The Knowledge

The Knowledge by Paul Richards 2022
Like the knowledge taken by London taxi drivers there is a base of knowledge that all cyber security consultants must be aware of. The following is the bare minimum required to be a cyber security practitioner. AKA 30 pages of ~~hell~~ fun bedtime reading.

Risk Management

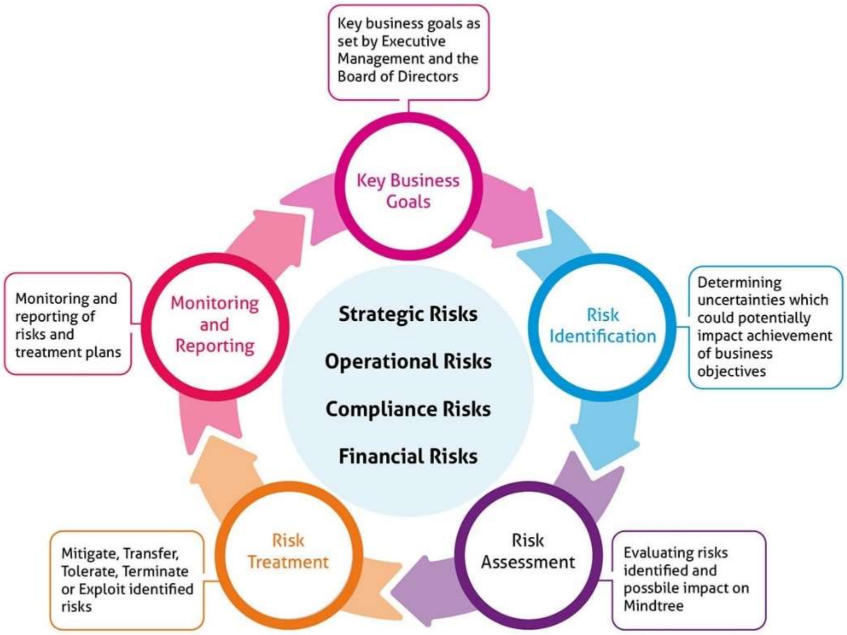
The effect a penetration test is likely to have on a system being tested is there will probably be many log entries and some accounts may be locked out by password guessing.

If a server is to be excluded from testing during certain hours, it is likely to be defined in the rules of engagement / scope

A company which has previously suffered a major fire in a key data centre would most likely have a business Continuity Plan

If the applied set of security controls does not eliminate all risk in a system, if the residual risk is low enough, it can be accepted.

In aiming to reduce the level of risk while conducting a penetration test you should establish an emergency point of contact in the event of an emergency.


Key business goals as set by Executive Management and the Board of Directors
Key Business Goals
Risk Identification
Determining uncertainties which could potentially impact achievement of business objectives
Risk Assessment
Evaluating risks identified and possbile impact on Mindtree
Risk Treatment
Mitigate, Transfer, Tolerate, Terminate or Exploit identified risks
Monitoring and Reporting
Monitoring and reporting of risks and treatment plans
Strategic Risks
Operational Risks
Compliance Risks
Financial Risks

Prior to starting a test on a safety critical or high-risk system you MUST: Have an understanding of any scope restrictions; Have a comprehensive understanding of the requirements for testing safety critical or other designated high-risk systems; Have permission to test

With regards to **risk** - during a penetration test the client's systems should not suffer any amount of disruption and the client should report any anomalous behaviour immediately

The four potential **risk** treatments are: Avoid, Reduce, Accept and Transfer

A **risk** that is implicitly associated with an activity or location is known as an inherent risk.

The primary objective of **risk management** to reduce the risk to an acceptable level.

Mitigating the **risk** is considered an acceptable option when managing a risk in some cases.

False negatives are considered by most as a serious risk associated with vulnerability assessment tools, as this indicates missed findings.

Threat identification, vulnerability identification and control analysis are considered valid data-gathering activities associated with a **risk assessment.**

Malware can be described as a threat with regards to **risk management**.

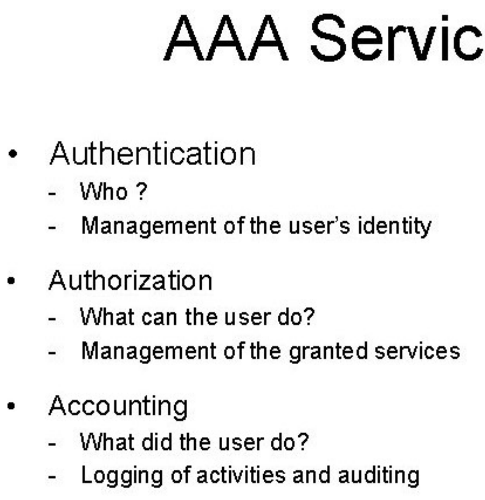
AAA (Authentication, Authorisation and Access Control)

A fingerprint is an example of Identification and Authentication

A username is an example of Identification

Something you think is not considered to be an **authentication factor,** for this we are looking for something you have (like a token), something you know (like a password) and something you are (so consider biometrics, fingerprints, etc)

Authentication is a way of proving who a user is, i.e. USER123, authentication is **not** a security exploit



AAA Services

- Authentication
  - Who ?
  - Management of the user's identity
- Authorization
  - What can the user do?
  - Management of the granted services
- Accounting
  - What did the user do?
  - Logging of activities and auditing

Penetration Testing and Tools

Pass the Hash can be useful during penetration testing because it allows the use of password hashes without having to crack them.

Mounting a **firewall's NFS** share and attempting to exploit uid resolution weaknesses is not a valid test for firewall testing.

The "**nbtstat**" tool will list all the members of the **Master Browser List** (using net the bios protocol)

Showmount is an NFS enumeration tool and cannot enumerate the SMB protocol.

NASL is the - Nessus Assessment Scripting Language

600 is the correct file permission for the authorized_keys file on an SSH service.

The **Arpspoof** tool on a UNIX platform enables an ARP packet to be redirected from a target host

The **amap** (yes amap not nmap) tool is best described as an application protocol mapping tool and banner grabber

A penetration test with no prior knowledge of the internal IT systems is known as a **black box test.**

The difference between a network vulnerability assessment and a penetration test is a **penetration test** exploits vulnerabilities, and a **vulnerability assessment** finds vulnerabilities.

If during an authorised penetration test you discover evidence of an intrusion on the target, halting all test activities and contacting the customer would be the most appropriate course of action for the team

A **False positive** is the name given to a finding which is incorrect as a result of automated testing.

Scoping, Testing, Report Writing, Debrief are the normal sequence of events in a penetration test.

Administrators monitoring the test and closing vulnerabilities as they are detected is a factor outside the **penetration testers** control that can repeatability pose a problem when conducting a test.

A **wash up meeting** is not required before a **penetration test**, in fact it's a meeting to discuss findings and is used post testing.

A **forensic investigation** is a process would you NOT expect to be included in a penetration test.

Contact the companies ISO or equivalent and advise them of a probable incident is while conducting a **penetration test** you notice the security logs are shrinking.

Most ARP poisoning tools work by creating a fake **ARP** reply that is a broadcast.

The terminology used to describe gaining access to an internal system from a compromised host is **Pivoting.**

The -e **netstat** flag lists all active connections.

When analyzing some **IDS logs**, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. This is known as a **False positive**.

The p0f tool used for **operating system** fingerprinting.

Nessus is a vulnerability scanner which can help with cracking passwords, and can check for default credentials but it is **not** a password cracker

nc (netcat / ncat) is commonly used to create a backdoor and will be identified as malware by most malware scanners.

