Question: 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

Correct Answer: 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."

===

Question: 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.

Correct Answer: C. nmap -A (A, based on https://security.stackexchange.com/questions/134658/difference-between-socks5-and-socks4-proxy) <- review says nmap -A

===

Question: 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.

Correct Answer: C. The jailbreak is not dependent on the OS version.

===

Question: 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 IAN

A.

C. Enacting the GDPR.

D. The Tallinn Manual concerning cyber warfare.

Correct Answer: C. Enacting the GDPR https://www.zdnet.com/article/icann-makes-last-minute-whois-changes-to-address-gdpr-requirements/

===

Question: 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.

Correct Answer: C. A password spraying attack.

===

Question: 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.

Correct Answer: D. To make sure packets not relevant to the sslstrip process get to their intended desti-nations.

===

Question: 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.

Correct Answer: A. It allows one to determine available services without actually querying the host.

===

Question: 1. Which of these files is most likely to contain database credentials?

A. global.asa

B. groups.xml

C. .htaccess

D. robots.txt

Correct Answer: global.asa (Really check)

===

Question: What is the netmask of the network associated with host 128.227.224.196 having 16,382 hosts?

A. 255.255.63.0

B. 255.255.128.0

C. 255.255.192.0

D. 255.255.255.0

Correct Answer: C. 255.255.192.0

===

Question: Which of these tools can be used to help fierce use active scanning to find hosts whose namesare not in the default dictionary and whose addresses are in private IP address ranges?

A. nmap

B. amass

C. Cewl

D. NES

Correct Answer: C. Cewl

===

Question: What reconnaissance is necessary if one wants to mount an effective attack with a USB rubberducky?

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

Correct Answer: A. Identify the VID/PID of the hardware in use at the site you will be visiting to avoidneedless popup messages.

===

Question: 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 multifactor authentication.

D. SQL mitigation techniques.

Correct Answer: A. A website using HSTS.

===

Question: 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

Correct Answer: C. Source Port

===

Question: 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.

Correct Answer: C. Port 1337.

===

Question: Which of these is most likely to render an arpspoof 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).

Correct Answer: C. Using resources from a cloud provider who uses layer-3 overlays and does not supportlayer 2 at all.

===

Question: 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.

Correct Answer: C. Snapd requires internet access to reach a server.

===

Question: 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 cryptographic protections while the Flaw HypothesisModel does.

Correct Answer: C. The OSSTMM addresses business risk, whereas the Flaw Hypothesis Model does not.

===

Question: 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.

Correct Answer: B. The frame pointer, while stored in the stack, can be overwritten to cause control totransfer to a different address.

===

Question: 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

Correct Answer: A. 25/tcp open ftp

===

Question: 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 35years.

B. Nikto automates SQL injection and cross-site script vulnerability checks.

C. Nikto's developers have included information from numerous web sites scanned in thepast.

D. Nikto uses the CUDA library to leverage the computational power and parallelism ofGPUs.

Correct Answer: B. Nikto automates SQL injection and cross-site script vulnerability checks.

===

Question: What is the primary difference between a SOCKS 4A proxy and a SOCKS 5 proxy?

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.

Correct Answer: B. SOCKS5 adds support for UDP and ICMP, which SOCKS4a ignores.

===

Question: 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.

Correct Answer: A. Communications will be encrypted using a custom public/private key pair.

===

Question: 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.

Correct Answer: C. Using a semi-tethered jailbreak.

===

Question: 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.

Correct Answer: C. A candidate password list. (check)

===

Question: What kind of iptables rule does sslstrip require?

A. A nat rule.

B. A filter rule.

C. A raw rule.

D. A security rule.

Correct Answer: A. A nat rule.

===

Question: 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.

Correct Answer: A. Execution of Powershell code.

===

Question: 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.

Correct Answer: C. Using an HTTPOnly cookie.

===

Question: 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 attack.

C. Broadcast on the same channel as the station under attack.

D. Arrange for a client under attack to connect to the WAN.

Correct Answer: D. Arrange for a client under attack to connect to the WAN.

===

Question: Which of these compiler techniques isnotused to ensureCFI?

A. Employing address space layout randomization.

B. Enforcing non-executable stack pages.

C. Unrolling loops to avoid jumps.

D. Analysis of transfer-point equivalence classes.

Correct Answer: C. Unrolling loops to avoid jumps.

