SEC 275 Index

Created by: Evan Lin

#

. *[b1.10,p133]* Current directory
.. *[b1.10,p133]* Parent directory
/ *[b1.9,p124]* Root of file system
0-Day *[b3.5,p86]* undiscovered exploit
12V power connector *[b1.2,p39]* For powering motherboard
~ *[b1.9,p124]* Home of current user's directory

Aa

A Record *[b1.20,p296]* Address mapping record - maps domain name to IPv4 Address
AAAA Record *[b1.20,p296]* Address mapping record - maps domain name to IPv6 Address
Access Control List (Windows) *[b2.13,p293]* Stores who is allowed which level of access
Active Directory *[b2.12;3.16,p263;324]* Central hub for controlling a network of computers
Add-ins *[b3.15,p316]* Microsoft Word allows for third parties to write add ins
Adminer *[b1.24,p345]* Graphical frontend for databases
Administrator (Windows Account Type) *[b2.13,p281]* Able to make changes that impact all users
Administrator (Windows) *[b2.13,p281]* Default account with nearly full control over machine
Administrators (Windows Default Group) *[b2.13,p287]* Members have full access to computer
AES/Advanced Encryption Standard *[b3.1,p13]* Keys of size 128;192;256 bits;modern encryption
Air-gapped *[b1.22,p326]* not connected to untrusted networks;ex: internet
Aliases (Windows cmdlets) *[b2.15,p328]* alternative names for common cmdlets
Alternative denial connective *[b1.4,p71]* Logical NAND
AlwaysInstallElevated *[b3.14,p295]* setting that can be enabled through windows group policy
Analytics (Web Servers) *[b1.23,p335]* Collect and analyze data on users of websites
AND *[b1.4,p66]* True if both inputs are true;false otherwise;conjunction connective
Apache *[b1.16,p234]* Generic web server
APFS *[b1.5,p86]* Apple File System;for MacOS
Application Layer (OSI) *[b1.21,p303]* ex: HTTP or FTP protocol
Application Layer (TCP/IP) *[b1.21,p311]* Same as for OSI;HTTP;FTP
Apropos (Linux) *[b1.13,p176]* command to pull up manual page on tools (Linux)
Apt-get (Linux) *[b1.14,p203]* Package manager on Linux
Argument from command line (C) *[b2.6,p177]* read data from command line in C
Arithmetic Logic Unit (ALU) *[b2.16,p334]* Part of the CPU responsible for performing arithmetic and logical operations
ARP Spoofing/Poisoning *[b3.16,p327]* Lie about MAC addresses to other computers
ARP/Address Resolution Protocol *[b1.21,p316]* How the source computer knows the MAC address of the destination computer
ARP/Address Resolution Protocol Cache *[b3.16,p322]* Lists IP addresses the computer has communicated with
Array (C) *[b2.6,p174]* collection of data
AS (SQL) *[b2.8,p207]* set an alias for a table or field
ASCII *[b1.3,p56]* Text stored as numbers;binary correlates to a character
ASLR/Address Space Layout Randomization *[b3.11,p202]* Randomize memory addresses every time a program gets loaded
Assembly *[b2.17;3.11,p348;196]* Programming language that CPU understands
Assertion *[b2.4,p133]* used to ensure that something is true
Asymmetric Cryptography *[b1.28;3.1,p385;17]* 2 keys;public and private linked mathematically
ATX *[b1.2,p22]* Motherboard size
ATX Connection *[b1.2,p39]* Connection that runs into motherboard
Authentication (Encryption) *[b3.1,p9]* Origin of message can be verified by the recipient
Authoritative Name Server *[b1.19;1.25,p292;351]* The name server that control the mapping between the domain name and IP address for a domain
Autopsy *[b,p]* GUI-digital forensics tool
Availability (Server) *[b3.3,p45]* Systems should be accessible when needed

Bb

Bare Metal Hypervisor *[b1.8,p107]* Type 1 Hypervisor: No host operating system;all virtual machines run directly on hardware
Base64 *[b1.3;3.7,p59;122]* binary to text encoding system
Bash (Linux) *[b1.9,p124]* Bourne Again Shell;path /bin/bash
Big-endian Format *[b3.11,p194]* LSB is stored last
bin folder (Linux) *[b1.10,p134]* Store executable files
Binary *[b1.3,p48]* How computers count
Binwalk *[b3.6,p100]* Tool to search a binary image for executables
BIOS *[b1.7,p102]* Basic input output system;stored on motherboard;prepares hardware to load the bootloader
Bit *[b1.3,p44]* Smallest unit of data that can be stored on computer;either 1 or 0
Block Storage (Cloud) *[b2.18,p363]* Data is split into blocks of equal size and assigned a unique identifier
Blue Team *[b3.3;3.6,p{40;42};113]* Acts as defenders
Boolean *[b1.3;2.1,p44;17]* True or False
Boolean Logic *[b1.4,p64]* Gates that take 2 inputs and produce 1 output;0 = 0 volts;1 = 5 volts
boot folder (Linux) *[b1.10,p134]* Files needed for boot up
Bootkit *[b3.15,p313]* write malware directly to disk
Bootloader *[b1.7,p101]* Program loaded by BIOS;responsible for loading the OS
Branch (Git) *[b2.1,p11]* Allow you to work on a specific feature;before merging
break (Python) *[b2.2,p76]* used to exit a loop in python
breakpoint *[b2.17,p345]* a marker that tells GDB to pause at a certain point in a function
BSD syntax (Linux) *[b1.14,p191]* alternative syntax to - params
Buffer Overflow *[b2.6;3.11,p175;{185;188}]* putting more data in a memory address than was allocated
Buffer Overflow (BLUE) *[b3.11,p202]* Check input length
Bus (Topology) *[b1.17,p248]* All computers connected with an ethernet cable
Buses *[b1.2,p23]* Physical connection between motherboard and other parts used to move data
Byte *[b1.3,p44]* 8 bits