To secure an **encrypted back channel** you could use cryptcat (Other options exist with ncat and flags to use tls/ssl etc)

Network sniffers all generally work by put the NIC into **promiscuous** mode.

The **Loki tool** uses the **ICMP protocol** to work by default.

The **traceroute** command is typically used to identify the route to a host on a network.

The **arpwatch** tool allows Ethernet /IP pairings to be monitored.

The **Cain tool** is capable of **ARP poisoning** attacks.

The term **reconnaissance** describes passive information gathering.

Center for internet **security (CIS) –** produce benchmarks (L1 and L2)

Policies and standards

An information Security policy should cover all of the information in an organisation

An **ISMS** is an Information Security Management System

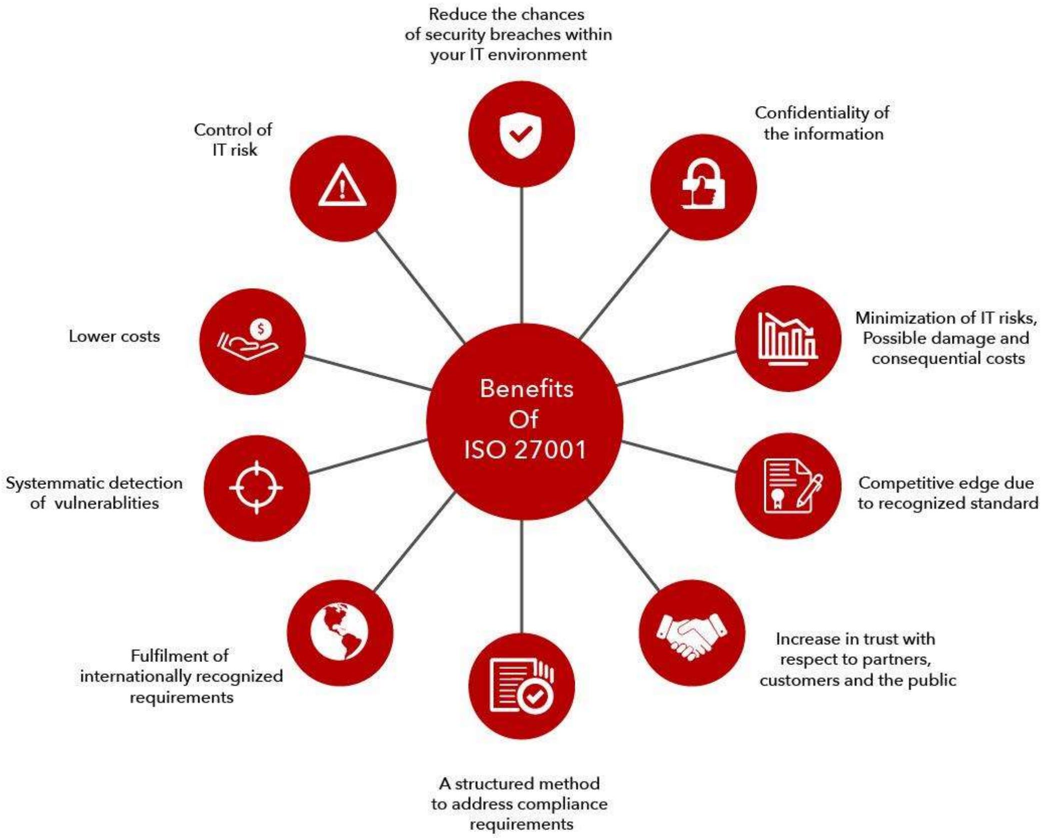
ISO 27001 is an **information security standard** and furthermore is a framework that sets out the specification for an information security management system.

An internal interdepartmental team would be the most likely group to be suitable to act as a **Computer Emergency Response Team (CERT)**.

ITIL is not a recognised security standard, it's more a set of ICT standards and management tools and processes which can and do contain security information.

PCI DSS standards pertain specifically to handling of card data and requires penetration testing at least once per year.

Password complexity is an account policy which requires a user to enter a 15 character password which contains both alphabetical and numerical characters.


Benefits Of ISO 27001
Reduce the chances of security breaches within your IT environment
Confidentiality of the information
Minimization of IT risks, Possible damage and consequential costs
Competitive edge due to recognized standard
Increase in trust with respect to partners, customers and the public
A structured method to address compliance requirements
Fulfilment of internationally recognized requirements
Systemmatic detection of vulnerablities
Lower costs
Control of IT risk

Laws

The **Computer Misuse Act, the Human Rights Act** and the **Data Protection Act** are the three main pieces of legislation that are relevant to penetration testing in the UK.

GDPR

According to GDPR laws data breaches must be reported if they pose a risk to the rights and freedoms of natural living persons.

According to GDPR laws who do organisation need to report data breaches too the supervisory authority

The EU General Data Protection Regulation affects how all companies store European citizens' data

Section 32 of the EU General Data Protection Regulation makes requirements for controllers and processors to ensure the security of the data processing process via testing. This may include penetration testing.

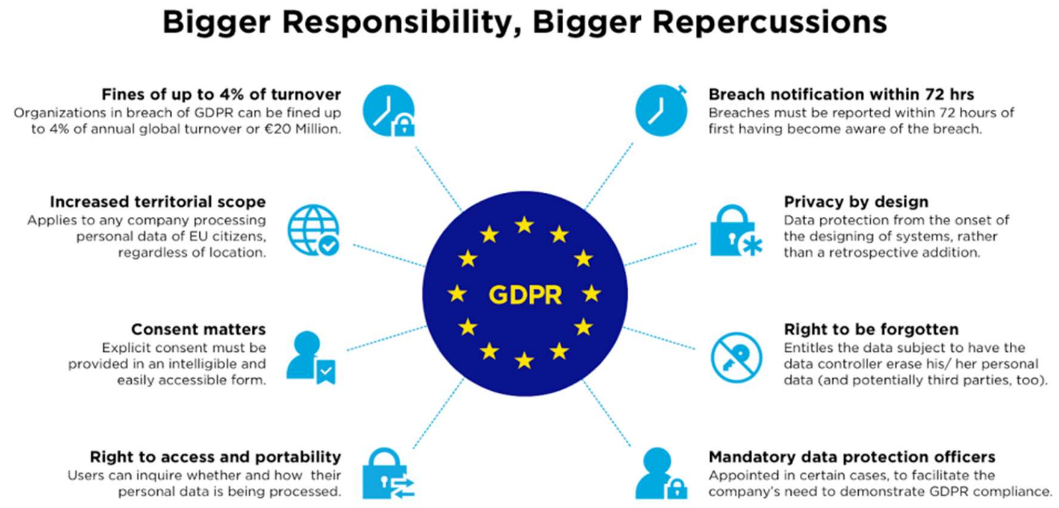
The GDPR requires organisations to report breaches within 72 Hours

“A clear action where the data subject freely and specifically expresses their consent” is considered as legal consent in the **GDPR**

20 million Euros and up to 4% of the annual worldwide turnover, is the maximum fine for **GDPR** noncompliance.

GDPR standards pertain specifically to handling of personal data

Right to erasure, right to object, right to rectification are not given rights to citizens under the EU **General Data Protection Regulation (GDPR)**.


Bigger Responsibility, Bigger Repercussions
GDPR
Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.
Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.
Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.
Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.
Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.
Right to be forgotten
Entitles the data subject to have the data controller erase his/ her personal data (and potentially third parties, too).
Right to access and portability
Users can inquire whether and how their personal data is being processed.
Mandatory data protection officers
Appointed in certain cases, to facilitate the company's need to demonstrate GDPR compliance.