===

Question: Which large password collection was reported by your instructor to have a most likely passwordlength of 9 characters?

A. The RockYou list.

B. Troy Hunt's list.

C. Crackstation's human password list.

D. The Ashley Madison password list.

Correct Answer: B. Troy Hunt's list.

===

Question: Which of these is a reason to use themigratecommand 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.

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

===

Question: 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.

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

===

Question: 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.

Correct Answer: C. ACK.

===

Question: What method of encoding is used by Veil's Powershell payload scripts?

A. Base64

B. ASE

C. XOR

D. Shikata Ga Nai

Correct Answer: A. Base64

===

Question: 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. AAA

A.

Correct Answer: C. SRV.

===

Question: 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.

Correct Answer: C. The user must either not notice or ignore the server fingerprint mismatch.

===

Question: 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 CC

C.

D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.

Correct Answer: D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.

===

Question: 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.

Correct Answer: D. You must have the sslstrip executable running in order to downgrade https URLs tohttp in web pages delivered to the target.

===

Question: Which of these isnottrue of IAM?

A. Services can act freely once a group is assigned.

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.

Correct Answer: B. Policies can be applied to other services.

===

Question: 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.

Correct Answer: B. Persistent.

===

Question: Which of these is least likely to succeed against a Linux host?

A. Dirty Sock

B. Dirty Cow

C. Spectre

D. Extrabacon

Correct Answer: D. Extrabacon

===

Question: 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.

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

===

Question: What name did a Russian security company give to the source of the exploits released by theShadowBrokers?

A. The NSA

B. Edward Snowden

C. Kaspersky Labs

D. The Equation Group

Correct Answer: D. The Equation Group

===

Question: 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.

Correct Answer: A. undocumented.ntinternals.net.

===

Question: 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.

Correct Answer: B. Use a salt of reasonably large size.

===

Question: 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

Correct Answer: A. A meterpreter port forward.

===

Question: 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.

Correct Answer: B. To give administrators a rational approach to distributing passwords for local administrators.

===

Question: Which of these isnota method of identifying malicious programs discussed by Lenny Zeltser?

A. Signatures.

B. Heuristics.

C. Behavior.

D. Categories.

Correct Answer: D. Categories.

===

Question: 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.

Correct Answer: C. In the browser.

===

Question: 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.

Correct Answer: A. NT AUTHORITY/SYSTEM identifies a SID, not a user.

===

Question: 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.

Correct Answer: C. Telnet employs UDP, which does not reliably order packets.

===

Question: 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.

Correct Answer: D. Disable USB autorun on all Windows desktop machines.

===

Question: 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.

Correct Answer: B. Dirty Cow.

===

Question: 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.

Correct Answer: A. Web server canonicalization errors. (CHECK)

===

Question: 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

Correct Answer: B. 401 Unauthorized.

===

Question: 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.

Correct Answer: B. The Android Master Key vulnerability.

===

Question: 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.

D. Security controls are never enforced on the client side of any network request.

Correct Answer: C. The app prevents debugging or detects and responds to a debugger being attached.

===

Question: 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.

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

===

Question: What does Chris Hadnagy define as "the act of bringing something out or arriving at a conclusion?"

A. Eliciation.

B. Exfiltration.

C. Information gathering.

D. Social engineering.

Correct Answer: A. Eliciation.

===

Question: 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

Correct Answer: D. /etc/passwd

===

Question: 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

Correct Answer: C. 15 characters

===

Question: How is the unquoted Windows search path vulnerability exploited?

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.

Correct Answer: A. By placing an appropriately named malicious program in the right directory.

===

Question: Which of these is required in order to achieve a Silver Ticket attack?

A. The application server must not verify the PA

C.

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.

Correct Answer: A. The application server must not verify the PAC.

===

Question: 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 MI

C.

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.

Correct Answer: C. If the MIC-set bit is set, a blank MIC can be used.

===

Question: Which of these ports is most likely to alert an IPS if used as a handler port for a reverse-httpsmeterpreter shell?

A. Port 8080.

B. Port 4444.

C. Port 443.

D. Port 80.

Correct Answer: C. Port 443.

===

Question: 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.

Correct Answer: C. Because you are a local rather than domain administrator.

===

Question: 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.

Correct Answer: 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.

===

Question: 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.

Correct Answer: 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.

===

Question: 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.