Cc

C *[b2.1;2.5,p10;153]* Close to a low-level programming language
Caching (DNS) *[b1.20,p293]* IP for domain names may be stored (cached) to load web pages faster
Caesar Cipher *[b3.1,p13]* Encryption done by shifting letters a certain amount
Cat (Linux) *[b1.12,p169]* command to concatenate and print to terminal (Linux)
cd (Linux) *[b1.10,p132]* Change directory command linux
cd (Windows) *[b2.14,p301]* Change Directory;ex: cd \ takes to root of windows file system
cdrom folder (Linux) *[b1.10,p134]* Access cdrom files
CEO Fraud *[b3.12,p249]* A type of spear phishing (aka whaling) targeting big names at the company
CeWL (RED) *[b3.5,p76]* tool used to pick out common words used on a site
Chain of Custody *[b3.6,p98]* Who was responsible for this evidence during what time frame?
Chaining commands (Linux) *[b1.13,p186]* Use ;or | to chain commands
Change directory *[b1.10,p132]* Change directory command linux
Changing Drives (Windows) *[b2.14,p302]* access other drive by typing name of other drive followed by :
char (C) *[b2.5,p162]* a character
Chgrp (Linux) *[b1.10,p138]* Linux command to change group owner of file
Child Account (Windows) *[b2.13,p281]* Standard account with parental controls
Chown (Linux) *[b1.10,p137]* Linux command to change owner of file
Class (python) *[b2.2,p99]* A template used to build objects
Classless Inter-Domain Routing/CIDR *[b1.18,p266]* shorthand for writing subnet masks
Clear (Linux) *[b1.11,p163]* linux command to clear terminal
Clickjacking (BLUE) *[b3.10,p168]* Use X-Frame-Options header in HTTP response
Clickjacking (RED) *[b3.10,p164]* When the user is tricked into clicking on something without realizing they clicked it
Client-side *[b1.23,p332]* Device being used to connect to website
Clock Speed *[b1.2,p24]* Instructions/second a core can process;ex: 4GHz = 4 billion instructions/second
Cloud Computing *[b1.6,p88]* Hosting applications and services in the cloud (not on-site)
Cloud Storage *[b2.18,p363]* Store data in cloud
Cluster *[b1.5,p81;82]* Smallest section of disk that can be used to store a file;has a memory address
cmdlet (Windows) *[b2.15,p324]* lightweight command used within PowerShell
CNAME Record *[b1.20,p296]* Canonical Name used for creating aliases for a domain
Command Injection (BLUE) *[b3.9,p148]* Program the application instead of using 3rd party command line tools
Command Injection (RED) *[b3.9,p142]* Takes advantage of how web applications process user input
Command Prompt (Windows) *[b2.14,p298]* Command line interpreter for Windows OS
Comment (C) *[b2.6,p170]* using // or /* */
Comment (Python) *[b2.1,p48]* add notes to code
Commit (Git) *[b2.1,p11]* Incremental change to a repository
Companies House (RED) *[b3.5,p75]* Get info on officers at a company
Compiled *[b2.1,p9]* Converting a program into machine code and saved as an executable
Computer Program *[b2.1,p9]* series of instructions for the processor of a computer
Conditional (C) *[b2.6,p171]* nearly the same as for python
Conditional (Python) *[b2.2,p53]* Check if a condition has been met
Confidentiality (Server) *[b3.3,p45]* Access to systems should only be shared amongst authorized persons or organizations
Conjunction connective *[b1.4,p66]* Logical AND
Connective *[b1.4,p66]* Used to connect 2 or more propositions
Connectors (PSU) *[b1.2,p37]* For power supply units SATA;main ATX;12V;PCI-E
Constraints (SQL) *[b2.11,p251]* rules for columns in an SQL table
Constructor (classes and objects) *[b2.2,p102]* allows for easier instantiation of a class
Container *[b2.19,p366;368]* lightweight;low cost packaging of applications;libraries and configurations
Containment (Incident Response) *[b3.6,p107]* Stop the attacker
Context Switching *[b1.2,p24]* Sharing processing time between multiple applications
Contingency *[b1.4,p78]* Statement that can either be true or false;based on inputs
Contradiction *[b1.4,p78]* Statement that is always false;no matter inputs
Cookies *[b1.16;3.10,p243;163]* Tiny file on user's computer
copy (Windows) *[b2.14,p306]* used to copy files to a different location
Cores (Processor) *[b1.2,p24]* Executes instructions
Cp (Linux) *[b1.12,p165]* command to copy (Linux)
CPU/Processor *[b1.2;2.16,p24;334]* Central Processing Unit;executes instructions in programs
Credential *[b3.14,p283]* may find passwords laying around in file system
Credential Harvesting *[b3.12,p246]* Relies on a attacker cloning a site and hosting it;tricking targets into giving login info
Crontab (Linux) *[b1.14,p200]* schedule tasks
Cross Site Request Forgery/CSRF (BLUE) *[b3.10,p170]* Make sure every HTTP request comes from the same origin;use CSRF Token
Cross Site Request Forgery/CSRF (RED) *[b3.10,p169]* Tricking someone to click on a link that leads to an action not in their best interest
Cross Site Scripting/XSS (BLUE) *[b3.9,p156]* Sanitize user input
Cross Site Scripting/XSS (RED) *[b3.9,p154]* run javascript code in the browser of clients
Crypture *[b3.6,p100]* Command line tool that performs steganography
CSRF Token *[b3.10,p170]* random value unique to a session;generated on the page before form submission
Cyclic Pattern *[b3.11,p191]* Pattern in which any 4 bytes are unique

Dd

Data *[b2.16,p341]* Binary data to read
Data Link Layer (OSI) *[b1.21,p308]* encoding/decoding packets into bits
Database *[b2.7,p189]* Store of data
Database Creation (SQL) *[b2.11,p247]* creating a database in SQL
Database Management System *[b2.7,p189]* Used to manage a database
Database Server *[b1.24,p343]* computer system that provides other computers with services relating to accessing and retrieving data
Datatype (SQL) *[b2.11,p249]* setting up tables in SQL
DDoS/Distributed Denial of Service *[b1.21,p318]* Using a huge number of systems to attack a target
Deb (Linux) *[b1.14,p207]* Software packaged for a linux distribution -> for debian
Debugging *[b2.4,p148]* Getting rid of bugs in programs

Default Accounts (Windows) *[b2.13,p281]* users created upon installing windows
Default Parameters (Python) *[b2.2,p82]* params that don't necessarily need to be set when calling the function
DefaultAccount (Windows) *[b2.13,p281]* Used as a template for all other user accounts
Defense in Depth *[b3.3;3.16,p44;321]* Setting up multiple defensive positions and being prepared to fall back to pre-arranged locations
Defensive programming *[b2.4,p133]* expect the unexpected
del (Windows) *[b2.14,p309]* used to delete a file
DEP (Windows) *[b3.11,p202]* Separate stack into areas for code and data
DES (Encryption) *[b3.1,p10]* Old form of encryption -> don't use
dev folder (Linux) *[b1.10,p134]* Files for hardware components
DHCP/Dynamic Host Configuration Protocol *[b1.21,p300]* Automatically assign network configurations to each host
Dictionary (Python) *[b2.1,p39]* collection of things;key and value pairs
dir (Windows) *[b2.14,p303]* view directory contents
Dirb (BLUE) *[b3.5,p84]* Avoid putting sensitive documents on the internet;watch server logs
Dirb (RED) *[b3.5,p84]* tool that uses wordlist to craft HTTP requestions to target
Directory Traversal (BLUE) *[b3.10,p173]* Don't use user input when making system calls
Directory Traversal (RED) *[b3.10,p172]* reference files outside of normal path
DirtyCOW *[b3.13,p258]* famous linux kernel exploit
Disjunction connective *[b1.4,p68]* Logical OR
Disk Capture *[b3.7,p120]* Produce an image of a disk
Display Port *[b1.2,p34]* A/V (Audio/visual) output;modern version of HDMI
DISTINCT (SQL) *[b2.8,p205]* return data without duplicates
DKIM/Domain Keys Identified Mail *[b1.19,p285;287]* Use public/private keys to ensure mail is legitimate
dll *[b3.15,p316]* format to hold executable code
DMZ/Demilitarized zone *[b3.16,p321]* High-risk area of network
DNS over HTTPS *[b1.25,p356]* DNS queries sent over HTTP or HTTP/2 instead of UDP
DNS over TLS *[b1.25,p356]* Encrypt DNS with TLS
DNS Recon (BLUE) *[b3.5,p83]* Avoid exposing internal DNS to outside world
DNS Recon (RED) *[b3.5,p82]* Find domain names to find information
DNS Records *[b1.20,p296]* A Record;AAAA Record;CNAME Record;MX Record;NS Record;PTR Record;TXT Record
DNS/Domain Name System *[b1.19;1.25,p290;350]* Glue that holds internet together;translates domain name into IP address
DNSSEC *[b1.25,p357;358;366]* Focused on cache poisoning
Docker *[b2.19,p368]* Container manager
Docker CLI *[b2.19,p369]* used to give instructions to docker
Docker Client (Container) *[b2.19,p368]* Component used to issue instructions
Docker Daemon (Container) *[b2.19,p368]* Does the real work behind containers -> building;running;delivery
Docker Hub (Container) *[b2.19,p368]* Registry of docker images
DOS Prompt *[b2.14,p298]* Command line interpreter for Windows OS
DoS/Denial of Service *[b1.21,p317]* Consume resources;prevent real customers from connecting
double (C) *[b2.5,p162]* number with a decimal point;double precision
Dpkg (Linux) *[b1.14,p207]* Install .deb or .rpm packages on linux
Drive by download *[b3.12,p241]* Attacker compromises a site the target visits often to compromise them when they visit
Drives (Windows) *[b2.14,p302]* hard drive or connected usb device
DROP (SQL) *[b2.11,p256]* delete a table
DVI *[b1.2,p33]* A/V (Audio/visual) output;more modern VGA