CMA

During a penetration test the Computer Misuse Act (1990) should be the law of most concern to a tester.

Examining discarded or stolen media without intent to commit further offences falls under Section 1 of the computer misuse act.

Section 1 of the Computer Misuse Act 1990 concerns the unauthorised access to computer material

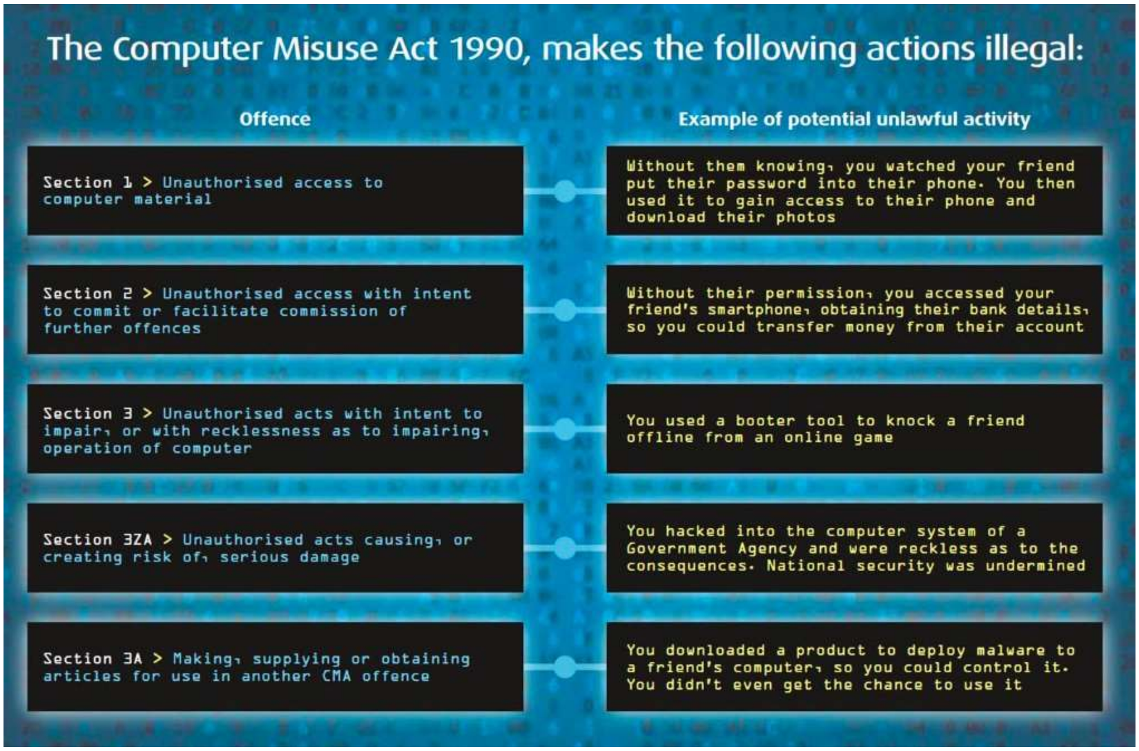
The Computer Misuse Act sections relevant to a penetration tester is primarily sections 1 to 3

Under Section 1 of the Computer Misuse Act 1990, a person is guilty if they cause a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; the access he intends to secure, or to enable to be secured, is unauthorised; and he knows at the time when he causes the computer to perform the function that that is the case.

The primary legal reason for obtaining written permission before starting a test is because otherwise the penetration test might breach the **Computer Misuse Act.**

The **Police and Justice Act 2006** is the act which amended the **Computer Misuse Act 1990**.

The three **computer misuse offences** defined by the UK Computer Misuse Act 1990 are: Unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences and unauthorised modification of computer material.



The Computer Misuse Act 1990, makes the following actions illegal:

Offence	Example of potential unlawful activity
Section 1 > Unauthorised access to computer material	Without them knowing, you watched your friend put their password into their phone. You then used it to gain access to their phone and download their photos
Section 2 > Unauthorised access with intent to commit or facilitate commission of further offences	Without their permission, you accessed your friend's smartphone, obtaining their bank details, so you could transfer money from their account
Section 3 > Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer	You used a booter tool to knock a friend offline from an online game
Section 3ZA > Unauthorised acts causing, or creating risk of, serious damage	You hacked into the computer system of a Government Agency and were reckless as to the consequences. National security was undermined
Section 3A > Making, supplying or obtaining articles for use in another CMA offence	You downloaded a product to deploy malware to a friend's computer, so you could control it. You didn't even get the chance to use it

Other

During a penetration test the human rights act (1998) is fully applicable as well as laws such as the CMA and the PJA.

During a penetration test you gain access to a database containing personal details of staff the best course of action is to note the issue but do not store any of the personal data on your system.

In a penetration test you and your colleagues identify instances of child pornography on a server, the correct course of action is to contact the Local Police.

In a penetration test you find evidence of insider trading and financial fraud on a server; the correct course of action is to contact the NCA.

Making supplying or obtaining articles for use in computer misuse offences is an offence under Section 37 of the Police and Justice Act 2006.

Article 8 - Right to respect for private and family life is part of the **Human Rights Act** and should be considered by consultants while testing

Principle 7 of the UK data protection act requires you to have appropriate security measures in place for any personal data you hold.

Users should be informed that a penetration test is being carried out, they have a right to know when their privacy may be breached unless the system's AUP says otherwise.

In 2003 the **Communications Act** made it illegal to use other people's wifi broadband connections without their permission

Full name date of birth and address would be considered personally identifiable information with regards to the **DPA (1998).**

Vulnerabilities

0x90 in Intel x86 assembly is known as the NOP (no operation) instruction – it's often used as part of a **buffer overflow attack**.

Missing patches are a big problem with both **Microsoft** and **Nix** devices and is classed as a common vulnerability.

DDoS stands for Distributive Denial of Service

A vulnerability whereby two processes are competing for a resource within a given timeframe is known as a **race condition.**

An action triggered by a specific condition is known as a **logic bomb**.

Improper error handling can lead to: - Attackers can use error messages to extract specific information from a system, unexpected errors can provide an attacker with a buffer or stack overflow condition that sets the stage for an arbitrary code execution, attackers can use unexpected errors to knock an application off line creating a denial-of-service attack.

A vulnerability whereby **ICMP packets flood** a network is known as a **Smurf Attack**.

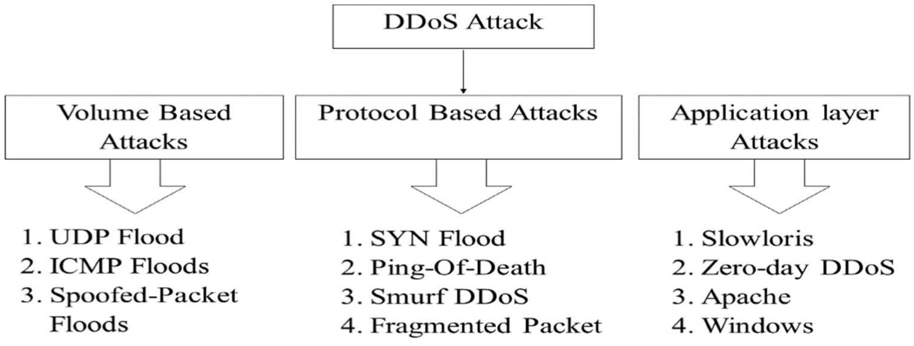
MAC flooding is a type of active sniffing attack that attempts to overflow the switch's content addressable memory (CAM).

