. Use SHA-256 or higher.** **D. Rotate which of a small set of hashes (fewer than ten or so) is used.**	B. Use a salt of reasonably large size.
46.	**Which of these can be used most effectively to use nmap to scan a given port on a machinebehind a firewall.** **A. A meterpreter port forward.** **B. A meterpreter route.** **C. A meterpreter migrate command.** **D. A meterpreter incognito assignment**	A. A meterpreter port forward.
47.	**Why did Microsoft issue the LAPS program?** **A. To fix a security problem introduced by LSASS.** **B. To give administrators a rational approach to distributing passwords for local admin-istrators.** **C. To provide a service that implements an authentication provider for a local domain.** **D. To address a security flaw in the lightweight administration protocol.**	B. To give administrators a rational approach to distributing passwords for local administrators.
48.	**Which of these isnota method of identifying malicious programs discussed by Lenny Zeltser?** **A. Signatures.** **B. Heuristics.** **C. Behavior.** **D. Categories.**	D. Categories.

49.	**Where is the security protection afforded by HSTS enforced?** **A. In the network stack.** **B. At the server.** **C. In the browser.** **D. At a firewall.**	C. In the browser.
50.	**What usually accounts for NT AUTHORITY/SYSTEM not being able to execute a commoncommand?** **A. NT AUTHORITY/SYSTEM identifies a SID, not a user.** **B. NT AUTHORITY/SYSTEM may not have access to local files.** **C. NT AUTHORITY/SYSTEM may not actually exist on a given Windows system.** **D. NT AUTHORITY/SYSTEM may not be able to enable debug privilege.**	A. NT AUTHORITY/SYSTEM identifies a SID, not a user.
51.	**Which of these isnota reason to avoid use of telnet for exfiltration in a penetration test?** **A. Telnet uses an unencrypted channel.** **B. Use of telnet requires a privileged port to be opened and contacted on your target.** **C. Telnet employs UDP, which does not reliably order packets.** **D. The telnet service is not usually enabled and enabling it may arouse suspicion.**	C. Telnet employs UDP, which does not reliably order packets.
52.	**Which of these isnotan effective method for an organization to reduce the likelihood ofResponder attacks?** **A. Make sure that the WPAD host is black-holed by your routers.** **B. Disable LLMNR on all Windows machines.** **C. Configure web browsers not to use proxy auto-discovery.** **D. Disable USB autorun on all Windows desktop machines.**	D. Disable USB autorun on all Windows desktop machines.

53.	**Which of these exploits is the most likely to be the result of patch analysis (at least accordingto your instructor's analysis)?** **A. The recent Linux sudo attack.** **B. Dirty Cow.** **C. Eternal Blue.** **D. MS08-067.**	B. Dirty Cow.
54.	**Which type of web vulnerability is least likely to be remediated by a small business?** **A. Web server canonicalization errors.** **B. Sample file vulnerabilities.** **C. Web server extensions.** **D. Custom applicaton input validation.**	A. Web server canonicalization errors. (CHECK)
55.	**What response is given by a web server whenever a request to a page requiring Basic Auth isencountered for the first time?** **A. 200 OK.** **B. 401 Unauthorized.** **C. 203 Non-authoritative Information.** **D. 400 Bad Request**	B. 401 Unauthorized.
56.	**Which of these types of attacks employs the same underlying type of vulnerability that theSSRF techniques developed by Orange Tsai exploit?** **A. Eternal Romance.** **B. The Android Master Key vulnerability.** **C. SSLstrip.** **D. GPP local admin password.**	B. The Android Master Key vulnerability.
57.	**Which of these security requirements applies only to MASVS-R, the strongest of the MASVSverification levels, and not to the weaker levels?** **A. The app uses proven cryptographic methods.** **B. Network-transmitted data is encrypted using TLS**	C. The app prevents debugging or detects and responds to a debugger being attached.

C. The app prevents debugging or detects and responds to a debugger being attached.
D. Security controls are never enforced on the client side of any network request.

58. **Which of these would be necessary in order to capture network-transmitted data from a non-rooted Android phone.**
A. Use ADB to download the apk file.
B. Use tcpdump in user mode.
C. Use MobSF to MITM the connection.
D. Configure the phone for Wifi in Airplane mode and capture packets on the WAN sideof the AP.

D. Configure the phone for Wifi in Airplane mode and capture packets on the WAN sideof the AP.

59. **What does Chris Hadnagy define as "the act of bringing something out or arriving at a con-clusion?"**
A. Eliciation.
B. Exfiltration.
C. Information gathering.
D. Social engineering.

A. Eliciation.

60. **Which of the following things would provide the least value in an offline password crackingattack?**
A. oclhashcat
B. John the Ripper
C. rockyou.txt
D. /etc/passwd

D. /etc/passwd

61. **In order to avoid susceptibility to L0phtCrack, what is the minimum length for an NTLMpassword?**
A. 7 characters
B. 14 characters
C. 15 characters
D. 17 characters

C. 15 characters

62. **How is the unquoted Windows search path vulnerability exploited?**

A. By placing an appropriately named ma-

	A. By placing an appropriately named malicious program in the right directory. **B. By overwriting a vulnerable service program.** **C. By modifying the parameters of a given service.** **D. By arranging for the update of a service that can be installed by a non-admin user.**	licious program in the right directory.
63.	**Which of these is required in order to achieve a Silver Ticket attack?** **A. The application server must not verify the PAC.** **B. The krbtgt account's hash must be captured somehow.** **C. The server must not have changed the krbtgt account password twice since it wascaptured.** **D. A domain admin must be specified as the intended service user.**	A. The application server must not verify the PAC.
64.	**In Zinar and Simakov's Defcon talk, what underlying problem with the MIC check in NTLMnegotiation was exploited?** **A. The MIC is created using information available in the exchange.** **B. It is possible to drop and replay a different connection with the same MIC.** **C. If the MIC-set bit is set, a blank MIC can be used.** **D. The MIC is weak, thus the payload can be modified to make the MIC match.**	C. If the MIC-set bit is set, a blank MIC can be used.
65.	**Which of these ports is most likely to alert an IPS if used as a handler port for a reverse-https meterpreter shell?** **A. Port 8080.** **B. Port 4444.** **C. Port 443.** **D. Port 80.**	C. Port 443.
66.		