Ee

EAX *[b2.16,p335]* General Purpose Register
EBP *[b2.16,p336]* Base Pointer Register
EBX *[b2.16,p335]* General Purpose Register
Echo Hiding *[b3.6,p100]* Algorithm used with audio steganography
ECX *[b2.16,p335]* General Purpose Register
EDI *[b2.16,p336]* Destination Index Register
EDX *[b2.16,p335]* General Purpose Register
EIP *[b2.16;3.11,p336;190]* Special Purpose Register (Instruction pointer)
ELIF (Python) *[b2.2,p63]* executed when the if statements before it fail (python)
ELK/Elasticsearch;Logstash;Kibana *[b1.26,p364]* Processing and querying
ELSE (Python) *[b2.2,p63]* executed when the conditions before fail
Email Forensics *[b3.7,p122]* study source and content of emails
Email Server *[b1.19;1.27,p280;369]* Email is text sent from 1 email server to another
Email Spoofing *[b1.19,p285]* Pretending to be a different person when sending an email
EnCase E01 files *[b3.7,p118]* produced when imaging hard disks
Encoding *[b1.3;3.1,p59;12]* Take data in 1 format and package it as another;used for storage and transfer;not secure
Encrypted Disk Detector *[b3.7,p120]* By Magnet: Tool used to determine if full disk encryption is enabled
Encryption *[b3.1,p9]* Convert data from 1 form to another;where only the intended recipient can understand it
End of support *[b3.12,p234]* when developers no longer support a software
Environment Variables (Linux) *[b1.10;3.13,p144;265]* Data stored in Linux terminal
Eradication (Incident Response) *[b3.6,p108]* Get rid of attacker
ESI *[b2.16,p336]* Source Index Register
ESP *[b2.16,p336]* Stack Pointer Register
etc folder (Linux) *[b1.10,p134]* Configuration files
EternalBlue *[b3.11,p183]* Leaked NSA exploit that led to Wannacry
Evidence *[b3.6,p97]* Processes if evidence is to be used in court
Exceptions (python) *[b2.2,p106]* An object that python uses as part of its error management system
Exchange *[b1.19,p283]* Software using MAPI protocol restricted to Windows
Exclusive disjunction connective *[b1.4,p75]* Logical XOR
exFAT *[b1.5,p83]* For USB drives and removable media;no file size limit;Supports Windows;Mac;Linux
Exfiltration *[b3.3;3.17,p49;334]* Exfiltrate data from system
Exfiltration and the Cloud *[b3.17,p342]* Good for covering tracks -> connections can hide among all the other traffic
Exfiltration via DNS *[b3.17,p339]* make DNS queries to subdomains to exfiltrate data
Exfiltration via HTTPS *[b3.17,p335]* common method to exfiltrate data
Exfiltration via ICMP *[b3.17,p340]* put data in the data field of ICMP protocol
Exfiltration via IRC/Internet Relay Chat *[b3.17,p337]* older chat protocol
Exfiltration via SMTP *[b3.17,p336]* good method;as people will be emailing all day
Exfiltration via Sound *[b3.17,p341]* used when there is an air-gapped network close to a network connected to the internet
ExifTool (Linux) *[b3.5,p64]* Used to examine metadata
EXISTS (SQL) *[b2.10,p235]* check for existence of a record in a table
exploit-db *[b3.11,p184]* database of exploits

Exploiting FTP Service *[b3.12,p212]* walkthrough of exploiting an FTP server
Exploiting Kernel *[b3.13,p257]* master of the kernel controls the computer
Exploiting Kernel (Windows) *[b3.14,p280]* used to gain SYSTEM level privileges
Exploiting Services *[b3.13,p256]* Find running services and find exploits for them
Exploiting Web Application *[b3.12,p219]* walkthrough of exploiting a web application
EXT3 *[b1.5;3.7,p85;119]* Extended file system 3;used in Linux (old)
EXT4 *[b1.5;3.7,p85;119]* Extended file system 4;used in Linux (modern)
Extract Passwords from Memory *[b3.16,p324;329]* Access RAM to extract passwords

Ff

FAT32 *[b1.5;3.7,p83;119]* For windows 95;Uses File Allocation Table to map clusters;Max 4GB;No permissions
Fetch-Decode-Execute *[b2.16,p337]* How the CPU executes instructions
fgets (C) *[b2.6,p176]* better way to take input in C
File (Linux) *[b1.13,p182]* command to see type of a file (Linux)
File Deletion *[b1.5;3.7,p81;121]* Index of where the data is found is deleted;but the data is not deleted
File Headers *[b1.3;3.8,p61;138]* Indicates the type of the file
File Inclusion (BLUE) *[b3.9,p151]* avoid dynamically including files based on user input
File Inclusion (Local) *[b3.9,p150]* load arbitrary files on the file system
File Inclusion (RED) *[b3.9,p150]* when a web page includes resources based on user input
File Inclusion (Remote) *[b3.9,p151]* load arbitrary files on remote file systems
File Permissions (Linux) *[b1.10,p136]* Who can do what to a file
File Storage (Cloud) *[b2.18,p363]* Data stored in a file system
File System *[b1.5;3.7,p81;118]* Determine how files are stored on a device
File System forensics *[b3.7,p118]* extract info from hard disk images
File Transfer Protocol *[b1.18,p273;276]* Used to uploading/downloading files to/from FTP server
File Upload Vulnerability (BLUE) *[b3.10,p177]* Restrict file types with a whitelist;scan into the files;rename files
File Upload Vulnerability (RED) *[b3.10,p175]* Upload a file and load the webpage to execute code
Find (Linux) *[b1.12,p171]* command to find files on system (Linux)
find (Windows) *[b2.14,p312]* searches inside files for specified strings
Fins *[b1.2,p36]* Create more surface area for heat dissipation
float (C) *[b2.5,p162]* number with decimal point;single-precision
Float (Python) *[b2.1,p17]* number with decimal point
Folder Permissions (Windows) *[b3.14,p294]* find a service which has an executable in a folder you can modify
Folder Structure Linux *[b1.10,p134]* Linux file system starting from /
For Loop (C) *[b2.6,p172]* more traditional version compared to python
For loop (Python) *[b2.2,p65]* iterate a set number of times
Foreign Key *[b2.7,p190]* Primary Key of another row stored in a different table
Forensics *[b3.6,p96]* Process of preserving and evaluating electronic data
Format String (C) *[b3.11,p205]* Inject format string specifiers into printf function in C
Format String (C) (BLUE) *[b3.11,p208]* Don't use printf without format string specifiers
Format String Specifier *[b2.5,p158;163;164]* used in printf in C
Forward Lookup (DNS) *[b1.20,p294]* Translate domain name into IP
Four pin connector *[b1.2,p38]* Four pin peripheral connector for fans
FROM (SQL) *[b2.8,p198]* identify which table to retrieve data from
FTK Imager *[b3.7,p120;125]* By AccessData: Used to take a live capture
Full Disk Encryption *[b3.7,p120]* data is encrypted when drive is at rest
FULL JOIN (SQL) *[b2.10,p240]* returns results from both tables
Function (C) *[b2.5,p167]* methods in C
Function (Python) *[b2.2,p79]* split code into smaller chunks that can be called

Gg

GDB (GNU Debugger) *[b2.17,p344]* Used to examine binary executables
GDB example: password *[b2.17,p353]* An example trace through a password executable
Get-ChildItem (Windows) *[b2.15,p327]* list contents of folder;similar to dir
Get-Command (Windows) *[b2.15,p326]* find all cmdlets that use a certain noun or verb
Get-Content (Windows) *[b2.15,p327]* display contents of file
Get-Process (Windows) *[b2.15,p327]* gather info on running processes
getsystem (Windows) *[b3.14,p277]* Switch from admin account to SYSTEM account
Gibibyte (GiB) *[b1.3,p45]* 1024 mebibytes
Gigabyte (GB) *[b1.3,p44]* 1000 megabytes
Git *[b2.1,p11]* Track changes to a programming project
GPU *[b1.2,p30]* Graphics Processing Unit;optional;for number crunching (crack passwords)
Graphics Card *[b1.2,p30]* Holds GPU;RAM for computer graphics;heatsink;fan
Grep (Linux) *[b1.13,p174]* command to search text within files (Linux)
Groups (Windows) *[b2.13,p287]* Users added to groups inherit the permissions of the group
Guest (Windows) *[b2.13,p281]* Default account for people without actual accounts
Guest Operating System *[b1.8,p105]* Operating system that runs inside the virtual machine
Guests (Windows Default Group) *[b2.13,p287]* Members do not have permanent accounts

Hh

Hard Drive *[b1.2,p28]* Provides data storage
Hash Collision *[b3.6,p105]* When 2 different pieces of data generate the same hash value
Hashing *[b3.1,p22]* One way encryption
haveibeenpwned.com *[b3.5,p79]* find if a email was in a prior breach
HDMI *[b1.2,p34]* A/V (Audio/visual) output;modern version of VGA and DVI
Heap *[b2.6;2.16,p179;340]* Unstructured section of memory
Heat Sink *[b1.2,p36]* Move heat away from sensitive components
Hexadecimal *[b1.3,p52]* Base 16
HFS+ *[b1.5,p86]* Hierarchical File System Plus;for MacOS
Hidden files (Linux) *[b1.10,p142]* files that start with . are hidden
Hidden Files (Windows) *[b2.13,p295]* hidden with the hidden attribute
high-level programming language *[b2.1,p10]* closer to english
History (Linux) *[b1.11,p155]* Holds all commands you have executed
Hives (Windows) *[b3.7,p124]* SAM;SECURITY;SYSTEM;SOFTWARE;DEFAULT
home folder (Linux) *[b1.10,p134]* Home folder for users
Honeypot *[b3.6,p108]* Trap for the attacker
Host Operating System *[b1.8,p105]* Operating System that runs the virtualization software
HTML *[b1.16,p238]* Markup language