A **MAC flooding** attack can be used to force some **switches** to forward frames to all ports.

A technique that forwards traffic to an attacker's system by associating the attacker's MAC address with the IP address of the target system is known as **ARP spoofing** or **ARP poisoning**

ARP poisoning would directly enable you to perform a man-in-the-middle type of attack.

An **ISAPI Extension buffer overflow** allows an attacker to take control of an IIS webserver from the Internet through a firewall.



CyberSecurity and Technical Controls

Detect is the first D represent in the **DDPRR security model**

OVAL stands for the following: - Open Vulnerability Assessment Language

The CIA model of security consists of Confidentiality Integrity and Availability. Another highly desirable security feature of a networked environment is accountability.

The term CVE Stands for Common Vulnerability and Exposure

Low is the risk rating is given to a vulnerability with a **CVSS of 1.5.**

The access control method known as **Discretionary Access Control (DAC),** places control of security considerations with the user.

A CVSS score of 10 relates to a high or critical vulnerability discovered which could result in full system takeover.

An audit trail is considered a **detective** control.

Smart card authentication is considered a **preventive** control

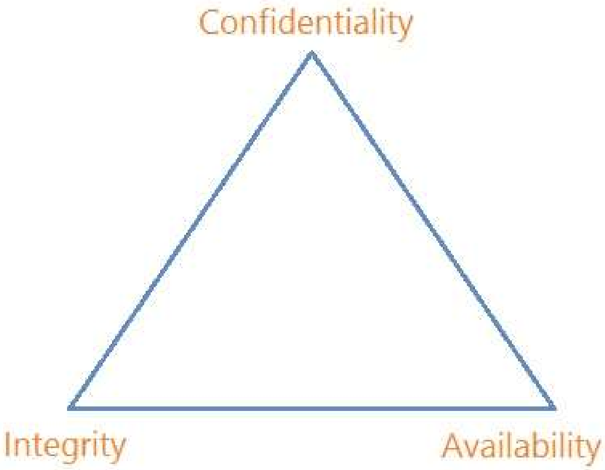
A **covert channel** is one that transfers information over a computer system, or network that is outside of the security policy.

Root squashing is a mechanism to Limit the capabilities of the root user.

SYN-cookies protect you from SYN floods.

Steganography is the concept of hiding a message within other information.

Encryption is a **Preventative** security control.



Red Teaming / Physical Security

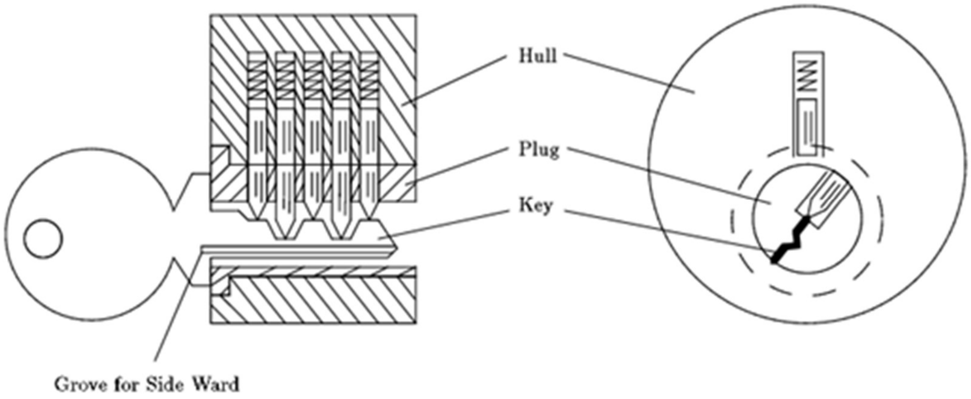
Open-source intelligence **(OSINT)**describes freely available material on the Internet which may be useful to an attacker

Use of mobile phone messages to induce people into divulging their personal information is known as **Smishing**.

Cipher locks include a keypad that can be used to control access into areas.

Piggybacking / tailgating is one of the primary ways that people can get past controlled doors.

Warded locks are considered easy to pick (A warded lock is a type of lock that uses a set of obstructions, or wards, to prevent the lock from opening unless the correct key is inserted. The correct key has notches or slots corresponding to the obstructions in the lock, allowing it to rotate freely inside the lock)



Shredders (shredding all confidential materials) are a physical security measure to prevent dumpster/bin/skip diving.

A system with a low crossover error rate (CER) would be a good biometric device to use as a technical control.

An eight-foot chain link fence is a the recommended **physical security** for premises.

Locks are considered a **Preventive** control

Attackers social engineering phone providers to give replacement SIMS is a weakness of **SMS 2FA**. Two Factor Authentication.

CHECK

Exploitation of vulnerabilities should always be the default unless the point-of-contact says otherwise, is the default stance according to NCSC regarding exploitation of vulnerabilities on a **CHECK test**.

Official-sensitive is the minimum classification of a **CHECK level penetration testing** report.

Its worth noting that with **CHECK level penetration testing** reports, copies may go to **NCSC** for auditing purposes

It should be noted that a list of all tools used, and all tool output must be recorded when conducting a **CHECK penetration test**.

Scoping

The **scope** of work should be defined before testing is started

When **scoping** a vulnerability scan User credentials are not required as such but can be requested a head of time as part of the clients **change process**.

Network segregation testing, internal penetration testing, and external (internet facing) penetration testing are all in scope for **PCI DSS compliance tests**.

Reporting

Non-technical style of language should be used in an executive summary of a penetration testing report.

The QA process is an important stage of the penetration testing report lifecycle simply because it improves the end product that the client sees. You become blind to your own errors sometimes and another set of eyes and a second opinion makes a big difference.

Cracked passwords should not be in a **penetration testing report** in an unredacted form.

A repeatable walkthrough of exploits would be expected in the detailed findings of a **penetration testing report**.

With regards to **penetration testing reporting**, attack surface is measured as a size (small, medium, large etc)

After gaining access to a span of network that connects local systems to a remote site, you discover that you can easily intercept traffic and data. In your report as a countermeasure, you should recommend **encryption**.

Web/Apps/Online

A valid **enumeration** technique is to send an email to a non-valid address or browse to a non-valid application page to generate a response back that will reveal information about servers.

LAMP stands for Linux Apache MySQL PHP which is a development software stack.

Enumerating Microsoft IIS 5.0 on a web port might be a sign of a Microsoft Windows Server 2000 operating system.

Parameterised statements or **prepared statements** are the best-practice method of protecting against SQL Injection attacks.

The **HTTP Host header** is used when two domains exist on a single web server.

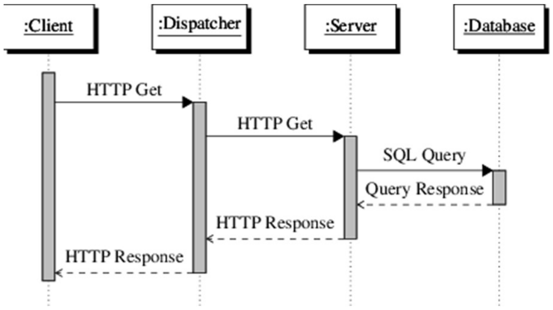
OWASP is an open-source test methodology used, typically, for application testing. It has a famous top 10 of web, mobile and API vulnerabilities which is updated from time to time.

“telnet webserverAddress 80 HEAD / HTTP/1.0” can be used to **fingerprint** a web server.