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

===

Question: 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.

Correct Answer: D. The Flaw Hypothesis Model for penetration testing.

===

Question: 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 relevantresponses.

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

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

===

Question: What is the maximum amount of time one can be imprisoned for under the Cyber SecurityEnhancement Act?

A. 90 days.

B. One year.

C. Twenty-five years.

D. Life.

Correct Answer: D. Life.

===

Question: 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

Correct Answer: Which of these is not a requirement to replace an executable in C:\System32A. 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

===

Question: 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.

C. MITM a connection to a site with an established HSTS supercookie.

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

Correct Answer: D. Mount an attack on NTP to cause supercookie expiration.

===

Question: What is the most important reason to use ncat as opposed to nc for exfiltrating data on apentest 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.

Correct Answer: C. ncat supports the use of ssl communication. (CHECK)

===

Question: Which mode must be used by an adaptor in order to mount a Reaver attack?

A. Master.

B. Managed.

C. Monitor.

D. Mesh.

Correct Answer: C. Monitor.

===

Question: What virtual machine is employed by Android systems to execute applications?

A. Java.

B. Dalvik.

C.

C.

D. APK.

Correct Answer: A. Java

===

Question: What network protocol allows one to redirect cell telephone calls and SMS messages to differentnumbers?

A. SS7.

B. LTE.

C. CDM

A.

D. Ethernet.

Correct Answer: What network protocol allows one to redirect cell telephone calls and SMS messages to differentnumbers?A. SS7.B. LTE.C. CDMA.D. Ethernet.

===

Question: What does Linde say that we lack for verifying system security and therefore must use penetration testing instead?

A. Competent system administrators.

B. Formal correctness proofs.

C. Good software developer

Correct Answer: B. Formal correctness proofs.

===

Question: What does the * mean in this windows commandnet 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.

Correct Answer: C. The password is to be read from input.

===

Question: What organization released the Mobile Application Security Verication Standard?

A. EC Council.

B. Oensive Security.

C. SANS.

D. OWASP.

Correct Answer: D. OWASP.

===

Question: Which of these password attack methods was rendered ineffective by the MS08-068 vulnerabilitypatch?

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.

Correct Answer: C. NTLM relay attack.

===

Question: If, on an engagement, you modify firewall rules to allow ssh connections only from your attackmachine, 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 that no IPS will detect logins.

D. Insure that SSHv1 is used by the server.

Correct Answer: A. Restore previous firewall settings before completing the engagement.

===

Question: Which of these was released by the Shadow Brokers?

A. Bettercap.

B. Fuzzbunch.

C. Stagefright.

D. WannaCry.

Correct Answer: B. Fuzzbunch. (Check?)

===

Question: 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.

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

===

Question: 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.

Correct Answer: A. Form-based authentication

===

Question: 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.

Correct Answer: 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.

===

Question: Which of these tools is not used for passing the hash?

A. SMBShell.

B. Bloodhound.

C. THC Hydra.

D. msvctl.

Correct Answer: Which of these tools is not used for passing the hash?A. SMBShell.B. Bloodhound.C. THC Hydra.D. msvctl.

===

Question: 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.

Correct Answer: 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 overD. It verifies checksums of credit card numbers.

===

Question: What company prepares and releases the Kali Linux distribution?

A. Offensive Security.

B. Debian.

C. Red Hat.

D. OWASP.

Correct Answer: A. Offensive Security.

===

Question: 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.

Correct Answer: A. OWASP. (CHECK)

===

Question: 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

Correct Answer: D. The Untangling the Web document from the NSA

===

Question: 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

C. 255.255.255.192

D. 255.255.255.224

Correct Answer: B. 255.255.255.128

===

Question: 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.

Correct Answer: A. Bruce Schneier.

===

Question: 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.

Correct Answer: B. Methods to use for encrypting any sensitive data that must be exchanged.

===

Question: 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.

Correct Answer: C. Because the passwords are salted, multiple rainbow tables would be required.

===

Question: 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 techniques used in exploiting vulnerabilities on the client's system.

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

===

Question: 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.

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

===

Question: In the Florida Computer Crimes Act, which of these terms is undefined?

A. Authorization

B. Network

C. Computer

Correct Answer: A. Authorization

===

Question: 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

Correct Answer: A. He said he had about nine followers, all relatives or close friends.

===

Question: 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

Correct Answer: 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."

