|  |
| --- |
| 1. An IPv4 address looks like? |
| 1. An IPv6 address looks like? |
| 1. What is the RFC that declares reserved IPv4 addresses? Ans: RFC 5737 |
| 1. What is the IP of the localhost or loopback adapter in IPv4 format? 127.0.0.1 |
| 1. What is the link local address in IPv4 format? 169.254.0.0/16 |
| 1. How many potential IP addresses are available in a class A network? 16,777,214 |
| 1. How many potential IP addresses are available in a class B network? 65534 |
| 1. How many potential IP addresses are available in a class C network? 254 |
| 1. What is the IP of the localhost or loopback adapter in IPv6 format? 0:0:0:0:0:0:0:1 |
| 1. What is the link local address in IPv6 format? FE80::/10 |
| 1. What is the appropriate CIDR notation for 256 available addresses? 255.255.255.0 /24 |
| 1. How many hosts does a CIDR notation of /23 provide? 510 hosts |
| 1. Which of the following is used to identify wireless networks across multiple Access Points? ESSID |
| 1. Which of the following is the MAC address of the Access Point Radio? BSSID |
| 1. Which of the following is not an Authentication Method? |
| 1. What command line tool is used to view a system's network information? Ipconfig -a |
| 1. What command do I run to see what services/ports are in use and what is connected? Netstat -anob |
| 1. In Windows, I would use which NET command to connect/map a network drive? Net use |
| 1. Using the simple RISK equation, what is the risk of not applying a patch that costs $100 per system   in an environment with 200 systems with a 50% probability of occuring? 10000 |
| 1. What Act, from 1974, was updated in 2004 to provide further restrictions on the use of an   individual's Social Security Number? Privacy Act of 1974 |
| 1. What Act, from 1984, established criminal offenses for password trafficking, insertion of malicious code, and   knowledgeable and unauthorized access to Government systems? Computer fraud and abuse act 1984 |
| 1. What Act, from 1987, established the National Informaiton Assurance Partnership which establishes an   international common criteria to evaluate them? Computer Security Act 1987 |
| 1. What Act, from 1996, implemented electronic healthcare transactions? HEALTH INSURANCE PORTABILITY AND   ACCOUNTABILITY ACT 1996 |
| 1. What Act, from 1998, made it legal to crack copyright protection to conduct encryption research,   assess product interoperability, and test computer security systems? Digital Milleninuim Copyright Act of 1998 |
| 1. What Act, from 1999, implemented protection and usage rules for Financial Electronic transactions? GRAMM-LEACH-   BLILEY ACT OF 1999 |
| 1. What Act, from 2002 and based on California's SB1386, requires protection of Personally Identifiable   Informaiton (PII)? SAFE DATA ACT(2002) |
| 1. In Maryland, damage caused in a computer related crime dictates a Felony charge if the the amount   is over what amount? 10000 |
| 1. If you have been contracted to perform an attack against a target system, you are what type of   hacker? White Hat hacker |
| 1. Which of the following describes an attacker who goes after a target to draw attention to a cause? Hactivist |
| 1. What level of knowledge about hacking does a script kiddie have? Low |
| 1. Which of the following does an ethical hacker require to start evaluating a system? Permission |
| 1. A white box test means the tester has which of the following? Complete knowledge |
| 1. Which of the following descirbes a hacker who attacks without regard for being caught or punished?   Suicide Hackers |
| 1. What is a code of ethics? description of expected behavior |
| 1. The group Anonymous is an example of what? Hacktivists |
| 1. Companies may require a penetration test for which of the following reasons?   Network performance is not the goal of security audits or penetration tests. |
| 1. What should a pentester do prior to initiating a new penetration test? Permission |
| 1. Which of the following best describes what a hacktivist does?   A hacktivist engages in mischief for political reasons |
| 1. Which of the following best describes what a suicide hacker does?   A suicide hacker does not worry about stealth or otherwise conceal their activities but is more concerned with  forwarding an agenda |