HTTP Protocol *[b1.16;1.18,p236;274]* HyperText Transfer Protocol: Series of requests and responses
HTTP Responses *[b1.23,p336]* Collection of HTTP responses
HTTPS (Encryption) *[b3.1,p21]* HTTPS uses both forms of encryption: asymmetric as the connection start;symmetric for the rest
Hub *[b1.17,p250]* Connects computers on a network together (not so smart)
Human Interface Devices *[b1.2,p31]* HIDs = input devices
Hypervisor *[b1.8,p105;107]* Breaks 1:1 relationship between hardware and software;Allows multiple operating systems to share hardware
Hypervisor (Type 1) *[b1.8,p107]* No host operating system;all virtual machines run directly on hardware
Hypervisor (Type 2) *[b1.8,p107]* Virtualization done by software that runs on an operation system

Ii

IaaS *[b1.6,p89]* Infrastructure as a Service;pay-as-you-go;as you need it (storage;networking;computing power)
ICMP/Internet Control Message Protocol *[b1.21,p299]* Transmits error messages and operational information
Identification (Incident Response) *[b3.6,p107]* Identify scope of incident
Image (Container) *[b2.19,p368]* Executable code built up in layers
IMAP/Internet Message Access Protocol *[b1.19;1.27,p283;370]* Most common protocol for accessing emails
Incident Response *[b3.6,p107]* How to respond to and identify threats;minimize effect of attacks
Incident Response - Containment *[b3.6,p107]* Stop the attacker
Incident Response - Eradication *[b3.6,p108]* Get rid of attacker
Incident Response - Identification *[b3.6,p107]* Identify scope of incident
Incident Response - Lessons Learned *[b3.6,p108]* Review attack; figure out what went wrong; prevent it from occurring again
Incident Response - Preparation *[b3.6,p107]* Prepare business to tacker incidents
Incident Response - Recovery *[b3.6,p108]* Return system to full working capacity
Indicators of Compromise *[b3.15,p301]* Find artifacts left behind by attackers
Initial Exploitation *[b3.3,p48]* Gain a foothold somewhere in the network
INNER JOIN (SQL) *[b2.9,p219]* retrieve data that matches a condition in both tables
Input devices *[b1.2,p31]* Send data to computer;ex: mouse;keyboard
Insert Data (SQL) *[b2.11,p253]* put data into tables in SQL
Installed components (Windows) *[b3.15,p309]* Executables run at boot time
Instruction *[b2.16,p341]* Binary data to execute
Integer (C) *[b2.5,p161]* store an int value
Integer (Python) *[b2.1,p17]* whole number
Integer Overflow (BLUE) *[b3.11,p187]* Make sure the integer stays within the correct range
Integer Overflow (RED) *[b3.11,p186]* Bring integer values over max value or under min value
Integrity (Encryption) *[b3.1,p9]* Proof that the message hasn't been changed since it was sent
Integrity (Forensics) *[b3.6,p105]* Identify unauthorized changes to files
Integrity (Server) *[b3.3,p45]* Systems should be accurate;trustworthy and complete
Internet Layer (TCP/IP) *[b1.21,p313]* Routing traffic over network
Internet of Things *[bx,px]* objects embedded with sensors and connected to a network
Interpreted *[b2.1,p9]* Program is converted and executed at the same time
Interrupt *[b1.7,p98]* Signal set to CPU that alerts it of a task requiring immediate attention
Interrupt (Hardware) *[b1.7,p99]* Interrupt generated by hardware;ex: keyboard;mouse
Interrupt (Linux) *[b1.11,p160]* CTRL + C
Interrupt (Software) *[b1.7,p100]* When a piece of software asks the kernel to perform a privileged action on its behalf
Intrusion Detection System (IDS) *[b3.5,p91]* Detects intruders in system
IP Address *[b1.17,p253]* Identifies computer on the network
IP Address (Private) *[b1.17,p253]* Internet facing IP address
IP Address (Public) *[b1.17,p253]* Assigned to computer on local network
IP Ranges (Private) *[b1.18,p267]* Should not be routed to internet
ipconfig (Windows) *[b2.14,p314]* access current settings for network
IPv4 *[b1.18,p262]* xxx.xxx.xxx.xxx format
IPv6 *[b1.18,p264]* xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format
Iterative Lookup (DNS) *[b1.20,p295]* DNS servers point you to the next DNS servers to ask if answer is not found

Jj

JavaScript *[b1.16,p239]* Programming language running in browsers
Job Postings (BLUE) *[b3.5,p74]* use a recruiting service that doesn't list company name
Job Postings (RED) *[b3.5,p73]* look at job postings and what skills they require
JOIN (SQL) *[b2.9,p213]* combine results from 2 or more tables
Joint denial connective *[b1.4,p73]* Logical NOR
Journaling *[b1.5,p85]* Changes to disk are tracked;helps with recovery

Kk

Kali Linux *[b3.4,p55]* Intended for security professionals
Kernel *[b1.7;3.13,p96;257]* First part of operating system to be loaded;has complete control over computer
kernelmode *[b3.15,p312]* type of rootkit
Kibibyte (KiB) *[b1.3,p45]* 1024 bytes
Kill (Linux) *[b1.14,p194]* command to kill a program (Linux)
Kilobyte (kB) *[b1.3,p44]* 1000 bytes
kitrap0d *[b3.14,p281]* exploit for windows XP

Ll

LaaS *[b1.26,p360]* Logging as a service
LAN *[b1.17,p247]* Local Area Network
Lateral Movement *[b3.3;3.16,p49;321]* Spread from initial foothold
Laws *[b3.2,p30]* Learn to protect yourself
LEFT JOIN (SQL) *[b2.9,p222]* return all results from 1st table and only matching results from 2nd table
Less (Linux) *[b1.12,p170]* command for reading long files (Linux)
Lessons Learned (Incident Response) *[b3.6,p108]* Review attack; figure out what went wrong; prevent it from occurring again
lib folder (Linux) *[b1.10,p134]* Shared libraries and kernels
Library (Python) *[b2.2,p93]* modules in python that can add functionality
LinkedIn (RED) *[b3.5,p74]* Social engineering;finding software a company might use
Linux *[b1.9,p114]* Linux kernel;a class of operating systems that share this kernel

Linux Distribution *[b1.9,p115]* An OS that shares the linux kernel - Desktop: with GUI;Server: text based
Linux GUI *[b1.9,p120]* Dock;start menu;system tray;applications;file browser;web browser;etc
Linux Server *[b1.9,p116]* Linux specialized for servers
Linux Terminal *[b1.9,p124]* Powerful;execute commands written by user
List (Python) *[b2.1,p31]* List of things in order
Little-endian Format *[b3.11,p194]* LSB is stored first
Live Capture *[b3.7,p120]* Imaging a disk that is turned on
LLMNR Poisoning *[b3.16,p329]* use responder.py and take advantage of protocols used by active directory
Local Storage *[b1.16,p243]* Files on users computer (5MB)
Log Files (Windows) *[b2.12;3.6,p277;103]* Holds a log of events that occur on the computer
Log Server *[b1.26,p360]* Log events of a variety of severity levels on systems and across networks
long (C) *[b2.5,p161]* long integer value
lost+found folder (Linux) *[b1.10,p134]* For orphaned files
Low-level programming language *[b2.1,p10]* closer to machine code
ls (Linux) *[b1.10,p130]* list files command linux
LSB/Least Significant Bit *[b3.6,p100]* Algorithm used with steganographic techniques to embed text into images/audio
lusrmgr.msc *[b2.13,p285]* Local User management console