===

Question: 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.

Correct Answer: C. nmap -A (A, based on https://security.stackexchange.com/questions/134658/difference-between-socks5-and-socks4-proxy) <- review says nmap -A

===

Question: 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.

Correct Answer: C. The jailbreak is not dependent on the OS version.

===

Question: 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 IAN

A.

C. Enacting the GDPR.

D. The Tallinn Manual concerning cyber warfare.

Correct Answer: C. Enacting the GDPR https://www.zdnet.com/article/icann-makes-last-minute-whois-changes-to-address-gdpr-requirements/

===

Question: 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.

Correct Answer: C. A password spraying attack.

===

Question: 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.

Correct Answer: D. To make sure packets not relevant to the sslstrip process get to their intended desti-nations.

===

Question: 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.

Correct Answer: A. It allows one to determine available services without actually querying the host.

===

Question: 1. Which of these files is most likely to contain database credentials?

A. global.asa

B. groups.xml

C. .htaccess

D. robots.txt

Correct Answer: global.asa (Really check)

===

Question: What is the netmask of the network associated with host 128.227.224.196 having 16,382 hosts?

A. 255.255.63.0

B. 255.255.128.0

C. 255.255.192.0

D. 255.255.255.0

Correct Answer: C. 255.255.192.0

===

Question: Which of these tools can be used to help fierce use active scanning to find hosts whose namesare not in the default dictionary and whose addresses are in private IP address ranges?

A. nmap

B. amass

C. Cewl

D. NES

Correct Answer: C. Cewl

===

Question: What reconnaissance is necessary if one wants to mount an effective attack with a USB rubberducky?

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

Correct Answer: A. Identify the VID/PID of the hardware in use at the site you will be visiting to avoidneedless popup messages.

===

Question: 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 multifactor authentication.

D. SQL mitigation techniques.

Correct Answer: A. A website using HSTS.

===

Question: 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

Correct Answer: C. Source Port

===

Question: 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.

Correct Answer: C. Port 1337.

===

Question: Which of these is most likely to render an arpspoof 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).

Correct Answer: C. Using resources from a cloud provider who uses layer-3 overlays and does not supportlayer 2 at all.

===

Question: 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.

Correct Answer: C. Snapd requires internet access to reach a server.

===

Question: 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 cryptographic protections while the Flaw HypothesisModel does.

Correct Answer: C. The OSSTMM addresses business risk, whereas the Flaw Hypothesis Model does not.

===

Question: 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.

Correct Answer: B. The frame pointer, while stored in the stack, can be overwritten to cause control totransfer to a different address.

===

Question: 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

Correct Answer: A. 25/tcp open ftp

===

Question: 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 35years.

B. Nikto automates SQL injection and cross-site script vulnerability checks.

C. Nikto's developers have included information from numerous web sites scanned in thepast.

D. Nikto uses the CUDA library to leverage the computational power and parallelism ofGPUs.

Correct Answer: B. Nikto automates SQL injection and cross-site script vulnerability checks.

===

Question: What is the primary difference between a SOCKS 4A proxy and a SOCKS 5 proxy?

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.

Correct Answer: B. SOCKS5 adds support for UDP and ICMP, which SOCKS4a ignores.

===

Question: 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.

Correct Answer: A. Communications will be encrypted using a custom public/private key pair.

===

Question: 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.

Correct Answer: C. Using a semi-tethered jailbreak.

===

Question: 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.

Correct Answer: C. A candidate password list. (check)

===

Question: What kind of iptables rule does sslstrip require?

A. A nat rule.

B. A filter rule.

C. A raw rule.

D. A security rule.

Correct Answer: A. A nat rule.

===

Question: 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.

Correct Answer: A. Execution of Powershell code.

===

Question: 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.

Correct Answer: C. Using an HTTPOnly cookie.

===

Question: 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 attack.

C. Broadcast on the same channel as the station under attack.

D. Arrange for a client under attack to connect to the WAN.

Correct Answer: D. Arrange for a client under attack to connect to the WAN.

===

Question: Which of these compiler techniques isnotused to ensureCFI?

A. Employing address space layout randomization.

B. Enforcing non-executable stack pages.

C. Unrolling loops to avoid jumps.

D. Analysis of transfer-point equivalence classes.

Correct Answer: C. Unrolling loops to avoid jumps.