Why might you have administrator privilege on a machine but not be able to access a share?
A. Because the files on that share do not have administrator read privilege set?
B. Because you do not have the kerberos ticket granting ticket password.
C. Because you are a local rather than domain administrator.
D. Because you are accessing the system through remote desktop.

C. Because you are a local rather than domain administrator.

67. **Which of these is not something that Responder supports?**
A. Use of LLMNR to trap host names not resolved via DNS.
B. Advertisement of a malicious WPAD server.
C. MITM of SSL connections.
D. Injection into html web pages.

68. **What is an intended use of gratuitous ARP replies?**
A. To allow hardware to be replaced without disruption.
B. To allow Layer 2 MITM.
C. To allow Layer 3 switches to be recongured automatically.
D. To generate a corresponding ARP request.

69. **Which of these is not true of the Dirty Cow exploit?**
A. It relies on an Intel hardware prefetch error in order to function correctly.
B. It relies on kernel code that had unintended consequences.
C. It can leave a system in an unstable state that may cause it to crash.
D. It employs memory-mapped les.

A. It relies on an Intel hardware prefetch error in order to function correctly.

70. **Which of the following is a creation of R.R. Linde?**

A. The sslstrip tool.
B. The arpspoof utility.
C. The Social Engineering Toolkit.
D. The Flaw Hypothesis Model for penetration testing.

D. The Flaw Hypothesis Model for penetration testing.

71. **Which of these elements is not true of traceroute?**
A. Traceroute can identify hosts as far away as 511 hops away on the internet.
B. Traceroute sends 3 packets for each different group of packets it send.
C. Traceroute successively increments the TTL eld to insure that it captures all relevant responses.
D. Traceroute now targets port 53 since so many hosts refuse to response to ping requests.

D. Traceroute now targets port 53 since so many hosts refuse to response to ping requests.

72. **What is the maximum amount of time one can be imprisoned for under the Cyber Security Enhancement Act?**
A. 90 days.
B. One year.
C. Twenty-five years.
D. Life.

D. Life.

73. **Which of these is not a requirement to replace an executable in C:\System32**
A. The file must be a Microsoft signed binary.
B. The file must be in the Windows protected file list.
C. The file must be the same size as the original.
D. The file must normally reside in C:\System32

74. **Which of these is a potential attack against HTTP Strict Transport Security?**
A. Downgrade the HTTPOnly supercookie to a normal supercookie and reset it.
B. Use sslstrip to downgrade the connection to HTTP.

D. Mount an attack on NTP to cause supercookie expiration.

	C. MITM a connection to a site with an established HSTS supercookie. **D. Mount an attack on NTP to cause supercookie expiration.**	
75.	**What is the most important reason to use ncat as opposed to nc for exfiltrating data on a pentest engagemnent?** **A. ncat is less likely than nc to be noticed and blocked by AV software.** **B. ncat has bug fixes that make it more robust than nc.** **C. ncat supports the use of ssl communication.** **D. ncat is fully open source now.**	C. ncat supports the use of ssl communication. (CHECK)
76.	**Which mode must be used by an adaptor in order to mount a Reaver attack?** **A. Master.** **B. Managed.** **C. Monitor.** **D. Mesh.**	C. Monitor.
77.	**What virtual machine is employed by Android systems to execute applications?** **A. Java.** **B. Dalvik.** **C. C.** **D. APK.**	A. Java
78.	**What network protocol allows one to redirect cell telephone calls and SMS messages to different numbers?** **A. SS7.** **B. LTE.** **C. CDMA.** **D. Ethernet.**	
79.	**What does Linde say that we lack for verifying system security and therefore must use penetra-**	B. Formal correctness proofs.

tion testing instead?
A. Competent system administrators.
B. Formal correctness proofs.
C. Good software developer

80. **What does the * mean in this windows command net use \\192.168.202.44nIPC$ * /u:Administrator**
A. All users are affected by this command.
B. This process should accept remote network input.
C. The password is to be read from input.
D. This process should be repeated as long as input is not exhausted.

C. The password is to be read from input.

81. **What organization released the Mobile Application Security Verication Standard?**
A. EC Council.
B. Oensive Security.
C. SANS.
D. OWASP.

D. OWASP.

82. **Which of these password attack methods was rendered ineffective by the MS08-068 vulnerability**
patch?
A. LMv1/NTLMv2 Rainbow Table attack using a rogue server.
B. NTLM reective attack using a rogue server.
C. NTLM relay attack.
D. Zack Attack.

C. NTLM relay attack.

83. **If, on an engagement, you modify firewall rules to allow ssh connections only from your attack machine, what must you do?**
A. Restore previous firewall settings before completing the engagement.
B. Make sure that PermitRootLogin is not set in the configuration.
C. Make sure you don't use port 22 to connect so

A. Restore previous firewall settings before completing the engagement.

that no IPS will detect logins.
D. Insure that SSHv1 is used by the server.

84. **Which of these was released by the Shadow Brokers?**
A. Bettercap.
B. Fuzzbunch.
C. Stagefright.
D. WannaCry.

B. Fuzzbunch. (Check?)

85. **How do canonicalization errors lead to web exploits?**
A. They let a user avoid 2FA, increasing the likelihood of a MITM attack.
B. These errors enable denial of service attacks to be mounted.
C. They enable the use of ssh side-channel attacks .
D. Such errors allow transmission of data that would otherwise be blocked.

D. Such errors allow transmission of data that would otherwise be blocked.

86. **Which of these auth methods is most likely to be encountered on eCommerce web sites?**
A. Form-based authentication.
B. Basic authentication.
C. Digest authentication.
D. Windows integrated authentication.

A. Form-based authentication

87. **What extra hardware is required to let Kismet generate data usable by wigle.net?**
A. A GPS sensor.
B. An external Wi adaptor.
C. A wi adaptor capable of operating in Master mode.
D. A modern GPU.

88. **Which of these tools is not used for passing the hash?**
A. SMBShell.
B. Bloodhound.

C. THC Hydra.
D. msvctl.

89. **What does the Luhn algorithm do.**
A. It implements Rainbow Table lookup.
B. It uses ARP packets to crack WEP.
C. It is used by Eternal Blue to exploit a heap over
D. It verifies checksums of credit card numbers.