| 1. Which type of hacker may use their skills for both benign and malicious goals at different times? Grey Hat |
| 1. What separates a suicide hacker from the other hackers? |
| 1. Which of the following would most likely engage in the persuit of vulnerability research? White Hat |
| 1. Vulnerability research deals with which of the following? passively uncovering weaknesses |
| 1. How is black box testing performed? no knowledge |
| 1. A contract is important because it does what? proof that permission and parameters were established. |
| 1. What does TOE stand for? target of evaluation |
| 1. Which of the following best describes a vulnerability? vulnerability is a weakness |
| 1. In which phase of the attack methodology do we try to identify hosts that we can then look for   vulnerabilities on? Ans: VULNERABILITY IDENTIFICATION |
| 1. In which phase of the attack methodology do we use google and social media to learn about our   target? RECONNAISSANCE |
| 1. In which phase of the attack methodology do we correlate open ports and running services to a   potential attack vector? SCANNING AND ENUMERATION |
| 1. In which phase of the attack methodology do we actually "break in" to a system? EXPLOITATION |
| 1. Which of the following best describes footprinting? investigation of a target |
| 1. Which of the following is not typically used during footprinting? port scanning |
| 1. Why use Google hacking? to fine-tune search results |
| 1. What is the role of social engineering? to gain information from human beings |
| 1. What is EDGAR used to do? check financial filings |
| 1. Which of the following can be used to tweak or fine-tune search results? operators |
| 1. Which of the following can an attacker use to determine the technology and structure within an   organization? Job boards |
| 1. Which of the following can be used to assess physical security? street views |
| 1. Which of the following can help you determine business processes of your target through human   interaction? social engineering |
| 1. The Wayback Machine is used to do which of the following? view archived versions of websites |
| 1. Which record will reveal information about a mail server for a domain? MX |
| 1. Which tool can be used to view web server information? net craft |
| 1. What can be configured in most search engines to monitor and alert you of changes to content? alerts |
| 1. What phase comes after footprinting? scanning |
| 1. If you can't gain enough information directly from a target, what is another option? competitive analysis |
| 1. What is the purpose of social engineering? gain info from a human being |
| 1. Which of the following would be a very effective source of information as it relates to social   engineering? social networking |
| 1. Footprinting can determine all of the following except? distribution |
| 1. Footprinting has two phased. What are they? active and passive |
| 1. Which tool can trace the path of a packet? tracert |
| 1. Which of the following is an example of Technical Reconnaissance?   SOCIAL ENGINEERING,REGISTRATION INFORMATION,OPEN SOURCE INTELLIGENCE,SOCIALMEDIA |
| 1. Which of the following is an example of "Low-Tech" Reconnaissance?   VISITING TARGET, BREAKING INTO TARGET, DUMPSTER DIVING,SOCIAL ENGINEERING |
| 1. Baiting is an example of Social Engineering using?   USB/CD/DVD |
| 1. Pretending to be a vendor or recruiter and calling a target is an example of? SOCIAL ENGINEERING |
| 1. The Domain Name Registration records provide which of the following? DOMAIN EXPIRATION DATE,   POINT OF CONTACT, AND ANY ADMIN INFO |
| 1. Open Source Intelligence requires us to access the target systems directly? No |
| 1. Shodan is an example of? osint |
| 1. Which of the following is the best search engine to find all Linksys WRT54G routers attached to   the internet? SHOWDANHQ.COM |
| 1. Bing can be BEST used to identify? IP ADDRESS CO-LOCATION |
| 1. In Google Hacking, what would you use to find all PDF documents within HCC's website? site:hcc.edu filetype:pdf |
| 1. In Google Hacking, what would you use to find all webservers with Directory Browsing enabled? intitle:index.of |
| 1. What file is available on most websites that tells you about portions of the website that may be sensitive in   an administrator's attempt to "secure" the site? Robots.txt |