===

Question: Which large password collection was reported by your instructor to have a most likely passwordlength of 9 characters?

A. The RockYou list.

B. Troy Hunt's list.

C. Crackstation's human password list.

D. The Ashley Madison password list.

Correct Answer: B. Troy Hunt's list.

===

Question: Which of these is a reason to use themigratecommand 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.

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

===

Question: 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.

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

===

Question: 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.

Correct Answer: C. ACK.

===

Question: What method of encoding is used by Veil's Powershell payload scripts?

A. Base64

B. ASE

C. XOR

D. Shikata Ga Nai

Correct Answer: A. Base64

===

Question: 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. AAA

A.

Correct Answer: C. SRV.

===

Question: 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.

Correct Answer: C. The user must either not notice or ignore the server fingerprint mismatch.

===

Question: 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 CC

C.

D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.

Correct Answer: D. No, as evidenced by aLTEr-attack, a DNS-spoofing attack against LTE networks.

===

Question: 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.

Correct Answer: D. You must have the sslstrip executable running in order to downgrade https URLs tohttp in web pages delivered to the target.

===

Question: Which of these isnottrue of IAM?

A. Services can act freely once a group is assigned.

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.

Correct Answer: B. Policies can be applied to other services.

===

Question: 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.

Correct Answer: B. Persistent.

===

Question: Which of these is least likely to succeed against a Linux host?

A. Dirty Sock

B. Dirty Cow

C. Spectre

D. Extrabacon

Correct Answer: D. Extrabacon

===

Question: 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.

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

===

Question: What name did a Russian security company give to the source of the exploits released by theShadowBrokers?

A. The NSA

B. Edward Snowden

C. Kaspersky Labs

D. The Equation Group

Correct Answer: D. The Equation Group

===

Question: 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.

Correct Answer: A. undocumented.ntinternals.net.

===

Question: 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.

Correct Answer: B. Use a salt of reasonably large size.

===

Question: 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

Correct Answer: A. A meterpreter port forward.

===

Question: 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.

Correct Answer: B. To give administrators a rational approach to distributing passwords for local administrators.

===

Question: Which of these isnota method of identifying malicious programs discussed by Lenny Zeltser?

A. Signatures.

B. Heuristics.

C. Behavior.

D. Categories.

Correct Answer: D. Categories.

===

Question: 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.

Correct Answer: C. In the browser.

===

Question: 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.

Correct Answer: A. NT AUTHORITY/SYSTEM identifies a SID, not a user.

===

Question: 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.

Correct Answer: C. Telnet employs UDP, which does not reliably order packets.

===

Question: 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.

Correct Answer: D. Disable USB autorun on all Windows desktop machines.

===

Question: 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.

Correct Answer: B. Dirty Cow.

===

Question: 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.

Correct Answer: A. Web server canonicalization errors. (CHECK)

===

Question: 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

Correct Answer: B. 401 Unauthorized.

===

Question: 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.

Correct Answer: B. The Android Master Key vulnerability.

===

Question: 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.

D. Security controls are never enforced on the client side of any network request.

Correct Answer: C. The app prevents debugging or detects and responds to a debugger being attached.

===

Question: 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.

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

===

Question: What does Chris Hadnagy define as "the act of bringing something out or arriving at a conclusion?"

A. Eliciation.

B. Exfiltration.

C. Information gathering.

D. Social engineering.

Correct Answer: A. Eliciation.

===

Question: 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

Correct Answer: D. /etc/passwd

===

Question: 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

Correct Answer: C. 15 characters

===

Question: How is the unquoted Windows search path vulnerability exploited?

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.

Correct Answer: A. By placing an appropriately named malicious program in the right directory.

===

Question: Which of these is required in order to achieve a Silver Ticket attack?

A. The application server must not verify the PA

C.

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.

Correct Answer: A. The application server must not verify the PAC.

===

Question: 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 MI

C.

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.

Correct Answer: C. If the MIC-set bit is set, a blank MIC can be used.

===

Question: Which of these ports is most likely to alert an IPS if used as a handler port for a reverse-httpsmeterpreter shell?

A. Port 8080.

B. Port 4444.

C. Port 443.

D. Port 80.

Correct Answer: C. Port 443.

===

Question: 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.

Correct Answer: C. Because you are a local rather than domain administrator.

===

Question: 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.

Correct Answer: 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.

===

Question: 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.

Correct Answer: 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.