90. **What company prepares and releases the Kali Linux distribution?**
A. Offensive Security.
B. Debian.
C. Red Hat.
D. OWASP.

A. Offensive Security.

91. **What is the basis for the report format used in this class?**
A. OWASP.
B. The Crest Standard.
C. The PTES.
D. The Open Source Security Testing Methodology Manual.

A. OWASP. (CHECK)

92. **Which of these is likely based in part on work by Johnny Long first published in 2004?**
A. Laudanum.
B. The Fierce domain scanner.
C. The PowerUp Powershell module.
D. The Untangling the Web document from the NSA

D. The Untangling the Web document from the NSA

93. **If I tell you that a machine has IP address 192.168.200.193 and host number 65 in its network,**
what is it's netmask?
A. 255.255.255.0
B. 255.255.255.128

B. 255.255.255.128

C. 255.255.255.192
D. 255.255.255.224

94.	**Who said, "I'm going to save you a lot of money by giving you this free penetration test: You're vulnerable."** **A. Bruce Schneier.** **B. Ed Skoudis.** **C. Brian Krebs.**	A. Bruce Schneier.
95.	**Which of these must be known in order to set your Rules of Engagement?** **A. The number of wireless networks you'll be penetration testing.** **B. Methods to use for encrypting any sensitive data that must be exchanged.** **C. The email addresses of all employees using your client's information resources.**	B. Methods to use for encrypting any sensitive data that must be exchanged.
96.	**Why can't you get effective Rainbow Tables for Linux passwords?** **A. Linux uses SHA256 which will generate hashes of too great a length to catalog.** **B. The shadow file is not readable except by root, so you can't get password hashes.** **C. Because the passwords are salted, multiple rainbow tables would be required.** **D. Rainbow Tables can only be created for symmetric key encryption methods.**	C. Because the passwords are salted, multiple rainbow tables would be required.
97.	**According to SySS, which of these should you do if you want to carry out ethical penetration tests?** **A. Make sure you asses a penetration testing fee based on a percentage of the company's gross income.** **B. Notify your client of any risks or potential negative outcomes that might arise as a result of testing.** **C. Avoid identifying sources of software or tech-**	B. Notify your client of any risks or potential negative outcomes that might arise as a result of testing.

	niques used in exploiting vulnerabilities on the client's system.	
98.	**Which of these potential parts of a penetration test report is of most value to a customer?** **A. The information gathering activities in which testers engaged.** **B. The attack narrative that explains what testers did and in what order they did it.** **C. The executive summary that identifies the company's security posture and discusses how to improve it.**	C. The executive summary that identifies the company's security posture and discusses how to improve it.
99.	**In the Florida Computer Crimes Act, which of these terms is undefined?** **A. Authorization** **B. Network** **C. Computer**	A. Authorization
100.	**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?** **A. He said he had about nine followers, all relatives or close friends.** **B. He said he followed his son, Brien Comey.** **C. He mentioned that his advisor from William and Mary, Reinhold Niebuhr, followed him**	A. He said he had about nine followers, all relatives or close friends.
101.	**Which of these could be the netmask for the network with IP address 255.255.64.0?** **A. 255.255.128.0** **B. 255.255.192.0** **C. 255.255.0.0**	Q0x02 Question 3
102.	**What does a dig request for record type AXFR achieve?** **A. Zone transfer if its supported.** **B. Transfer of an extended address record.** **C. Nothing, you totally made that up.**	A. Zone transfer if its supported.

103. **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?** **A. Nothing. This can't be done.** **B. Zone transfer.** **C. Reverse lookup.**	C. Reverse lookup.
104. **Which of these is not a layer in the OSI networking model?** **A. Presentation** **B. Protocol** **C. Physical**	B. Protocol
105. **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?** **A. It will have ACK (but not SYN) set and the sequence number will be A+1.** **B. It will have SYN and ACK set and the sequence number will be chosen randomly.** **C. It will have SYN and ACK set and the acknowledgment number will be randomly chosen.**	B. It will have SYN and ACK set and the sequence number will be chosen randomly.
106. **What is the number of bits in UDP port?** **A. 8** **B. 32** **C. 16**	C. 16 (CHECK)
107. **What do the last 3 octets of a MAC address identify?** **A. The specific device ID.** **B. The vendor who manufactured the device.** **C. The network address.**	A. The specific device ID.
108. **How is OpenVAS's full and fast scan configuration different from full and fast ultimate?** **A. The ultimate scan avoids host-alive tests.**	B. The ultimate scan will not rely on cached results.

B. The ultimate scan will not rely on cached results.
C. The ultimate scan uses half-open scanning for stealth rather than full-connect scanning.

109. **How does ASLR help preserve program control-flow integrity**
A. It makes it hard to identify the addresses of values written in the stack.
B. It randomly assigns return locations, making program tracing hard.
C. It makes it impossible to execute code on the stack.

Q0x05 QUESTION 1

110. **When do you set a payload in the metasploit framework?**
A. When you run it using the exploit command.
B. After you use an exploit.
C. Before you decide which exploit to use.

Q0x05 QUESTION 2

111. **Which of these malware artifacts did not use the vulnerability identified in MS08-067?**
A. Eternal Blue.
B. Conficker.
C. Stuxnet.

A. Eternal Blue.

112. **What register is used to hold the base- or frame-pointer in the X64 architecture**
A. rbx.
B. rbp.
C. rfp.

B. rbp.

113. **If I see a file with permissions -rwxr-xr-x+, which of these statements must be true?**
A. The file is a directory.
B. The file has an access control list (ACL).
C. All users other than the owner cannot write the file.

Q0X06 QUESTION 1

114.