| 1. Using the Harvester, what command would allow me to search for the first 500 google results   for HCC email addresses? theharvester -d hcc.edu -l 500 -b google |
| 1. Using the Harvester, what command would allow me to search for the first 200 Linkedin results   for Microsoft employees? theharvester -d microsoft.com -l 200 -b linkedin |
| 1. Which of the following is used for banner grabbing? telnet |
| 1. Which of the following is used for identifying a web server OS? netcraft |
| 1. Which of the following is used to perform customized network scans? nmap |
| 1. Which of the following is not a flag on a packet? END |
| 1. A SYN attack used which protocol? TCP |
| 1. Which of the following types of attack has no flags set? null |
| 1. What is missing from a half-open scan? ACK |
| 1. During a FIN scan, what indicates that a port is closed? RST |
| 1. During a XMAS tree scan, what indicates a port is closed? RST |
| 1. What is the three-way handshake? The opening of a TCP connection. SYN -> SYN/ACK -> ACK |
| 1. A full-open scan means that the three-way handshake has been completed.   What is the difference between this and a half-open scan? Final ACK is never sent in a half-open scan |
| 1. What is the sequence of the three-way handshake? SYN -> SYN/ACK -> ACK |
| 1. What is an ICMP echo scan? A ping sweep. Submits a ping to all targets |
| 1. Which best describes a vulnerability scan? A way to automate the detection of vulnerabilities |
| 1. What is the purpose of a proxy? To hide info/location of the person conducting the scan |
| 1. What is TOR used for? TOR is used to hide the person creating a connection by routing requests through   onion routing |
| 1. Why would you need to use a proxy to perform scanning? To make yourself more anonymous |
| 1. A vulnerability scan is a good way to do what? Find open ports, weaknesses, and vulnerabilities |
| 1. A banner can do what? Identify a service |
| 1. NMAP is required to perform what type of scan? port scanning |
| 1. In TCP/IP, what is the correct way to open a connection to a remote system using the 3-way handshake?   SYN -> SYN/ACK -> ACK |
| 1. In TCP/IP, what is the correct way to close a connection with a remote system using the 3-way handshake?   FIN -> FIN/ACK -> ACK |
| 1. Who created NMAP? Gordon Lyon |
| 1. Which NMAP scan type attempts to complete the 3-way handshake with each scanned port?   TCP Connect Scan |
| 1. Which NMAP scan type only sends the initial SYN request and waits for an ACK to detect the   open port? SYN Scan/Half-open scan |
| 1. A NMAP scan type with FIN, URG, and PUSH code bits set is which type of scan type? Xmas Scan |
| 1. When using a NMAP TCP FIN (-sF) scan type, what response indicates the port may be open? SYN/ACK |
| 1. Which NMAP scan type allows an attacker to get past some packet filtering devices? ICMP Echo Scan |
| 1. Which two scan types are known as NMAP PING scans? Network scan (-sN) and TCP/SYN Scan (-SP) or (-PS) |
| 1. Which of the following NMAP command line strings will scan a full class C network, perform version   detection, and output to a file? nmap -sn 192.168.1.1/24 -oN filename.txt |
| 1. Which NMAP -T option would you use in a network where you want to minimize any detection and   potential unintended consequences of your scan? -t0 |
| 1. Which NMAP -T option would you use in a network where you need to find out as much information as quick as   possible but don't want to encounter any traffic loss? -t3 |
| 1. Which NMAP scan sends one packet ever 15 seconds? -t1 |
| 1. Which of the following NMAP command line strings will scan a target for specific web ports, and   perform version detection of those ports? nmap -sV -p [port number] |
| 1. Identify which of the follow this war chalking graphic represents |
| 1. Enumeration is useful to system hacking because it provides which of the following? Usernames |
| 1. Enumeration does not uncover which of the following pieces of information? Ports |
| 1. \_\_\_\_\_\_\_ involves grabbing a copy of a zone file. Zone Transfer |
| 1. Which of the following would confirm a user named chell in SMTP? vrfy chell |
| 1. VRFY is used to do which of the following? Validate an email address |
| 1. \_\_\_\_\_\_\_ is a method for expanding an email list. EXPN |
| 1. An attacker can use \_\_\_\_\_\_ to enumerate users on a system. NetBIOS |