ICANN oversees “.co.uk” domain registrations.

Cross-site scripting is a **vulnerability** that affects the **integrity** of client-side application code.

Cross-site scripting is a **vulnerability** that affects the **confidentiality** of a web application user’s data:



A **Proxy server** is the best choice for a device to filter and cache content from web pages.

On the **Microsoft IIS** web server, you would expect to find **ISAPI** filters and extensions.

PHPMyAdmin is used to manage SQL Databases

Basic sqlmap flags: -

-u url

-r request

-p parameter

Inject client-side scripting languages into a website application describes an XSS (Cross-Site Scripting) vulnerability

HTTP response code **307** - Address Changed Temporarily

HTTP response code **413** - Request Entity Too Large

HTTP response code **301** - Moved Permanently

HTTP response code **407** - Proxy Authentication Required

A **directory traversal vulnerability** permits traversal to directories not in the expected path.

The purpose of a **robots.txt** file is to inform web crawlers where to index and not index.

www.v1p3r.net/download.php?file=passwords.txt is an example if Insecure Direct Object Reference (IDOR)

SQL Injection is classed as a **Server-side** attack.

A **Cross Site Request Forgery (CSRF)** vulnerability can be used to impersonate a user on a web application.

Session hijacking is performed after the 3-way handshake.

To enumerate a **Cisco IronPort** web security appliance, look for the following **Set-Cookie: ARPT=ITOUQOwebserver1CKUQW**

RIPE is an internet organisation residing in Europe.

Nikto and **skipfish** are applications that can ‘specifically’ be used in order to perform an automated vulnerability scan of a web server.

The following are types of SQL injection techniques: **Union, Time and Error.**

The following are examples of HTTP Web Verbs: **PUT, HEAD, POST and PROPFIND (get properties)**

Client-side data validation is **NOT** recommended for securing Web applications against authenticated users

The **wayback machine** is an archive web service for finding information from historical web pages.

The **wget** and **curl** tools can download web pages for further inspection.

The default privilege of an **IIS4** server is **local system.**

The default privilege of an **IIS6** server is IUSR_Computername.

Exploiting a vulnerability in a **CGI script** might leave the following in a **log file**: http://server/cgi-bin/phf?v1p3r=x%0a/bin/cat%20/etc/passwd.

Networking / Firewalls / Routing / Protocols

Firewalls / Network security devices

An **ACK scan** would allow you to determine if a stateless firewall is being used.

A **circuit level gateway** works at layer 4 (TCP) of the **OSI Model**.

A company **firewall** engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:Untrust (Internet) (Remote network = 217.77.88.0/24)DMZ (DMZ) (11.12.13.0/24)Trust (Intranet) (192.168.0.0/24)The engineer wants to configure remote desktop access from a single host on the remote network to a remote desktop server in the **DMZ**. The advice to achieve this might be - Permit 217.77.88.12 11.12.13.50 RDP 3389.

The **firewall** requirements of an organisation states the firewall needs the capability to stateless filter traffic by port or IP address. An **access control list** implemented on a router can fulfil this.

A hardware requirement of an **IDS/IPS** system or a **proxy server** is they must be **dual homed**.

If a **firewall** is only monitoring TCP handshaking of packets at the session layer of the OSI model. This would be an example of a **Circuit-level gateway firewall**.

A network you are testing has **NAC**, that filters the MAC address of devices. To gain access you could plug into the same port and **spoof** the MAC address of the host you have unplugged.

“**Firewall rules**” describes a method of managing the flow of network traffic by allowing or denying traffic based on ports, protocols, and addresses.

Firewalking is a technique used to discover what rules are configured on the gateway (A gateway can be used to describe a firewall, a router, an entry point to a network ie vpn concentrator).

Routing / Routers

CIDR – Classless inter-domain routing - ***CIDR*** is a bitwise, prefix-based standard for the interpretation of IP addresses

Distance Vector - RIP, RIP2, RIP NG, IGRP

Link State – OSPF, IS-IS

Hybrid - EIGRP

OSPF stands for **Open Shortest Path First**.

The routing protocol RIP is normally based on port **UDP 520.**

In **RIP v1** routers only actually communicate to those directly connected to each other.

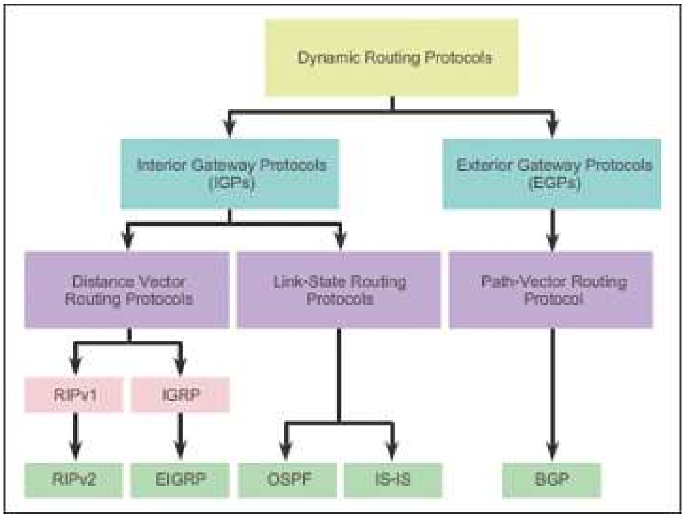
The potential security implications of an attacker being able to modify routing information on a network are: **Man-in-the-middle attacks, Interception and Denial of Service.**

In **network routing** if the **TTL (time to live)** reaches 0 before a given packet arrives at its destination the datagram is discarded and an **ICMP error message** is sent back to the sender.

The primary aim of a router is to stop **broadcast traffic** (Cisco Knowledge) – the maximum recommended number of devices on a subnet is 500.

A security feature of OSPF is it can authenticate peers using MD5 authentication.

The principles underlying security in **RIP Version 2** are it supports **authentication** in **plaintext** by default.


Dynamic Routing Protocols
Interior Gateway Protocols (IGPs)
Exterior Gateway Protocols (EGPs)
Distance Vector Routing Protocols
Link-State Routing Protocols
Path-Vector Routing Protocol
RIPv1
IGRP
RIPv2
EIGRP
OSPF
IS-IS
BGP

DNS

CNAME, HINFO, MX and **A** are all examples of DNS record.

DNS usually uses TCP port 53 for zone transfers and UDP port 53 for lookups.

With the Domain Name System (DNS), the **MX** record is used to refer to a Mail Server.

The command **nslookup** is specifically used to perform a **DNS IP lookup** for a specified hostname.