Mm

MAC Address *[b1.17,p253]* Media Access Control Address: address burned into a Network interface card
Magnet Axiom *[b3.7,p126]* Automated parsing tool
Magnet IEF *[b3.7,p126]* Automated parsing tool
Main ATX connector *[b1.2,p39]* For powering motherboard
Malloc *[b2.6,p182]* Used to put contents of variable on the heap
Man in the middle attack (MITM) *[b3.16,p326]* rely on attacker inserting themselves in the middle of communication between 2 systems
MariaDB *[b2.7,p189;193]* Open source version of MySQL
Master (Git) *[b2.1,p11]* Default branch of repository
MD5 *[b3.1;3.6,p22;105]* Older hashing algorithm;broken
MDNS Poisoning *[b3.16,p329]* use responder.py and take advantage of protocols used by active directory
Mebibyte (MiB) *[b1.3,p45]* 1024 kibibytes
Mechanical Drive *[b1.2,p29]* Moving parts;unreliable;slower than solid state
media folder (Linux) *[b1.10,p134]* For mounting usb keys and floppy disks
Megabyte (MB) *[b1.3,p44]* 1000 kilobytes
Memory *[b2.6,p179]* Made of the stack and the heap
Memory Capture *[b3.8,p132]* Copy of everything written to RAM since the last power cycle
Memory Forensics *[b3.8,p131]* analysis of volatile memory captures
Memory Register *[b2.16,p335]* Hold limited data for CPU
Merging and Pull Request (Git) *[b2.1,p12]* A pull request asks to merge changes from one branch to the master branch
Metadata *[b1.5,p81]* Data that describes data
Metagoofil (Linux) *[b3.5,p65]* Finds files from a given domain of a certain type using google
Metasploit *[b3.12,p215;227]* Used to generate shellcode and delivering exploits in a modular manner
Method (Windows cmdlet) *[b2.15,p330]* used to manipulate the object
MFT/Master File System *[b3.7,p119]* provide wealth of information on file system
MIME/Multipurpose Internet Mail Extension *[b1.27,p380]* Used for sending non-ascii data over email
mimikatz *[b3.8;3.16,p133;324]* tool used to glean cleartext passwords from memory
Mirroring (RAID 1) *[b2.18,p362]* duplicates data across both drives;storage capacity halved
Mkdir (Linux) *[b1.12,p166]* command to make directory (Linux)
mkdir (Windows) *[b2.14,p305]* command used to create directory
mnt folder (Linux) *[b1.10,p135]* For mounting usb keys and floppy disks
more (Windows) *[b2.14,p311]* used to display contents of a file 1 page at a time
Motherboard *[b1.2,p22]* Central piece to which all other components connect to
move (Windows) *[b2.14,p308]* command used to move files from one location to another
MS-DOS *[b2.14,p298]* Command line interpreter for Windows OS
msfvenom *[b3.12;3.14,p215;{286;291}]* tool used to generate malicious file
msi file *[b3.14,p289]* installer file
Mv (Linux) *[b1.12,p167]* command to move file/folder (Linux)
MX Record *[b1.20,p296]* Mail exchange;specifying mail server used for handling email for a domain
MySQL *[b2.7;2.8,p189;196]* Production DBMS to run at scale

Nn

NAND *[b1.4,p70]* AND followed by NOT;alternative denial connective
Nano (Linux) *[b1.13,p177]* command-line based text editor (Linux)
NBT-NS Poisoning *[b3.16,p329]* use responder.py and take advantage of protocols used by active directory
Negation connective *[b1.4,p69]* Logical NOT
Nested Loops (Python) *[b2.2,p70]* loop through collections of data within collections of data
net (Windows) *[b2.14,p315]* mount shared folders
Netcat (Linux) *[b2.3;3.16,p118;323]* Tool used to create connections
NetFlow *[b3.8,p135]* Term used to describe capturing meta-data from network traffic
netsh (Windows) *[b2.14,p314]* command used to start Network Shell to manage network settings
netstat *[b3.15,p302]* windows tool used to find listening ports on a system
Network *[b1.17,p247]* Set of computers connected to each other
Network Access Layer (TCP/IP) *[b1.21,p314]* Combination of data link and physical layers from OSI
Network Address Translation/NAT *[b1.18,p263]* Responsible for public vs private IP addresses
Network Attached Storage/NAS *[b2.18,p363]* Commonly uses file storage
Network Forensics *[b3.8,p135]* investigation of network traffic
Network Layer (OSI) *[b1.21,p307]* routing packet over internet
Networking (Linux GUI) *[b1.9,p122]* How to configure network in Linux w/ GUI
Networking (Windows CLI) *[b2.14,p314]* check network settings of local machine
Networking (Windows) *[b2.12,p268]* Handled using DHCP usually
Nginx *[b1.16,p234]* Generic web server
Nibble *[b1.3,p44]* 4 bits
NIC/Network Interface Card *[b1.17,p251]* Allows computer to interface with network
NMap (BLUE) *[b3.5,p91]* Patch software that listens on open ports
NMap (RED) *[b3.5;3.12,p86;212]* Tool to find open ports on a system

nologin *[b2.14,p198]* accounts that can't be logged into on a linux system
Non-Relational Database *[b2.7,p189;191]* used to store unstructured data
Non-repudiation (Encryption) *[b3.1,p9]* The sender cannot deny sending the message
Nop sled *[b3.11,p199]* If the EIP points within the NOP sled;the code will run
Nop \x90 *[b3.11,p197]* Instruction to do nothing and move on in assembly
NOR *[b1.4,p72]* OR followed by NOT;joint denial connective
NOT *[b1.4,p69]* Inverts input;negation connective
NotPetya *[b3.7,p127]* Ransomware targeting windows
NS Record *[b1.20,p296]* Name Server;points to name server authoritative for the domain
nslookup *[b1.27,p372]* used to look up MX records
NTFS *[b1.5;3.7,p84;119]* New Technology File System;for Windows
NULL byte *[b2.5,p158]* when a string ends;0x00
Number Base Notation *[b1.3,p47]* 0d = denary;0b = binary;0x = hexadecimal
Number Bases *[b1.3,p46]* Basis of counting
NX No Execute (Linux) *[b3.11,p202]* Separate stack into areas for code and data

Oo

Object (python) *[b2.2,p99]* An instance of a class
Object Storage (Cloud) *[b2.18,p363]* No hierarchy;data is stored in a flat structure as objects containing data and metadata
Object-oriented Programming *[b2.4,p137]* Use classes to model objects
OpenStego *[b3.6,p100]* Tool to attach secret message files in image files
Operating System *[b1.7,p94]* Software that runs the computer and manages how it operates
Operators (MySQL) *[b2.10,p231]* arithmetic;comparison and logical operators in SQL
opt folder (Linux) *[b1.10,p135]* Optional folder
OR *[b1.4,p68]* True if at least 1 of the inputs is true;false otherwise;disjunction connective
ORDER BY (SQL) *[b2.8,p201]* how to sort data requested
Order of precedence *[b2.2,p61]* AND comes before OR
Origin (Git) *[b2.1,p11]* Location of remote repository
OS Detection *[b3.5,p90]* Fingerprint the OS of target
OSI/Open Systems Interconnection Model *[b1.21,p301]* Describes how computers communicate over a network
Output Devices *[b1.2,p33]* Accept data from computer;ex: monitor;printer

Pp

PaaS *[b1.6,p90]* Platform as a Service;vendor provides hardware and software to enable you to deliver applications
Packet *[b1.17,p254]* Unit of data to be transmitted over the network
Packet Headers *[b1.21,p315]* encapsulate data for transmission
Parameter (Command Line) *[b1.11,p157]* 1 dash = single letter param;2 dashes = full word param
Parameter (Python function) *[b2.2,p80]* arguments passed into a function
Passwd file (Linux) *[b1.14,p198]* Holds info on users on a Linux system
Password reuse *[b3.5,p79]* when someone re-uses a password
Patching/Patch Cycles *[b2.12;3.12,p267;233]* Used to keep a system running securely
PATH (Linux) *[b1.10,p145]* Terminal looks down paths to find executable binaries
PCI-E *[b1.2,p40]* For powering graphics card
PDF *[b3.12,p240]* Lots of issues with pdf readers;and executable files can be embedded into pdfs
pdftk *[b3.5,p68]* tool used to remove metadata
Penetration Test *[b3.2,p31]* Try to get into a system;protect yourself
PEP8 Style Guide *[b2.4,p131]* Standard for how python code should be formatted
Permissions (Linux) *[b1.10,p136]* Who can do what to a file
Permissions (Windows) *[b2.13;3.14,p293;272]* Who is allowed to do what with files
Persistence *[b3.3;3.5;3.15,p48;63;301]* Maintain Access
Phishing *[b3.12,p237]* Form of social engineering performed over email
PHP *[b1.16,p241]* Server side programming language
PHPMyAdmin *[b1.24,p345]* Graphical frontend for databases
Physical Layer (OSI) *[b1.21,p309]* converting packets into electrical signals
Pipes (Linux) *[b1.14,p195]* Use |
Pointer *[b2.6,p179]* Memory address that points to the contents of a variable
POP3/Post Office Protocol 3 *[b1.19;1.27,p283;370]* Very old email protocol
Port *[b1.17,p257]* Communication channel for applications on a system to listen to
Port (HTTP;HTTPS) *[b1.16,p234]* Connection -> 80: Unencrypted HTTP;443: Encrypted HTTPS
Portscanner *[b2.3;3.16,p125;323]* find ports that are listening on a target system
Power Supply Unit *[b1.2,p37]* Take;convert;and deliver power to computer components
PowerShell (Windows) *[b2.15;3.14,p323;275]* includes scripting language and command line shell
PowerShell Commands (Windows) *[b2.15,p326]* use verb-noun naming system
PowerShell ISE (Windows) *[b2.15,p325]* Integrated Scripting Environment;used to write;test;and run PowerShell scripts
PowerShell Object (Windows) *[b2.15,p330]* cmdlets output objects containing information about result
Prefetch *[b3.7,p124]* Stores specific data about applications you run
Preparation (Incident Response) *[b3.6,p107]* Prepare business to tacker incidents
Presentation Layer (OSI) *[b1.21,p304]* ex: XML;JSON
Pretexting *[b3.12,p236]* Call/email someone pretending to be someone else
Primary Key *[b2.7,p190]* Value in a row unique to that row;used in relational databases
Print (C) *[b2.5,p156;158]* print string to output
Privilege escalation *[b3.3;3.13,p48;253]* Gain access to higher permissions
proc folder (Linux) *[b1.10,p135]* Process folder
Procedural Programming *[b2.4,p137]* Break tasks into steps to solve problems
Process *[b1.7,p97]* Series of actions or steps taken to achieve a goal
Process (Linux) *[b1.14,p191]* a running program
Processor/CPU *[b1.2;2.16,p24;334]* Central Processing Unit;executes instructions in programs
Program *[b2.1,p9]* series of instructions for the processor of a computer
Programming Language *[b2.1,p9;10]* what computer programs are written in
Programming Paradigm *[b2.4,p137]* A pattern or model for programming
Prompt (Linux) *[b1.9,p124]* What shows when you open a linux terminal;~ = home folder of user;# = higher permissions
Property (Windows cmdlet) *[b2.15,p330]* contain information about object
Proposition *[b1.4,p64]* A statement that is true or false
Protocol *[b1.17,p255]* Set of rules of how 2 computers will talk to each other
ps (Linux) *[b3.13,p256]* command to list all running processes