	Which of these is true about the RockYou password breach? **A. This breach occurred in 2016.** **B. The passwords were stored in plain text.** **C. 64 Million passwords were exfiltrated.**	B. The passwords were stored in plain text.
115.	**Which of these is most likely to keep a penetration tester from being able to guess passwords through SMB on a particular machine?** **A. Closing ports 139, 445 with a firewall that limits traffic entering the network for that machine.** **B. Make sure the host uses hashed passwords.** **C. Closing ports 139 and 445 with the machine's local firewall.**	Q0X06 QUESTION 3
116.	**What did I report as the most common length for a password in the Have I Been Pwned password list?** **A. 12.** **B. 5.** **C. 9.**	C. 9.
117.	**The Zack Attack can also be described as an** **A. NTLM reflective attack.** **B. NTLM relay attack.** **C. attack on Kerberos.**	B. NTLM relay attack.
118.	**Which of these was not a vulnerability of LDAP(S) session signing?** **A. A blank NetBIOS computer name could be passed in requests.** **B. The "MIC is Set" bit was checked but not the MIC itself.** **C. The relayer could use its NetBIOS computer name in relayed messages.**	C. The relayer could use its NetBIOS computer name in relayed messages.
119.	**If you want to get a Kerberos server long term key, which type of encryption should be enforced?** **A. MD4**	C. RC4

B. kerberos
C. RC4

120.	**Which of these commands will allow you to communicate with a web server on the host targetmachine.com?** **A. nc -c targetmachine.com:80** **B. nc targetmachine.com 80** **C. nc -l -p 80 targetmachine.com**	B. nc targetmachine.com 80
121.	**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?** **A. Connect to the service provided on port 445 by 172.30.0.96 by connecting to localhost port 8000.** **B. Automatically target 172.30.0.96 in another exploit from the same metasploit console.** **C. Connect to the service listening on port 8000 of 172.30.0.96 by connecting to port 445 on localhost.**	A. Connect to the service provided on port 445 by 172.30.0.96 by connecting to localhost port 8000.
122.	**Why might it be preferable to use a powershell payload rather than a native .exe file payload?** **A. Powershell runs much faster than native code.** **B. A machine might execute powershell, but not native code.** **C. The powershell payload need never be stored in the filesystem.**	C. The powershell payload need never be stored in the filesystem.
123.	**Which of these integrity levels is used by Internet Explorer in protected-mode?** **A. Medium.** **B. Low.** **C. High.**	B. Low.
124.	**Where was the AES-encrypted Microsoft Local Administrator password stored for distribution**	

	(until some time after 2014)? **A. In the Security Accounts Manager (SAM) local file.** **B. In the SYSVOL directory on the domain controller.** **C. Nowhere. RC4 encryption was used for this password.**	B. In the SYSVOL directory on the domain controller.
125.	**What account executes sethc.exe when 5 successive shift key press event occur before login?** **A. What account executes sethc.exe when 5 successive shit key press event occur before login?** **B. NT AUTHORITY/System.** **C. The local Administrator account (UID 500).**	B. NT AUTHORITY/System.
126.	**Which of these is not true about carrying a successful stealthy arpspoof campaign?** **A. We must be running a web server on port 80.** **B. We must be able to perform IP forwarding.** **C. We must have access to the affected hosts on a single layer 2 network.**	A. We must be running a web server on port 80.
127.	**Which of these must be done in order to run SSLStrip?** **A. Provide an https server running on port 443.** **B. Enable IP forwarding.** **C. Provide a web server running on port 80.**	B. Enable IP forwarding.
128.	**Which of the following is true of HSTS super-cookies?** **A. They cannot be removed from a compliant browser by using any browser function available to the user.** **B. They are a server technology that requires no special browser support.** **C. Once stored by a compliant browser, they never expire.**	A. They cannot be removed from a compliant browser by using any browser function available to the user.
129.		Q0X0a QUESTION 4

Which of these is true of ssh?
A. When using the public-key authentication scheme, passwords cannot be sniffed by a MiTM.
B. Diffie-Hellman exchange authenticates both the client and server machines.
C. Any password sniffing attack requires the attacker to have the server public key.

130. **Which of these can be a security principal?**
A. A computer.
B. A user account.
C. An organizational unit.

B. A user account.

131. **Which of these is not an underlying approach to malware detection?**
A. Signature detection.
B. Heuristic detection.
C. Pessimistic detection.

C. Pessimistic detection.

132. **How can an attacker exploit the following unquoted service path?**
"C:\Program Files\Printer Software\EpsonDriver.exe"
A. By storing Program.exe in "C:\".
B. By storing Printer.exe in C:\Program Files".
C. By doing what either of the other two answers says.

C. By doing what either of the other two answers says.

133. **How does nmap determine that a port is closed?**
A. it gets a FIN response to a SYN packet.
B. It gets no response to a SYN packet.
C. It gets a RST response to a SYN packet

C. It gets a RST response to a SYN packet

134. **What organization is responsible for issuing internet RFCs?**
A. ICANN.
B. The IETF.
C. IANA.

B. The IETF.

135. **What is the point of the General Data Protection Regulation?** **A. To provide network standards for ensuring that data is not modified while in transit.** **B. To ensure that data that could be used to prosecute cybercrimes is protected from being destroyed.** **C. To ensure that the personal data of users of computer services is not disclosed without permission.**	C. To ensure that the personal data of users of computer services is not disclosed without permission.
136. **What work is likely based, in part, on Johnny Long's Google Hacking for Penetration Testers?** **A. No answer text provided.** **B. The web reconnaissance framework Recon-ng.** **C. The Pen Test Execution Standard.** **D. The document Untangling the Web: a Guide to Internet Research.**	D. The document Untangling the Web: a Guide to Internet Research.
137. **Which of these commands must be implemented as a shell builtin in order to exhibit the right behavior?** **A. whoami** **B. tail** **C. cd**	C. cd
138. **Which of these steps to enable telnet service for a user is not necessary on a Windows host?** **A. Ensure the tlntsrv service is running** **B. Ensure that the user is in the TelnetClients group.** **C. Ensure that you have opened port 22 in the firewall.**	C. Ensure that you have opened port 22 in the firewall.
139. **What does WPAD do?** **A. Supports editing of Active Directory policies.** **B. Proxies web requests for Windows web servers.**	Q0X0b QUESTION 2