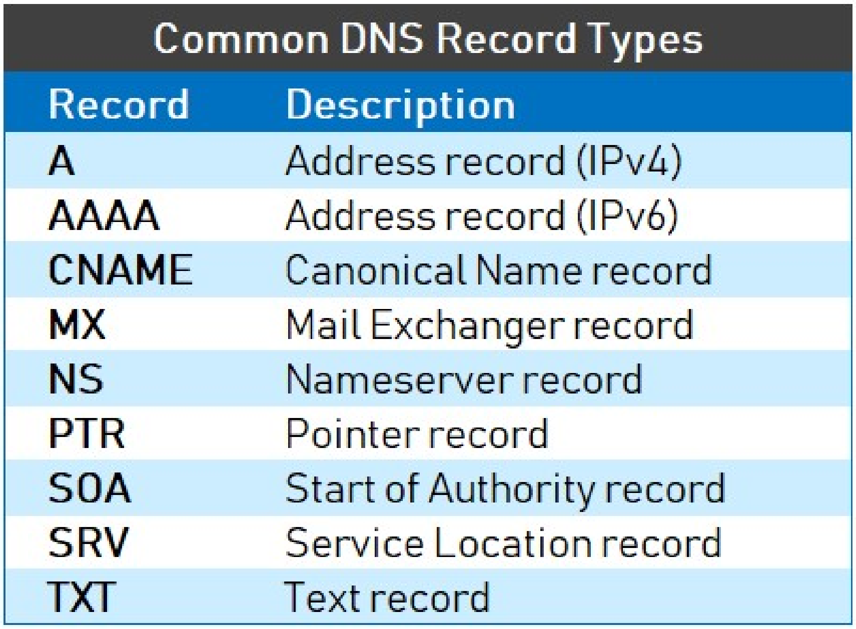
When a primary **SOA serial** number is higher that a secondary SOA, the secondary name server requests a zone transfer from a primary name server.

SOA (in DNS) stands for start of authority. The **SOA** determines the length of CACHE settings etc – which might be of concern if the DNS is hacked.

Running the command **dig @dns.fidus.com version.bind txt chaos** is an attempt to identify the software version.

A **PTR** (DNS) record is for an IP to Hostname lookup

BIND is open-source software that enables you to publish your Domain Name System **(DNS)** information on the Internet, and to resolve DNS queries for your users. DNS does not by default encrypt its traffic.



Common DNS Record Types

Record	Description
A	Address record (IPv4)
AAAA	Address record (IPv6)
CNAME	Canonical Name record
MX	Mail Exchanger record
NS	Nameserver record
PTR	Pointer record
SOA	Start of Authority record
SRV	Service Location record
TXT	Text record

SNMP

SNMP stands for Simple Network Management Protocol

SNMP v1 and **2c** sends data in the clear and is therefore considered to be insecure.

With SNMP, MIB stands for **Management Information Base**.

An **SNMP** message has the following format (in order): Version Number, Community Name, SNMP PDUs

In order to access information saved on a MIB (**think SMTP**) you need to know the community string on versions 1 and 2/2c and the credentials on version 3. The default write string is “Private”.

SNMP uses the UDP protocol by default but not exclusively.

The main difference between **SNMPv3** and **SNMPv2** is enhanced security.

With SNMP, OID stands for **Object Identifiers**

SNMP normally operates on UDP/161

TCP/IP/UDP/ICMP/OSI Model

ICMP (Internet control messaging protocol)

The lack of an **ICMP Port Unreachable** message is how Nmap discover an open UDP port

The destination port information takes up 16 Bits in a **TCP packet**.

The combination of the **IP address** and a port number make up a **Socket (ie 192.168.0.1:8080).**

There are **128 bits** in an **IPv6** address

There are **4 bytes** in an **IPv4** address (4 x 8 bits 32bits)

A class B network supports 65534 (65536-2) hosts (2^16 the same as the number of TCP ports)

There are **7 layers** in the **OSI model -** Physical, Data Link, Network, Transport, Session, Presentation, Application.

The 32-bit **internet address** 10000000 00001010 00000010 00011110 can be written in dotted decimal notation as 128.10.2.30.

The **subnet mask** 255.255.0.0 allows for 65,534 hosts.

The maximum number of hosts within a **Class C Subnet** is 254.

If a system on a **Class B** subnet has the IP address 172.16.58.195 and the subnet mask 255.255.0.0. Its **broadcast address** would be 172.16.255.255

You know services, such as web and mail, are on a device but you cannot get a ping reply from these devices. A reason for this could be that a packet filter is blocking **ICMP ping**.

HTTP/FTP/POP3 are at Layer 7 (Application Layer) of the OSI model.

TCP/UDP are at Layer 4 (Transport Layer) of the OSI model.

IPV4 is at Layer 3 (Network Layer) of the OSI model.

ARP is at Layer 2 (Datalink Layer) of the OSI model.

Logical Link Control (LLC) is a sub-layer of layer **2** of the OSI model

Segmentation of a data stream happens at the Transport (4) layer of the **OSI model**.

A **Datagram** is defined in the **RFC 1594** as “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."

The TCP and UDP ports, **0 - 1023** inclusive, are called **privileged ports** where only a privileged user can listen on them.

Point-to-Point Tunnelling Protocol PPTP - is an obsolete method for implementing virtual private networks. (TCP port 1723 and IP protocol 47)

The function of the **ARP** protocol is to map **IP addresses** to layer-2 hardware addresses.

Decimal to binary - The IP Address 192.160.1.14 represented in binary as 11000000.10100000.00000001.00001110

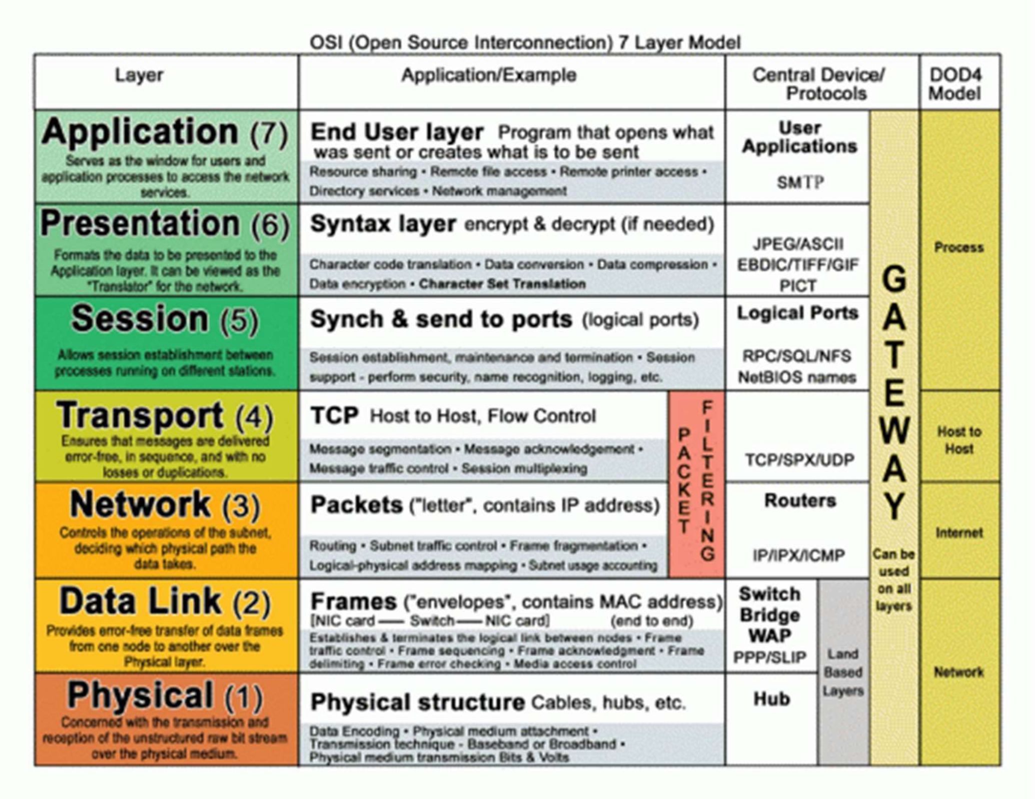
Mac addresses - The OUI part of the Ethernet MAC address 00:0B:45:48:29:80 is 00:0B:45

The purpose of the ICMP protocol is to take care of error-handling in the network.

The **TCP three-way** handshake is Syn Syn-Ack Ack.