PS/2 *[b1.2,p32]* Earlier version of USB
PSExec *[b3.16,p330]* Powershell module designed for network admins
PST/Personal Storage Table Files *[b3.7,p122]* Personal folder files in Microsoft Outlook
Pseudocode *[b2.4,p140]* Way to think through code without writing code
PTR Record *[b1.20,p296]* Pointer Record for reverse lookups
Public key infrastructure *[b1.28,p385]* How public keys are shared to the world
Purple Team *[b3.6,p114]* collaboration between red and blue teams
pwd (Linux) *[b1.10,p133]* Print working directory command
pwndbg *[b2.17,p344]* GDB extension to add functionality
Python *[b2.1,p10;14]* High-level programming language
Python Documentation *[b2.4,p129]* find information on different things in python

Qq

qpdf *[b3.5,p68]* tool used to remove metadata

Rr

RAID 0 (Striping) *[b2.18,p362]* for performance and read/write speed;lack of fault tolerance
RAID 1 (Mirroring) *[b2.18,p362]* duplicates data across both drives;storage capacity halved
RAID 10 *[b2.18,p362]* combination of RAID 0 and RAID 1;read/write speed optimized
RAID 5 (Striping with parity) *[b2.18,p362]* need at least 3 drives;optimized for read;slower write
RAID 6 (Striping with double parity) *[b2.18,p362]* need at least 4 drives;optimized for read;slower write
RAID/Redundant Array of Independent Disks *[b2.18,p362]* Several drives groups together
RAM *[b1.2;2.16,p26;338]* Random Access Memory/memory - how much you have have open at once;Volatile
Reading from files (C) *[b2.6,p178]* Read data from files in C
Reading from files (python) *[b2.3,p112]* read data from files
Reconnaissance (BLUE) *[b3.5,p68]* Scrub documents of metadata;find what others can find about your company
Reconnaissance (RED) *[b3.3,p48]* Pick target;find as much info as possible about them
Recovery (Incident Response) *[b3.6,p108]* Return system to full working capacity
Recursive Lookup (DNS) *[b1.20,p295]* Asking DNS servers until answer is found (Not used anymore)
Recursive resolver *[b1.25,p350]* responsible for receiving queries from client machines via applications
Red Team *[b3.3;3.6,p{40;41};112]* Acts as attackers
Redirect (Linux) *[b1.14,p196]* Take output of command and redirect to file
regedit *[b2.12,p275]* used to edit Windows Registry
Register (CPU) *[b2.16,p334]* Memory registers are faster than RAM;hold limited data
Registry (Windows) *[b2.12;3.7;3.14;3.15,p275;123;289;307]* database of settings for the operating system
Registry Permissions (Windows) *[b3.14,p289]* may be able to change paths to point to custom executable files
Relational Database *[b2.7,p189;190]* organized store of data
Remote Desktop Users (Windows Default Group) *[b2.13,p287]* If you want to connect to the computer remotely
Repository (Git) *[b2.1,p11]* Place where a project lives
Response Headers (HTTP) *[b1.23,p337]* Carry status of a request
Responsible Disclosure *[b3.11,p183]* Process to follow when a security researcher finds a flaw in software
return value (Python) *[b2.2,p85]* what a function returns
Reverse command search (Linux) *[b1.11,p154]* Search through command history linux
Reverse Lookup (DNS) *[b1.20,p294]* Translate IP into domain name
RIGHT JOIN (SQL) *[b2.9,p226]* return all results from the 2nd table and only matching results from the 1st table
Risk Management (Server) *[b3.3,p45]* Likelihood of attack multiplied by potential impact of attack
Rm (Linux) *[b1.12,p168]* command to remove
rmdir (Windows) *[b2.14,p310]* used to remove a directory
robocopy (Windows) *[b2.14,p307]* used to copy files;directories and drives to other locations
Robots.txt (BLUE) *[b3.5,p71]* don't use robots.txt;use the robots meta tag in the HTML header
Robots.txt (RED) *[b3.5,p70]* opt certain pages out of being indexed
root (Linux) *[b1.10,p127]* Name of admin account on linux system (can break OS if it wants to)
root folder (Linux) *[b1.10,p135]* root user folder
Root name server *[b1.25,p250]* first port of call for the resolver to query
Rootkit *[b3.15,p312;314]* form of malware designed to allow an attacker back into a system at a later date
Router *[b1.17,p250]* Device that connects 2 networks together
Rpm (Linux) *[b1.14,p207]* Software packaged for a linux distribution -> for fedora
rSteg *[b3.6,p100]* Java based tool to hide text inside images
Rsync (Linux) *[b3.13,p262]* Syncs contents of 2 folders
run folder (Linux) *[b1.10,p135]* Temp file storing runtime info when booting up
runlevels (Linux) *[b3.15,p305]* specifies mode in which the OS system is running under

Ss

SaaS *[b1.6,p89]* Software as a Service;software via a 3rd party
SATA (Serial ATA) *[b1.2,p38]* For powering hard drives
sbin folder (Linux) *[b1.10,p135]* Holds binary executables for admin purpose
Scripting Table (SQL) *[b2.11,p254]* automate creation of tables and databases in SQL
Search Engine *[b1.15,p218]* Use crawlers to index pages
Security Control - Access Monitoring and Control *[b3.3,p47]* Actively manage the life-cycle of system and application accounts - their creation;use;dormancy;deletion
Security Control - Application Software Security *[b3.3,p47]* Manage the security life-cycle of all in-house developed and acquired software
Security Control - Boundary Defense *[b3.3,p47]* Detect;prevent;correct the flow of information transferring across networks of different trust levels
Security Control - continuous vulnerability assessment and remediation *[b3.3,p46]* acquire;assess;take action on new info to identify vulnerabilities and fix them
Security Control - Controlled Access Based on the Need To Know *[b3.3,p47]* Track;control;prevent;correct and secure access to critical assets according to the formal determination of which persons;computers and applications have a need and a right to access these critical assets
Security Control - controlled use of admin privileges *[b3.3,p46]* track;control;prevent;correct use of admin privileges on computers;networks;and applications