C. Provides automatic configuration for Windows browse

140.	**What is a canonical representation?** **A .One that uses the fewest possible characters.** **B. One that has been tested and verified.** **C. One that is given by a formal rule.**	C. One that is given by a formal rule.
141.	**What is true of an idempotent command?** **A. Applying the command more than once will yield the same result.** **B. The command was once implemented, but is no longer available to be executed.** **C. Applying the command will not change any resources on the web server**	A. Applying the command more than once will yield the same result.
142.	**Which of these methods of authentication is most often encountered in web applications?** **A. Basic authentication.** **B. Digest authentication.** **C. Form-based authentication.**	Q0X0d QUESTION 3
143.	**Which of the following is not a reason to use a web proxy?** **A. To reduce the number of web hosts in the path between a client and server on the first download of a page.** **B. To enable a penetration tester to forge requests and responses from a web browser to a web server.** **C. To reduce the number of times a remote server is queried for an oft-requested web page.**	A. To reduce the number of web hosts in the path between a client and server on the first download of a page.
144.	**Which of these is true of sqlmap** **A. If you want to use it for POST requests, you must provide a request template.** **B. It is intended to work exclusively with MSSQL.** **C. It can provide information about the structure of a backing database, but not its contents.**	A. If you want to use it for POST requests, you must provide a request template.

145. **Which of these factors will not contribute to enabling server-side request forgery?** **A. A user may employ an out-of-date browser that does not support HSTS.** **B. A web application may use two incompatible parsing modules like requests and urllib.** **C. Web application developers may have made different assumptions about how to interpret URLs and other input.**	A. A user may employ an out-of-date browser that does not support HSTS.
146. **What method does the FMS WEP cracking approach use?** **A. It uses a side channel attack to reconstruct the pairwise master key.** **B. It drops connections then sniffs the four-way handshake.** **C. It replays ARP packets repeatedly to discover the shared key.**	C. It replays ARP packets repeatedly to discover the shared key.
147. **Which of these is not an element of AAA management protocols** **A. Accounting** **B. Attribution** **C. Authorization**	B. Attribution
148. **Which of these will the Evil Twin attack perform?** **A. Client deauthorization to force reauthorization.** **B. Denial of Service attacks to downgrade Wifi quality.** **C. SQL injection to capture portal passwords.**	A. Client deauthorization to force reauthorization.
149. **Which of these cannot be true of a communication that is readily accessible to the general public?** **A. It uses frequency bands employed for emergency communications.** **B. It uses modulation techniques with publicly known parameters.**	C. It is communicated over channels reserved for satellite communications.

	C. It is communicated over channels reserved for satellite communications.	
150.	**What can an iPhone user do to prevent interception of communications?** **A. Make sure only to use LTE communications.** **B. Use an IMSI-catcher detecting app sold on the App store.** **C. Use an end-to-end encryption app like Signal.**	C. Use an end-to-end encryption app like Signal.
151.	**What is the underlying cause of the Android Master Key vulnerability?** **A. The master key was leaked unwittingly by Google in a blog post.** **B. Incompatible installation and execution PK zip methods.** **C. A buffer overflow vulnerability in the mediaserver.**	B. Incompatible installation and execution PK zip methods. (CHECK) Q0X10 QUESTION 1
152.	**Why is the checkm8 vulnerability more persistent than earlier jailbreaks?** **A. Because it is not tethered.** **B. It is written using Swift, which is compatible with many iOS versions.** **C. Because it is a boot ROM vulnerability independent of the OS version**	C. Because it is a boot ROM vulnerability independent of the OS version
153.	**Which of these security measures is least likely to insure applications security.** **A. Using secure encrypted communication channels.** **B. Using secure key-storage APIs.** **C. Employing code obfuscation to make app reverse engineering difficult.**	C. Employing code obfuscation to make app reverse engineering difficult.
154.	**If you want to MITM communications between an iPhone app and a server with a pinned certificate, which tool should you use?** **A. ssl-killswitch-2.**	A. ssl-killswitch-2.

B. JADX.
C. Hopper.

155.	**Which of these is the worst idea to use if you want to avoid CSRF attacks?** **A. Use POST requests over HTTPS rather than GET requests so their parameters cannot be sniffed.** **B. Use only HttpOnly cookies for session and other identifying tokens.** **C. Employ redundant verification of intent (such as CAPTCHAs or multi-factor authentication).**	A. Use POST requests over HTTPS rather than GET requests so their parameters cannot be sniffed.
156.	**Which of these types of authentication is susceptible to MITM attack and password cracking, but not direct password decoding?** **A. Basic Authentication.** **B. Integrated Windows Authentication.** **C. Digest Authentication**	Q0X0e QUESTION 1
157.	**Which of these is a Linux kernel vulnerability?** **A. Eternal Red aka SambaCry.** **B. Linux eBPF privilege Escalation.** **C. Dirty Sock.**	B. Linux eBPF privilege Escalation.
158.	**Which of these is true of the popular exploitdb exploit for DirtyCOW?** **A. It will work on any Linux system.** **B. It allows people with no login access on a Linux machine to become root.** **C. After using it, the system is unstable and may crash.**	C. After using it, the system is unstable and may crash.
159.	**Which of these Shadow Brokers exploits was not used by WannaCry?** **A. Eternal Blue** **B. Double Pulsar** **C. Extrabacon**	C. Extrabacon
160.		

When using a meterpreter, which command can be used to increase the likely longevity of your session?
A. shell.
B. background.
C. clearev.
D. migrate.

161. **If you are using Burp Suite to proxy your connection to a website, which of the following must you do?**
A. Insure that Burp Suite is running on the same machine as the web browser.
B. Set the proxy settings on your web browser to refer to the IP address and Port on which Burp is listening.
C. Insure that Burp Suite has a certificate that is generated by a legitimate Certificate Authority.
D. Make sure that javascript is enabled in your browser.

162. **Which of these types of wireless encryption standards is subject to an attack that employs replayed ARP requests?**
A. Open.
B. WEP.
C. WPA2/PSK.
D. WPA2/EAP.

163. **Which of these IP packet elds will not be modied when a router forwards a packet**
A. Flags.
B. Source Address.
C. Checksum.
D. TTL.

164. **Which of these DNS record types is critical to identifying a hostname given an IP address.**
A. A.

B. CNAME.
C. MX.
D. PTR.

165. **Which of these attacks requires a rogue access point to use a different channel from the legitimate access point?**
A. KrackAttack.
B. WPA2 attacks using FreeRadius WPE.
C. WEP attacks using FMS.
D. Reaver WPA2 attack.