===

Question: 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.

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

===

Question: 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.

Correct Answer: D. The Flaw Hypothesis Model for penetration testing.

===

Question: 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 relevantresponses.

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

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

===

Question: What is the maximum amount of time one can be imprisoned for under the Cyber SecurityEnhancement Act?

A. 90 days.

B. One year.

C. Twenty-five years.

D. Life.

Correct Answer: D. Life.

===

Question: 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

Correct Answer: Which of these is not a requirement to replace an executable in C:\System32A. 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

===

Question: 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.

C. MITM a connection to a site with an established HSTS supercookie.

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

Correct Answer: D. Mount an attack on NTP to cause supercookie expiration.

===

Question: What is the most important reason to use ncat as opposed to nc for exfiltrating data on apentest 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.

Correct Answer: C. ncat supports the use of ssl communication. (CHECK)

===

Question: Which mode must be used by an adaptor in order to mount a Reaver attack?

A. Master.

B. Managed.

C. Monitor.

D. Mesh.

Correct Answer: C. Monitor.

===

Question: What virtual machine is employed by Android systems to execute applications?

A. Java.

B. Dalvik.

C.

C.

D. APK.

Correct Answer: A. Java

===

Question: What network protocol allows one to redirect cell telephone calls and SMS messages to differentnumbers?

A. SS7.

B. LTE.

C. CDM

A.

D. Ethernet.

Correct Answer: What network protocol allows one to redirect cell telephone calls and SMS messages to differentnumbers?A. SS7.B. LTE.C. CDMA.D. Ethernet.

===

Question: What does Linde say that we lack for verifying system security and therefore must use penetration testing instead?

A. Competent system administrators.

B. Formal correctness proofs.

C. Good software developer

Correct Answer: B. Formal correctness proofs.

===

Question: What does the * mean in this windows commandnet 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.

Correct Answer: C. The password is to be read from input.

===

Question: What organization released the Mobile Application Security Verication Standard?

A. EC Council.

B. Oensive Security.

C. SANS.

D. OWASP.

Correct Answer: D. OWASP.

===

Question: Which of these password attack methods was rendered ineffective by the MS08-068 vulnerabilitypatch?

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.

Correct Answer: C. NTLM relay attack.

===

Question: If, on an engagement, you modify firewall rules to allow ssh connections only from your attackmachine, 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 that no IPS will detect logins.

D. Insure that SSHv1 is used by the server.

Correct Answer: A. Restore previous firewall settings before completing the engagement.

===

Question: Which of these was released by the Shadow Brokers?

A. Bettercap.

B. Fuzzbunch.

C. Stagefright.

D. WannaCry.

Correct Answer: B. Fuzzbunch. (Check?)

===

Question: 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.

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

===

Question: 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.

Correct Answer: A. Form-based authentication

===

Question: 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.

Correct Answer: 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.

===

Question: Which of these tools is not used for passing the hash?

A. SMBShell.

B. Bloodhound.

C. THC Hydra.

D. msvctl.

Correct Answer: Which of these tools is not used for passing the hash?A. SMBShell.B. Bloodhound.C. THC Hydra.D. msvctl.

===

Question: 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.

Correct Answer: 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 overD. It verifies checksums of credit card numbers.

===

Question: What company prepares and releases the Kali Linux distribution?

A. Offensive Security.

B. Debian.

C. Red Hat.

D. OWASP.

Correct Answer: A. Offensive Security.

===

Question: 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.

Correct Answer: A. OWASP. (CHECK)

===

Question: 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

Correct Answer: D. The Untangling the Web document from the NSA

===

Question: 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

C. 255.255.255.192

D. 255.255.255.224

Correct Answer: B. 255.255.255.128

===

Question: 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.

Correct Answer: A. Bruce Schneier.

===

Question: 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.

Correct Answer: B. Methods to use for encrypting any sensitive data that must be exchanged.

===

Question: 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.

Correct Answer: C. Because the passwords are salted, multiple rainbow tables would be required.

===

Question: 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 techniques used in exploiting vulnerabilities on the client's system.

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

===

Question: 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.

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

===

Question: In the Florida Computer Crimes Act, which of these terms is undefined?

A. Authorization

B. Network

C. Computer

Correct Answer: A. Authorization

===

Question: 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

Correct Answer: A. He said he had about nine followers, all relatives or close friends.

===