Security Control - Data Protection *[b3.3,p47]* Prevent data exfiltration;mitigate the effects of exfiltrated data and ensure the privacy and integrity of sensitive information
Security Control - Data Recovery Capability: back up critical info to be able to recover quickly** *[b3.3,p46]*
Security Control - email and web browser protections *[b3.3,p46]* minimize attack opportunities for attackers to trick users
Security Control - Incident Response and Management *[b3.3,p47]* Developing and implementing an incident response infrastructure.
Security Control - Inventory of authorized and unauthorized devices *[b3.3,p46]* Manage;inventory;track;correct all hardware devices on network
Security Control - Inventory of authorized and unauthorized software *[b3.3,p46]* Manage;inventory;track;correct all software devices on network
Security Control - Limitation and Control of Network Ports;Protocols and Services *[b3.3,p46]* manage;track;control;correct use of ports;protocols and services on networked devices
Security Control - Maintenance;monitoring and analysis of log files *[b3.3,p46]* collect;manage;analyze audit logs to detect;understand and recover from breaches
Security Control - malware defenses *[b3.3,p46]* control installation;spread;execution of malicious code
Security Control - Penetration Tests and Red Team Exercises *[b3.3,p47]* Test the overall strength of an organization's defenses by simulating the objectives and actions of an attacker
Security Control - Secure configurations for hardware and software *[b3.3,p46]* Manage;track;report on;correct security configurations for all devices on network
Security Control - Secure Configurations for Network Devices such as Firewalls;Routers and Switches *[b3.3,p46]* Establish;implement and actively manage the security configuration of network infrastructure devices
Security Control - Security Skills Assessment and Appropriate Training to Fill Gaps *[b3.3,p47]* Identify the specific knowledge;skills and abilities needed to support defense of the enterprise
Security Control - Wireless Access Control *[b3.3,p47]* Track;control;prevent;and correct the security use of wireless local area networks;access points and wireless client systems
Security Controls *[b3.3,p46]* Implemented to increase security of system
Segmentation Fault *[b3.11,p189]* Occurs due to buffer overflow
SELECT (SQL) *[b2.8,p198]* retrieve data from table
self (classes and objects) *[b2.2,p100]* Refer to attributes inside a class
SEM/Security Event Management *[b1.26,p362]* Real time analysis of SIM data
Server *[b1.22,p321]* Receive connections from client devices
Server Hardware *[b1.22,p322]* computer than runs software that provides services
Server Software *[b1.22,p324]* Software that sits and listens for connections and processes requests
Server-side *[b1.23,p333]* Where the computations happen to deliver a web page
Service Detection *[b3.5,p89]* Find services running on open ports
Session Guessing (BLUE) *[b3.10,p163]* Use truly random session tokens
Session Guessing (RED) *[b3.10,p162]* Guessing a session token
Session Layer (OSI) *[b1.21,p305]* opening;closing;managing connections between computers
Session Token *[b3.10,p162]* A token that identifies you after login
SGID/Set Group ID *[b3.13,p255;264]* When the file is run;it is run with the same privileges as the group owner of the file
SHA1 *[b3.1,p22]* Successor to MD5;broken
SHA2 *[b3.1,p22]* Secure hashing algorithm
SHA256 *[b3.1;3.6,p22;105]* Secure hashing algorithm
SHA3 *[b3.1,p22]* Secure hashing algorithm
SHA512 *[b3.1,p22]* Secure hashing algorithm
Shadow file (Linux) *[b1.14,p198]* Holds passwords of users on a Linux system
Shell (Linux) *[b1.9,p124]* The program that runs when the terminal is opened
Shellcode *[b3.11,p196]* hex representation of assembly
short (C) *[b2.5,p161]* short integer value
Shortcut (Windows) *[b3.15,p310]* shortcuts can be hijacked to run code as the user is interacting with system
SIEM/Security Information and Event Management *[b1.26,p363]* Combining SIM and SEM
SIFT *[b3.4,p54]* Forensic focused distribution
Signed Integer *[b2.5;3.11,p161;186]* int that can be positive or negative
SIM/Security Information Management *[b1.26,p362]* Tools used to collect and store security data
Single responsibility principle *[b2.2,p83]* a function should only do one thing
Slack Space *[b1.5,p81]* Wasted space when file size is smaller than cluster size
Slingshot *[b3.4,p53]* Distribution by SANS Institute
SMB/Server Message Block *[b3.8,p135]* File transfer protocol
SME Network *[b1.21,p319]* small-medium enterprise
SMTP Response Code *[b1.27,p377]* 3 digits responses when using SMTP
SMTP/Simple Mail Transfer Protocol *[b1.19;1.27,p281;370]* Connection oriented;text based protocol for sending emails
Social Engineering *[b3.12,p235]* Tricking someone into doing something that is not in their best interest
Socket (Python) *[b2.3,p115]* allow you to make and receive network connections
Sockets (Motherboard) *[b1.2,p23]* Classified via socket type;must match socket type of CPU
Solid State Drive (SSD) *[b1.2;3.7,p29;121]* No moving parts;reliable;faster;more expensive than mechanical drives
Spam Filter *[b1.27,p374]* Rules to prevent malicious emails from reaching user inbox
Spear Phishing *[b3.12,p237;249]* Targeted phishing;usually more convincing
SPF/Sender Policy Framework *[b1.19,p285]* List of IP addresses of mail servers allowed to send mail from a domain
SQL Injection (BLUE) *[b3.9,p158]* Don't pass insecure queries to databases
SQL Injection (RED) *[b3.9,p157]* Injecting SQL code into a query
SQL Injection - BLIND *[b3.9,p157]* When the flaw in SQL doesn't print data
SQL server *[b1.24,p346]* Most widespread form of a database server
SQL Statement *[b2.8,p196]* syntax of SQL
SQL/Structured Query Language *[b2.7;3.9,p189;157]* Used to manage relational databases
SQLite *[b2.7,p189]* lightweight DBMS
srv folder (Linux) *[b1.10,p135]* Holds data used by services
SSH (Kali Linux) *[b3.4,p58]* disabled by default
SSH (Linux) *[b1.14,p214]* Secure SHell - log into a linux computer over the internet
SSL Certificate *[b3.1,p21]* A certificate signed by a certificate authority that acts as a public key for a site
Stack *[b2.6;2.16,p179;339]* Structured section of memory
Stack Canary *[b3.11,p202]* Value that sits before the return pointer
Stack Frame *[b2.6;2.16,p179;339]* Section of memory assigned to a function
Stack Protector *[b3.11,p202]* If Stack Canary is overwritten;its sketchy

Standard Account (Windows) *[b2.13,p281]* Can't impact other users;but can do most other things
Star (Topology) *[b1.17,p248]* All computers are connected to a central point
Start-Process (Windows) *[b2.15,p328]* starting running a new process
Start-up folder (Windows) *[b3.15,p307]* put malware in the user's startup items folder
Start-up items *[b3.15,p305]* have malware execute upon startup
STARTTLS *[b1.19,p280]* Used to encrypt emails
Steganalysis *[b3.6,p99]* Method of detecting concealed files
Steganography *[b3.6,p99]* Concealing data within other data
Steghide *[b3.6,p100]* Tool to hide secret files inside image/audio files
Stop-Process (Windows) *[b2.15,p328]* ends a running process
Storage *[b1.2,p28]* Provides data storage
Storage Area Network (SAN) *[b2.18,p363]* Storage network
String (Python) *[b2.1,p17]* string of characters
String Manipulation (Python) *[b2.1,p20]* Working with strings
Strings (Linux) *[b1.13,p183]* command to see strings in binary files (Linux)
Striping (RAID 0) *[b2.18,p362]* for performance and read/write speed;lack of fault tolerance
Striping with double parity (RAID 6) *[b2.18,p362]* need at least 4 drives;optimized for read;slower write
Striping with parity (RAID 5) *[b2.18,p362]* need at least 3 drives;optimized for read;slower write
su (Linux) *[b1.10,p128]* Switch user command linux
subinacl.exe *[b3.14,p289]* tool used to look at registry permissions from command line
Subnet *[b1.18,p265]* sub-network;way of splitting a network into segments
Subquery (SQL) *[b2.10,p232]* query within a query
sudo (Linux) *[b1.10;3.13,p128;267]* Temporarily take privileges of root
sudoers file (Linux) *[b1.10;3.13,p128;267]* List of accounts allowed to use superuser privileges
SUID/Set User ID *[b3.13,p255;264]* When the file is run;it is run with the same privileges as the user owner of the file
Superuser (Linux) *[b1.10,p127]* Admin account on Linux system
Switch *[b1.17,p249]* Connects computers on a network together (smart)
symlinks (Linux) *[b3.15,p306]* shortcuts to programs
Symmetric Encryption *[b3.1,p13]* 1 key used to encrypt and decrypt
Syn Scan *[b3.5,p88]* Starts the TCP connection but does not finish handshake
Synchronization servers *[b1.28,p384]* Sync data between multiple locations
sys folder (Linux) *[b1.10,p135]* Holds info on system
SYSTEM (Windows User) *[b3.14,p272]* Can do anything on windows system
systemd (Linux) *[b3.15,p306]* way to have programs start at startup