166. **What type of filesystem supports the ip forward file which must be modified in order to enable IP forwarding?**
A. ramfs.
B. ext4.
C. zfs.
D. proc.

167. **Why should one not rely on using ICMP Echo Request for traceroute nowadays?**
A. The IETF has banned the use of ICMP Echo Request on IP networks.
B. ICMP Echo Requests are ignored by numerous internet hosts and routers.
C. Since the European Union passed the GDPR legislation, ICMP Echo Requests are not allowed in Europe.
D. ICMP Echo Request packets do not support session management.

168. **Which of these mimikatz commands most likely needs to be executed to retrieve LSASS cached credentials.**
A. privilege::debug
B. kerberos::hash
C. kerberos:ptt
D. sekurlsa:pth

169. **Which of these is not a reasonable approach to avoiding Cross-Site Request Forgery?**
A. Use CAPTCHAs to verify intent.
B. Employ two-factor authentication.
C. Insure that tokens are HTTPOnly and are not easily guessable.
D. Insure that only Post request are employed (rather than Get requests).

170. **What variable must be set to use a Metasploit reverse payload but need not be set to use a bind payload?**
A. RHOST.
B. LHOST.
C. RPORT.
D. PAYLOAD.

B. LHOST.

171. **Which flag(s) must have value 1 in the second Packet of a TCP three-way handshake?**
A. RST and SYN.
B. RST.
C. ACK.
D. SYN and ACK.

172. **Microsoft Azure software defined networks do not support Layer 2 switching. Which of these methods is rendered ineffectual by that design?**
A. Use of a WPAD-established web proxy.
B. Use of BeEF for browser hooking.
C. Use of sslstrip to downgrade https connections.
D. Use of netcat for pivoting in a network.

173. **Which layer of the OSI 7-Layer Model does UDP fall into?**
A. Datalink.
B. Application.
C. Transport.
D. Session.

C. Transport.

174. **What kind of program is most likely to be exploited by the unquoted Windows search path vulnerability?**
A. A service.
B. Internet explorer.
C. A program update script written using Powershell.
D. A user installed executable.

D. A user installed executable. (CHECK)

175. **Which UAC integrity level is used by Internet Explorer?**
A. None
B. Low
C. Medium
D. High

176. **Which of these is the type of cross-site scripting injection that would be used in an attack mounted by a single malicious email message?**
A. Fluctuating.
B. Persistent.
C. Viral.
D. Reflected.

177. **Which of these is a valid value for the TCP Data offset eld?**
A. 0.
B. 4.
C. 8.
D. 16.

178. **Why did Linus Torvalds' remove the patch that addressed the problem underlying Dirty Cow in around 2007?**
A. It caused problems for IBM S390 machines.
B. The NSA paid him to leave it vulnerable.
C. It didn't actually resolve the problem.

A. It caused problems for IBM S390 machines.

179. **Which of these was demonstrated by the app InstaStock, developed by Charlie Miller?**

C. The Apple App Store's app verifica-

	A. The Stagefright vulnerability could be used to cause remote code execution. **B. Cross-site scripting can lead to the exfiltration of investment account information.** **C. The Apple App Store's app verification method is insecure.** **D. None of the above.**	tion method is insecure. (Check)
180.	**Which of these is not required to mount an sslstrip attack?** **A. The ability to forward packets.** **B. Access to a valid SSL certificate issued by a trusted authority.** **C. Access to the layer-2 network to which the target host is attached. D.Ability to route packets to the internet through a gateway host**	B. Access to a valid SSL certificate issued by a trusted authority
181.	**1. Which of these is a valid Linux password hash entry from the file /etc/shadow?** **A. 5MnfsQ4iNZMTpp-KN16y/tIsUYs/obHlhdP.Os80yXhTurpBMUbA5** **B. AAD3B435B51404EEAAD3B435B51404EE** **C. 7aGFzaAo=$VGhpcyBpcyBteSB-wYXNzd29yZAo=** **D. 1Etg2ExUZ$F9NTP7omafhKIlqaBMqng1**	D. 1Etg2ExUZ$F9NTP7omafhKIlqaBMqng1
182.	**Which of these is not a requirement of sethc.exe?** **A. It must be digitally signed by a valid Microsoft key.** **B. Windows Defender must not identify it as malware.** **C. It must lie inside the file system under C:\Win-**	B. Windows Defender must not identify it as malware.

dows\System32.
D. It must be in the Windows protected file list.

183. **1. Which of these port designations could not be a result of running nmap as follows? nmap 172.18.0.24**

A. 21/tcp open ftp
B. 53/tcp open domain
C. 80/tcp open http
D. 445/tcp open https

D. 445/tcp open https

184. **Which of the following did Microsoft's 2014 patch for the Local Administrator Password not do?**

A. Remove the groups.xml file from affected hosts.
B. Address a problem created by releasing an AES encryption key in 2012 or before.
C. Attempt to solve a problem with local administrator account distribution.
D. Remove the ability to store passwords in group policies.

A. Remove the groups.xml file from affected hosts

185. **Which of these is true of HTTP Basic Authentication?**

A. It employs public-key cryptography.
B. Apache's implementation authenticates both the client and server to each other.
C. It uses AES symmetric encryption.
D. It is insecure if used on http.

D. It is insecure if used on http.

186. **1. Which of these is not true concerning using Web Proxy Auto Discovery and a bogus Proxy AutoConfig file to exploit vulnerable Windows?**

A. Responder implements this exploit.
B. This can be avoided by providing a black-hole

C. This attack requires access to a Linux host on same the layer-2 network as the target host.

	entry for the WPAD host in your DNS server. **C. This attack requires access to a Linux host on same the layer-2 network as the target host.** **D. This is typically exploited by providing a rogue LLMNR server.**	
187.	**1. Which of these elements that must be present in a web application in order for persistent cross-site scripting to occur.** **A. The server must use http.** **B. The web application must be vulnerable to injection.** **C. The server must not use HTTP Strict Transport Security.** **D. The server must not provide HTTP-Only cookies.**	B. The web application must be vulnerable to injection.
188.	**1. What is the primary reason Nikto is so effective?** **A. Nikto's developers have included information about numerous web servers that have been scanned in the past.** **B. Nikto is written in Python and uses a module that is 35 years in the making.** **C. Nikto uses GPU parallelism to achieve high performance.** **D. Nikto automates SQL injection and XSS vulnerability detection.**	A. Nikto's developers have included information about numerous web servers that have been scanned in the past.
189.	**Why is the Dirty Cow vulnerability only useful as a post-exploitation tool?** **A. It uses a kernel vulnerability.** **B. It requires a very special sequence of instructions to be executed that no Linux service uses.** **C. It requires direct access to email services.**	A. It uses a kernel vulnerability.