| 1. A \_\_\_\_\_\_\_ is used to connect to a remote system using NetBIOS. NULL session |
| 1. \_\_\_\_\_\_\_ is used to synchronize clocks on a network. NTP |
| 1. Port number \_\_\_\_\_ is used for SMTP. 25 |
| 1. Port number \_\_\_\_\_ is used by DNS for zone transfers. 53 TCP |
| 1. Which command can be used to view NetBIOS information? nbtstat |
| 1. SNScan is used to access information for which protocol? SMNP |
| 1. SMTP is used to perform which function? email |
| 1. Which ports does SNMP use to function? 161 and 162 |
| 1. LDAP is used to perform which function? Query a database |
| 1. SNMP is used to do which of the following? Monitor Network devices |
| 1. SNMP is used to perform which function in relation to hardware? Trap Messages |
| 1. What is a SID used to do? Identify a user |
| 1. A DNS zone transfer is used to do which of the following? Synchronize server information |
| 1. OpenVAS is an example of what? Free General Scanner |
| 1. A vulnerability is known as the intersection of which three elements?   System susceptibility or flaw  Access to the flaw  Exploitation of the flaw |
| 1. A vulnerability is known as the intersection of exploiting a flaw, access to a flaw, and what? |
| 1. Which of the following is a publicly available vulnerability list? NIST Vulnerability Database, |
| 1. What personal software inspection tool can you use to scan your own system to ensure your applications   are up to date? Secunia PSI |
| 1. What Microsoft based tool can you use to scan your Windows system to check for security issues?   Microsoft Baseline Secuirty Analyzer (MBSA) |
| 1. What network based vulnerability scanner can be used to audit your systems for vulnerabilities,   as well as compliance checks? Nessus |
| 1. Enumeration is useful to system hacking because it provides \_\_\_\_\_\_\_\_. Usernames |
| 1. What does the enumeration phase NOT discover? Ports |
| 1. How would you use Netcat to set up a server on a system? nc -l -p 192.168.1.1 |
| 1. \_\_\_\_\_\_\_ is the process of exploiting services on a system. System hacking |
| 1. How is a brute-force attack performed? |
| 1. A \_\_\_\_\_\_\_ is a type of offline attack. Rainbow Attack |
| 1. An attacker can use a(n) \_\_\_\_\_\_\_\_ to return to a system. Backdoor |
| 1. A \_\_\_\_\_\_\_ is used to represent a password. Hash |
| 1. A \_\_\_\_\_\_\_ is a file used to store passwords. SAM DB |
| 1. \_\_\_\_\_\_\_ is a hash used to store passwords in older Windows systems. LM |
| 1. \_\_\_\_\_\_\_ is used to partially encrypt the SAM. syskey |
| 1. Which system should be used instead of LM or NTLM? kerberos |
| 1. NTLM provides what benefit versus LM? Stronger protocol |
| 1. ADS requires what to be present? NTFS |
| 1. What utility may be used to stop auditing or logging of events? Auditpol |
| 1. On newer Windows systems, what hashing mechanism is disabled? LM |
| 1. Which of the following is a utility used to reset passwords? TRK |
| 1. A good defense against password guessing is \_\_\_\_\_\_\_. Complex Passwords |
| 1. If a domain controller is not present, what can be used instead? NTLMv2 |
| 1. Alternate Data Streams are supported in which file systems? NTFS |
| 1. What is an exploit? |
| 1. Which of the following are types of exploits? |
| 1. Core Impact is an example of what? Exploit Framework/Pen Test Suite |
| 1. Exploit-DB is a resource to find? Exploits |
| 1. Packet Storm is a resource to find? Exploits |
| 1. Who created Metasploit? HD Moore |
| 1. Metasploit was originally written in which programming language? Perl |
| 1. Metasploit was ported to which programming language in 2006? Ruby |
| 1. Which company purchased Metasploit in 2009? Rapid7 |
| 1. In Metasploit, a port scanner module would be an example of what? auxillary modules |
| 1. In Metasploit, the Meterpreter shell is an example of what? |
| 1. In Metasploit, what command do you use to list the sessions of the systems you have exploited? -l |
| 1. Given the following set of Metasploit Commands, which command is missing in order to make this work? |
| 1. When using Meterpreter, what command shows all processes on the remote system? ps |
| 1. When using Meterpreter, what command provides you with the Windows Password store? hashdump |
| 1. What is the name of the Graphical Front End to Metasploit? Armitage |