Tt

Tab completion (Linux) *[b1.11,p150]* Makes using the linux terminal easier
Tautology *[b1.4,p78]* Statement that is always true;no matter inputs
TCP Client (Python) *[b2.3,p115]* create TCP connection
TCP Handshake *[b1.18,p269]* Initial connection for TCP protocol
TCP Protocol *[b1.17,p256]* Reliable delivery of information between 2 computers;272 -> more detail
TCP Server (Python) *[b2.3,p116]* receive connections using TCP
TCP Teardown *[b1.18,p270]* Closing TCP connection
TCP/IP Model *[b1.21,p310]* Theoretical model to show how computers communicate
tcpdump *[b3.8,p137]* Used to sniff packages across a network
Tebibyte (TiB) *[b1.3,p45]* 1024 gibibytes
Terabyte (TB) *[b1.3,p44]* 1000 gigabytes
Thermal Paste *[b1.2,p36]* Used to connect heat sink to components
Threads *[b2.3,p121;122]* allows programs to run multiple things at the same time
TLD/Top Level Domain *[b1.19;1.25,p291;350]* Bit at the end of a domain name
tmp folder (Linux) *[b1.10,p135]* Temp file system
Top (Linux) *[b1.11,p160]* Command to see info on system
Topology *[b1.17,p248]* How a computer network is laid out
Touch (Linux) *[b1.10,p142]* Linux command to create a file
Transport Layer (OSI) *[b1.21,p306]* end to end connections;ex: TCP;UDP
Transport Layer (TCP/IP) *[b1.21,p312]* Same as for OSI;TCP;UDP
Truth table *[b1.4,p64]* Used to show outputs of logic gates based on inputs
TSK/The Sleuth Kit *[b3.7,p125]* CLI-digital forensics tool
Tuple (Python) *[b2.1,p37]* Immutable;store 2 items
TXT Record *[b1.20,p296]* Stores textual data associated with domain name (For SPF;DKIM;etc)
Type conversion (Python) *[b2.1,p28]* converting data from 1 type to another

Uu

UAC Levels *[b2.13,p292]* How permissive UAC should be
UAC Prompt *[b2.13,p290]* Ask if an application can perform a task that requires a higher privilege level
UDP Client (Python) *[b2.3,p119]* create UDP connection
UDP Protocol *[b1.17;1.18,p258;272]* Fast transmission of data between 2 computers
UDP Server (Python) *[b2.3,p120]* receive connections using UDP
UEFI *[b1.7,p102]* Unified Extensible Firmware Interface;Successor to BIOS
UNION (SQL) *[b2.10,p239]* combine results from 2 SELECT statements
Unit Test *[b2.4,p134]* used to ensure a function is working as expected
Unquoted Service Paths *[b3.14,p284]* paths are executed by SYSTEM
Unsigned Integer *[b2.5;3.11,p161;186]* int that can only be positive
URL *[b1.23,p333]* Gives path to a web pages from domain
USB *[b1.2,p31]* Universal Serial Bus - transfer data
USB-C *[b1.2,p35]* Powerful connector;can transfer power and data
User Account Control (Windows) *[b2.13;3.14,p289;272]* Used to make the Windows OS more secure
User Account Control Bypass *[b3.14,p274]* ask user for permission
User Accounts (Windows CLI) *[b2.14,p317]* manage users from command line
User Accounts (Windows) *[b2.13,p281]* used to sign into computer
User input (C) *[b2.6,p175]* taking input from user;vulnerable
User input (command line) *[b2.2,p93]* taking input from user from command line
User input (Python) *[b2.2,p87]* taking input from user
usermode *[b3.15,p312]* type of rootkit
Users (Windows Default Group) *[b2.13,p287]* Where standard users are placed
usr folder (Linux) *[b1.10,p135]* User controlled files

Vv

Var folder (Linux) *[b1.10,p135]* Holds files that increase in size over time
Variable (C) *[b2.5,p157;161]* storing data in C
Variable (PowerShell) *[b2.15,p331]* used $ to declare a variable
Variable (Python) *[b2.1,p16]* a way of storing data in programs
Version control system *[b2.1,p11]* Track changes to a programming project
VGA *[b1.2,p33]* A/V (Audio/visual) output
Vim (Linux) *[b1.13,p179]* command-line based text editor (Linux)
Virtualization *[b1.8;2.19,p105;367]* Creating a virtual computer that behaves as a separate computer
Volatility *[b3.7;3.8,p125;133]* Tool for memory forensics
Vulnerability Scanner (BLUE) *[b3.10,p180]* These scanners are noisy!
Vulnerability Scanner (RED) *[b3.10,p179]* Crawling all pages of a site;and performing multiple attacks on each page

Ww

WAN *[b1.17,p247]* Wide Area Network
WannaCry *[b3.11,p183]* Malware that brought NHS down for several days
Wear leveling *[b3.7,p121]* Constantly moving files to prevent parts of the disk from wearing out
Web Application Firewall *[b3.10,p180]* intercepts suspicious traffic
Web Servers *[b1.16;1.23,p234;{329;340}]* Software applications that accept and process requests according to HTTP protocol
Wget (Linux) *[b1.13,p185]* web get - download files from internet (Linux)
WHERE (SQL) *[b2.8,p203]* set a condition for data to be retrieved
where (Windows) *[b2.14,p313]* similar to which command from Linux;used to locate files
Which (Linux) *[b1.10,p146]* Linux command to find where a program is installed on system
While loop (C) *[b2.6,p172]* nearly the same as for python
While loop (Python) *[b2.2,p74]* run until a condition is no longer met
WHOIS (BLUE) *[b3.5,p81]* Use the WHOIS privacy services
WHOIS (RED) *[b3.5,p80]* WHOIS system tracks who is responsible for a domain name
Wildcard *[bx,px]* * = matches everything -> used in many places
Wildcard Injection *[b3.13,p261]* takes advantage of how the linux terminal supplies parameters
Windows *[b2.12,p261]* OS developed by Microsoft
Windows Command Processor *[b2.14,p298]* Command line interpreter for Windows OS
Windows Defender *[b2.12,p273]* Built in antivirus on Windows
Windows Desktop *[b2.12,p262]* 90% of desktop computers run a version of Windows
Windows Firewall *[b2.12,p274]* Built in software firewall
Windows IoT *[b2.12,p264]* Windows designed to run on lower power computers
Windows on Mobile Devices *[b2.12,p265]* Windows on a mobile device
Windows Server *[b2.12,p263]* Version of windows designed to run on servers
Wireshark *[b1.18;3.8,p277;136]* Tool to monitor network connections
wll *[b3.15,p316]* format to hold executable code;just dll
Word Macros *[b3.12;3.15,p238;315]* Microsoft Word documents can hold code to be executed when the document is opened
Word Template *[b3.15,p315]* each blank document is loaded from template->the template can be compromised
Wordlist *[b3.4;3.5,p56;76]* used for dictionary attacks
Writing data to files (python) *[b2.3,p113]* write data to files

Xx

X-Frame-Options Header *[b3.10,p168]* Used to mitigate clickjacking
XBox *[b2.12,p266]* Runs a version of windows
XOR *[b1.4,p74]* Exclusive OR;true if inputs are different;false otherwise;exclusive disjunction connective
XOR Encryption *[b1.4,p76]* plaintext XOR key = cipher;cipher XOR key = plaintext;cipher XOR plaintext = key
XSS/Cross Site Scripting (BLUE) *[b3.9,p156]* Sanitize user input
XSS/Cross Site Scripting (RED) *[b3.9,p154]* run javascript code in the browser of clients

Yy

Yara *[b3.15,p317]* signature detection tool for detecting indicators of compromise
Yum (Linux) *[b1.14,p206]* Alternative package manager

Zz

Zend Escaper File *[b3.9,p156]* Filter for XSS
Zone Transfer *[b3.5,p82]* pulling a complete list of every DNS record for a domain
Zsh (Linux) *[b1.14,p215]* Alternative to bash

Tools:

nmap:*[b3.5;3.12,{p86;91};212]*
- -p- = scan all ports
- -vv = second level of verbosity
- -sT = Connect scan
- -sS = Syn scan
- -sV = Version detection
- -O = Fingerprint OS

metagoofil:*[b3.5,p65]*
- -d = set domain
- -t = set file type
- -l = set how far back in the Google search results to look
- -o = set folder to save the downloaded files into
- -f = set name of the output file where the results are saved

msfvenom: *[b3.12;3.14,p215;{286;291}]*
- -a = architecture of target
- -p = set payload
- --platform = platform target is running
- -b = set bad characters

netcat/nc: *[b2.3;3.16,p118;323]*
- -l = listen
- -u = set UDP connection
- -pultn = look for listening ports