It requires access to the file /bin/passwd which cannot be access by Linux services.

190. **Why is it preferable to use ncat over nc?**

A. Because ncat supports SSL encryption.
B. Because ncat is available for both Windows and Linux.
C. Because ncat can be used as both a client and listener.
D. Because ncat can execute dependent programs (like a shell).

A. Because ncat supports SSL encryption.

191. **What should you know about the Shadow Brokers?**

A. They worked with Edward Snowden to release XKeyScore.
B. They released a number of tools created by the Equation Group (presumably of the NSA).
C. They mounted the WannaCry virus ransomware attack on the British National Health Service.
They have been identified as being affiliated with Fancy Bear (APT 28).

B. They released a number of tools created by the Equation Group (presumably of the NSA).

192. **On what ports does sslstrip provide services to external machines?**

A. Port 53 (dns).
B. Port 80 (http).
C. Port 443 (https).
D. Both ports 80 (http) and 443 (https).

B. Port 80 (http).

193. **Which of these statements is true of using proxychains to forward traffic to a DNS?**

A. That would work just fine.
B. That wouldn't work because DNS uses ICMP to function correctly.

C. That wouldn't work because DNS uses UDP to function correctly.

C. That wouldn't work because DNS uses UDP to function correctly.
D. That would work intermittently because ARP requests may change a host's MAC address.

194. **What is the problem with unquoted Windows service paths?**

A. They allow executables to be executed by a service if properly placed in writable directories closer to the root directory than the original service executable.
B. They allow executables to be executed by a service if properly placed in writable directories further from the root directory than the original service executable.
C. They let users write into DLLs that normally should be unwritable.
They can cause users to be able to exploit the sticky-keys vulnerability.

A. They allow executables to be executed by a service if properly placed in writable directories closer to the root directory than the original service executable.

195. **Why is it absolutely critical that you consult a lawyer concerning any penetration test contract that you might sign?**

A. State and local laws require that you contact a lawyer before providing consulting services.
B. Lawyers are generally crack penetration testers and you really want one on your team.
C. Lawyers provide expert economic advice to allow you to maximize your earnings.
D. If you are not a lawyer, you need a lawyer to advise you on complex contractual agreements.

D. If you are not a lawyer, you need a lawyer to advise you on complex contractual agreements.

196. **Which of these is true of ARP spoofing?**

A. Multiple addresses must be spoofed in order to achieve denial of service.
B. ARP spoofing can never result in denial of

D. ARP spoofing of a target must be achieved from a network host that can communicate via

	service. **C. ARP spoofing of a target can be achieved from any network host that can communicate via IP to the target.** **D. ARP spoofing of a target must be achieved from a network host that can communicate via layer 2 (MAC address) to the target.**	layer 2 (MAC address) to the target.
197.	**Which of these does KrackAttack require?** **A. Ability to communicate on two different wifi channels.** **B. Access to a monitor-mode wifi interface.** **C. A FreeRADIUS-WPE implementation.** **D. The PSK of the wireless access point being attacked.**	B. Access to a monitor-mode wifi interface.
198.	**Which of the following is not a reason that Powershell is an important penetration testing tool?** **A. It has been part of Windows installations since Windows 7.** **B. It runs as administrator and thus provides immediate privilege escalation.** **C. It can execute programs downloaded from the internet without modifying the file system.** **D. It can execute programs delivered as Base64 encoded strings.**	B. It runs as administrator and thus provides immediate privilege escalation.
199.	**Which of the following properties does the meterpreter satisfy?** **A. The meterpreter can be migrated from one process to another to help you keep it alive.** **B. Meterpreter payloads are almost never recognized by intrusion detection systems.** **C. The meterpreter is small enough to be included in practically any buffer overflow.**	A. The meterpreter can be migrated from one process to another to help you keep it alive

The meterpreter uses TLS encryption which means that its sessions cannot be hijacked.

200. **What is the maximum number of times a packet may be forwarded when going from one internet host to another?**

A. 31
B. 63
C. 255
D. 65,535

C. 255

201. **Which of these terms is not defined by the Florida Computer Crimes Act (State Statue 815.01-07)?**

A. Access
B. Authorization
C. Computer
D. Network

B. Authorization

202. **Why would you consider sending deauth packets to a WPA2 host?**

A. To make sure reaver will run successfully.
B. To force another three-way handshake.
C. To force another four-way handshake
D. To generate more packets for an FMS attack.

C. To force another four-way handshake

203. **Why might a UDP nmap scan take longer than a TCP scan?**

A. UDP may be spending time waiting for missing packets in the stream.
B. UDP packets cause more network delay due to Diffie-Hellman exchange.
C. A UDP service is not required to respond to any packet.
D. TCP packets are generally smaller than UDP packets, thus they require less bandwidth.

C. A UDP service is not required to respond to any packet.

204. **Which of these methods of jail-breaking an iPhone would be best if you're not certain it will leave your system in an operable state?**

A. Eternal Romance.
B. Dirty Cow.
C. Untethered jailbreak.
D. Tethered jailbreak.

C. Untethered jailbreak.

205. **1. Which of these files is most likely to contain database credentials?**

A. global.asa
B. groups.xml
C. .htaccess
D. robots.txt

A. global.asa

206. **Why is it that you cannot execute a sudo command with the Laudanum shell?**

A. Laudanum does not run with appropriate credentials.
B. Laudanum does not have access to the exec primitive of Linux.
C. Laudanum does not establish a tty connection and you can't provide the input password.
D. PHP doesn't have sudo.