Record Route (ping -r or ping -R #depends on the system) store the list of hops in the **IP Header.**

TCP: - **TCP** should be used where **reliability IS** a concern, TCP is stateful, TCP is a transport protocol, TCP supports error-checking.



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

192.168.14.220 is an example of a non '**routable**' external IP address.

0:0:0:0:0:0:0:1 or ::1. corresponds to the IPv6 loopback address.

10.0.0.0/16 does NOT correspond to an RFC 1918 reserved address range.

If you issue an **ICMP type 8** request to an IP address on the local network that has not been assigned to a computer, you will get a **ICMP type 3 code 1** host unreachable response.

VPN concentrator is a network device that allows remote users access to a network.

fe80:b3ff:fe1e:8329 is an invalid **IPv6 address**, its important to know why

The **CDP** protocols is proprietary to **Cisco**.

IPv4:- the IPv4 protocol is primary concerned with routing, the IPv4 protocol operates at layer 3 of the OSI reference model and the IPv4 protocol contains a header checksum

Multicast is a technique to send packets to multiple destinations using the most efficient way to produce a simultaneous delivery.

01:00:0c:cc:cc:cc is an example of an ethernet **multicast MAC address**.

Record Route is an IP option in the **IP protocol**.

192.168.259.1 is not a valid **IPv4** address, it's important to know why.

2001:0db8:1428:57ab is not a valid **IPv6** address, it's important to know why.

ICMP message types: -Source Quench, Echo reply, Echo request, Router Solicitation

A **TCP port scan** would be most likely to discover a firewall that blocks all traffic to itself from the interface connected to the network you are scanning from

IPV6 address- 16 bytes (octets)- 128bit

IPV4 address - 4 bytes (octets) - 32 bit

Control Bits (6 Bits):

– URG: Urgent pointer field significant.

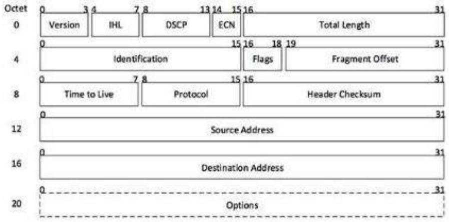
– ACK: Acknowledgement field significant.

– PSH: Push function.

– RST: Reset the connection

– SYN: Synchronize sequence numbers.

– FIN: No more data from the sender.



[Image: IP Header]

SMB/NFS

'**NFS**' traditionally stands for **Network File System**.

CISCO

CDP - Cisco discovery protocol- spoofing- dos attack , v1 and v2

HSRP - Hot Standby Router Protocol - Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway

VRRP - Virtual Router Redundancy Protocol (VRRP) provides for automatic assignment of available Internet Protocol (IP) routers to participating hosts.

VTP On Cisco Devices, VTP (VLAN Trunking Protocol) maintains VLAN configuration consistency across a single Layer 2 network

STP - The Spanning Tree Protocol (STP) is a network protocol that builds a loop-free logical topology for Ethernet networks.

ND - The Neighbor Discovery Protocol is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6). It operates at the link layer of the Internet model (RFC 1122), - is responsible for gathering various information required for internet communication.

Misc

SFP – small form-factor Pluggable modules (GBIC, SONET, Fibre, RJ45)

C14 Cable – data centre 13amp converters

Message authentication code, Ticket granting service, Authentication service are all parts of the **Kerberos** authentication implementation.

128 is the default **TTL** (Time To Live) for a Windows device (64 for nix, 254 for some network devices or old nix systems)

RSH uses .rhosts files and /etc/hosts.equiv for authentication.

MS-RDP (typically) runs on TCP port 3389

TFTP does not require authentication, which can be considered a weakness if not used correctly.

The **FTP** protocol uses TCP/20 and TCP/21 ports in active mode

The FTP transfer modes are: Stream, block, compressed and the communication modes are active and passive modes. The data types are Ascii, Binary (image mode), EBCDIC and local. Distributed is **not** an **FTP transfer** mode or **communication mode**

995 TCP is associated with a POP3 service (secured POP3)

DHCP stands for Dynamic host configuration protocol.

TELNET is an is an example of an unencrypted protocol. **Telnet** sends data, usernames and passwords in the clear.

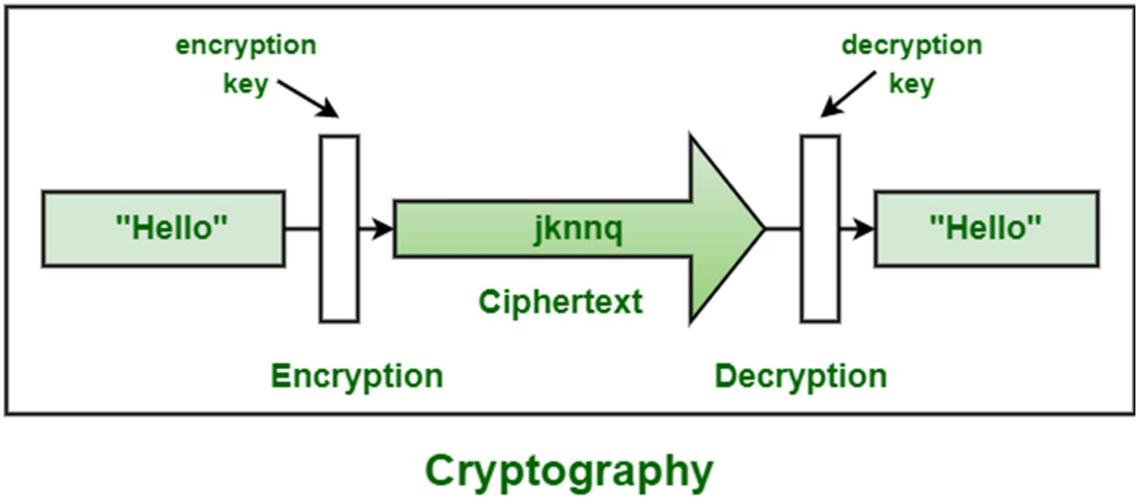
VLAN segregation can mitigate ARP poisoning attacks in a network. **VLAN 1** is the default VLAN on most switches.

Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology, user or system authentication and network security enforcement

Cryptography

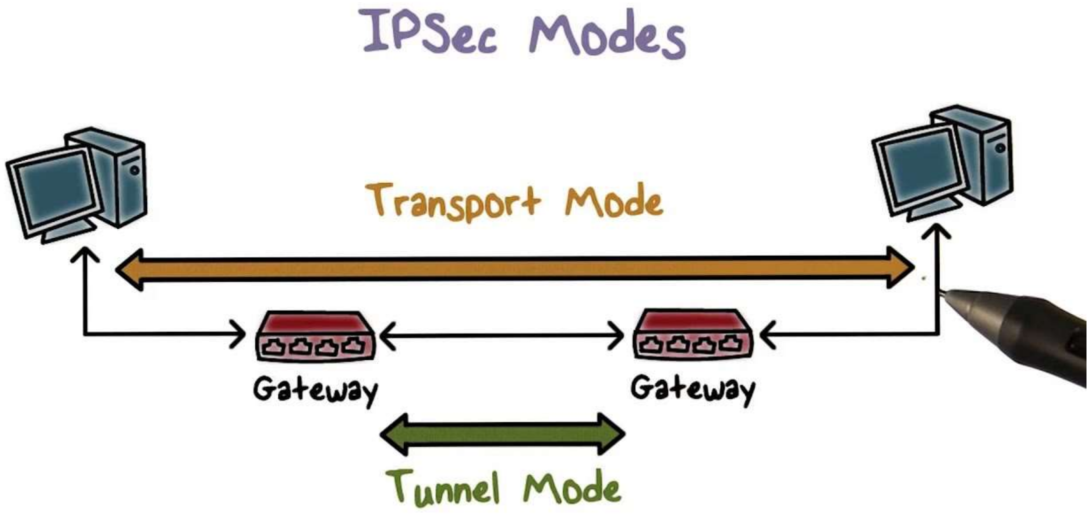
Symmetric – 2 x same key - AES, DES, IDEA, Blowfish, RC4,5,6 (Rivest cipher)