C. Laudanum does not establish a tty connection and you can't provide the input password.

207. **Which of these is not a reason to use a reverse-https meterpreter as opposed to reverse-http payload in a phishing attack?**

A. It helps maintain stealth because the traffic is expected to be encrypted.
B. It provides an extended set of commands, including incognito mode.
C. It is likely to succeed because traffic to port 443 is likely to be permitted through a firewall.
D. It is convenient and maintains stealth be-

C. It is likely to succeed because traffic to port 443 is likely to be permitted through a firewall.

	cause exploited hosts will connect to the listener and won't need to be interrogated individually.	
208.	**1. What type of server must an attacker provide in order to capture credentials from WPA2/EAP users?** **A. FreeRADIUS-WPE** **B. DNS** **C. Apache** **D. NetBIOS**	A. FreeRADIUS-WPE
209.	**In order to avoid susceptibility to L0phtCrack, what is the minimum length for an NTLM password?** **A. 7 characters** **B. 14 characters** **C. 15 characters** **D. 17 characters**	C. 15 characters
210.	**Which of these precautions should a website use for session token cookies?** **A. Make sure they are sequential.** **B. Encode them using Base64.** **C. Make them HttpOnly.** **D. Make sure they are persistent.**	C. Make them HttpOnly.
211.	**What kind of packet does traceroute traditionally use to identify intermediate hosts?** **A. SYN to port 20** **B. Gratuitous ARP reply** **C. SYN to port 80** **D. ICMP ECHO Request**	D. ICMP ECHO Request
212.	**1. Which of these techniques can effectively prevent CSRF?**	B. Require user interaction for redundant verification

A. Refuse to accept GET requests.
B. Require user interaction for redundant verification of intent.
C. Require the HTTP Referrer to be a protected web page.
D. Use sequentially numbered session tokens.

213. **Which of these is not a reason for penetration testers to be careful when using MITM techniques on a typically configured desktop computer?**

A. You may inadvertently cause denial of service.
B. You may capture PII that is not in the scope of your test.
C. You may increase the network traffic load on a host that is not equipped to handle it.
D. You may allow hosts to route to destinations that are not reachable by their normal gateway.

D. You may allow hosts to route to destinations that are not reachable by their normal gateway.

214. **Which of the following is the most reasonable phishing goal in a penetration test?**

A. To shame employees who are caught.
B. To pick up some extra cash with a Nigerian bank scam.
C. To deliver a persistent XSS attack.
D. To deliver a reflective XSS attack

A. To deliver a reflective XSS attack.

215. **Which of these types of attacks employs the same underlying type of vulnerability that the SSRF techniques (of Orange Tsai) exploit?**

A. Eternal Romance.
B. The Android Master Key vulnerability.
C. SSLstrip.
D. GPP local admin password.

B. The Android Master Key vulnerability.

216.

How can Digest Authentication be exploited?

A. Capture the server nonce and decrypt the password.
B. MITM a connection and downgrade to Basic Authentication.
C. Capture the password from a non-HttpOnly cookie.
D. Use a replay attack to decrypt the hashed password.

B. MITM a connection and downgrade to Basic Authentication.

217. **Which of the following files would provide the least value in an offline password cracking attack?**

A. oclhashcat
B. John the Ripper
C. rockyou.txt
D. /etc/passwd

D. /etc/passwd

218. **Why isn't the rainbow table method used on Linux passwords?**

A. SHA hashes cannot be indexed with rainbow tables.
B. Rainbow tables can only be implemented on Windows.
C. Linux passwords use cryptographic hashes.
D. Linux passwords are salted.

D. Linux passwords are salted.

219. **Which of these devices that a USB Rubber Ducky can emulate will be connected without question to a host machine?**

A. Printer
B. USB Drive
C. USB Network Adapter
D. HID

A. HID (CHECK)

220.

C. Exfiltration Potential

Which of these is not a part of the Microsoft DREAD risk model?

A. Damage Potential
B. Reproducibility
C. Exfiltration Potential
D. Affected Users

221. **Which of these fields does not appear in a UDP packet?**

A. Acknowledgment Number
B. IP Source Address
C. Destination Port Number
D. Checksum

A. Acknowledgment Number (tcp uses ack not udp) (CHECK)

222. **Which of the following was determined by a North Dakota court to be illegal?**

A. DNS zone transfer.
B. Slave DNS servers.
C. DNS alias records.
D. Public-key encryption.

A. DNS zone transfer.

223. **1. Which tool may be useful in password guessing?**

A. Fierce
B. CeWL
C. dig
D. Bloodhound

C. CeWL

224. **Which of these is required to be able to intercept calls to a phone via SS7?**

A. User permission.
B. An IMSI catcher.
C. A femtocell.
D. The user's phone number.

D. The user's phone number.

225. **Which of these methods is most likely to yield a payload that will bypass AV?**

A. Use the default meterpreter.
B. Use the shikata-ga-nai encoder.
C. Use a code signing certificate.
D. Use an unsigned jnlp

C. Use a code signing certificate.

226. **Which of these is not a microexpression identified by Paul Ekman?**

A. Awe
B. Disgust
C. Contempt
D. Surprise

A. Awe

227. **Which of these exploits, developed by the Equation Group, was released by ShadowBrokers?**

A. Stagefright
B. Heartbleed
C. Shellshock
D. Extrabacon

D. Extrabacon

228. **Which of these tools cannot be used for post-exploitation on a Windows host?**
A. WMIC
B. Powershell
C. Bash
D. Responder

C. Bash (Linux Only?) (CHECK)

229. **Which of these is not a required for the metasploit tomcat_mgr_upload exploit used with the bind_tcp payload?**

A. HttpUsername
B. HttpPassword
C. lhost
D. lport

D. lport (CHECK)

230. **Which of these is not necessary to specify in order to enable a meterpreter port forward?**

A. IP address
B. Gateway
C. Netmask
D. Session

`

231. **Which of the following can only be used on Linux?**

A. Inveigh
B. Cain
C. Responder
D. WMIC

C. Responder

232. **Which of the following is enabled by ARP cache poisoning?**

A. MAC address flooding.
B. Remote code execution via buffer overflow.
C. User Account Control bypass.
D. Smurf attack.

A. Smurf attack
The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

233. **What language are the nmap NSE scripts written in?**

A. English
B. Lua
C. Go
D. Python

B. Lua