Asymmetric – Public Key (RSA - Rivest, Shamir, & Adleman) - Diffie-Hellman, Elliptic curv, RSA (Rivest, Shamir, & Adleman) Cramer-Shoup, YAK used in IPSec, PGP, GPG, TLS/SSL, SSH - Signing with private key



IPsec

- Used for app data at the data layer, routers (routing data), auth without encryption, VPN.
- 2 modes transport and tunnel - Encoding separate from modes
- Encoded using either ESP or AH
- ESP- Encapsulating Security Payload
  - data integrity, encryption, authentication, and anti-replay. Provides authentication for payload.
  - AH-Authentication Header - data integrity, authentication, and anti-replay - it does not provide encryption



This password “7 052D131D33556C081D021200” is an example of a password encoded with the **reversible Cisco** vigenere algorithm.

Payload encryption is a benefit of **IPsec**.

The **ssh-keygen** Linux tool can be used to generate an SSH key pair.

SSH 1.0 and **1.99** have significant flaws and should not be used. V 1.99 supports v1.0 and v2.0 and this can lead to v1.0 being used and it is known to be vulnerable to certain attacks.

If a system encrypts data prior to transmitting it over a network, and the system on the other end of the transmission media decrypts it using a different key, then an **asymmetric** encryption algorithm is used.

DES has an effective key length of 56 bits

Heartbleed was a vulnerability in **OpenSSL**

An **MD5sum** is made up of 32 characters.

If a file with one-way encrypted passwords were obtained, the type of process undertaken to find the encrypted passwords would be a **password cracking attack**.

If a user encrypted a project file with his **public key**. Later, an administrator accidentally deleted his account that had exclusive access to his **private key**, the file could be recovered if the organization uses a recovery agent.

Payload encryption is a benefit of **IPsec**.

The following are examples of a **TLS/SSL** vulnerability: **POODLE, Heartbleed, Beast, CRIME**

128, 192 and 256 are the valid key lengths for the **AES encryption cipher**.

TLS 1.0 – AES ciphers are affected by the **BEAST TLS/SSL Attack.**

SSL stands for **Secure Sockets Layer**.

Utilisation of the common “sslstrip” program can impact the data of the device being attacked in a compromise of **confidentiality** of the data-in-transit.

Weaknesses in the **TLS/SSL** cipher configuration of a service primarily impact the security of the data being transported in what way - Compromise of data confidentiality.

Rijndael is an encryption standard chosen as the replacement for **3DES**

If you **digitally sign** and inject a footer on an e-mail message in the wrong order, the footer will invalidate the signature.

An **MD5 hashing algorithm** produces a 128-bit hash value

A **hash function** is a one-way mathematical function that does not allow the original value to be calculated from the result.

The senders private key is generally used to create a **digital signature.**

Internet Key Exchange (IKE) is the protocol used to set up a security association in the IPsec protocol suite.

TLS/SSL used to encrypt data as it travels over a network.

128 bits is the **blocksize** of the **AES encryption cipher**

64 bits is the **blocksize** of the **DES encryption cipher**

The difficulty with **symmetric encryption** is assurance of secure receipt of the secret key used both for encrypting and decrypting

The purpose of **message integrity codes (HMAC)** is to simultaneously verify both data integrity (via cryptographic hashing function) and message authenticity (by use of a secret key)

Mitigation against the 'sslstrip' program is implementing a **Strict Transport Security** header.

Rainbow Tables would be useful to speed up a password cracking attack

RSA is an encryption algorithm which uses prime numbers to generate keys.

MD5 is considered a less secure encryption cipher than most.

The **SHA-256 algorithm** cannot be used for reversible encryption.

The **Diffie-Hellman** algorithm could be used to negotiate a shared encryption key.

The term '**Collision**' best describes what happens when two message digests produce the same hash.

A **file hash** would be different if you: - rename the file extension, change the content or change the file size.

The **CFB cipher** modes use a block cipher to generate a key stream that can be used as a **stream cipher**.

RSA is an asymmetric cipher encryption algorithm

3DES is a symmetric cryptographic standard. DES ECB is considered the weakest form of DES.

When using a **salt** value in a **password encryption algorithm**, two users with the same password could have different password hashes.

Of the accepted key sizes (128, 192, 256) for Advanced Encryption Standard (AES) algorithm, 2048 is **not** one of them.

Hashing algorithms such as **MD5** ads used for integrity

2048 bits **key sizes** are considered the minimum recommended for a new **SSL certificate.**

Being reusable is not a desirable feature for a **digital signature**

The **Diffie-Hellman protocol** was developed to be used for key exchange.

Base64 encoding is not designed for security encryption but for the storage and transit of data (such as binary to ascii).

Within **public key infrastructure (PKI)** - data encrypted with a public key can only be decrypted with the matching private key.

Integrity checking hashes will identify if computer files have been changed.

RSA (**Rivest–Shamir–Adleman**) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages.

RC5 is an example of a **symmetrical algorithm** and uses the same key to encode and decode data.

The **X.509** standard defines the structure of a digital certificate.

Collision resistance ensures that a hash function will not produce the same hashed value for two different messages.

IPsec uses UDP port 500, IP protocol 50 and IP protocol 51

Tunnel mode is a valid mode of operation for the **IPSec** protocol

Old legacy **Windows** systems may use **LM and NTLM** hashes. LM stored user passwords that are fewer than 15 characters long (Technically 14 chars plus a parity bit) and all chars were upper cased and there was a split at the 7th character so each half could be cracked independently. eg "PASSWOR" "D123". Both **LM and NTLM** hashes are stored by default on a Windows 2003 systems. LM and NTLM are not salted passwords. Because of the 7-digit split you can even tell if the 2nd part of the hash is in use or not and have some idea of the password length.

Metasploit / Exploitation

The **getsid** command can be use in **meterpreter** to show the security ID (SID) on a **Windows** device.

The **VNC authentication** bypass vulnerability in **Metasploit**: - affects version 4.0 of REAL VNC but this bypass does not stop active directory authentication.

Postgresql is used to support metasploit framework

Armitage is the name of the graphical version of **Metasploit.**

Sessions -i can be used to resume a background session in **Metasploit**.

Setg can b used to set global settings in **Metasploit**.

Metasploit's framework is written in **Ruby.**

The "Check" command in **Metasploit** checks if the vulnerability might be successful.

The "**execute –f cmd –I**" Which of the following commands would execute a command shell in **Metasploit**.

Mimikatz is a standalone program and a module in Metasploit to find cached credentials

The **MSFVennom Metasploit** tool can create custom payloads.

A **Bind** payload connect directly to the target host.

A **Reverse** payload connects back to the attacker's device.

AntiVirus software can cause a **meterpreter shell** to fail consistently after a few seconds

WIFI /VPN and Comms

The term **POTS** stand for **Plain Old Telephone System**

WEP stands for **Wired Equivalent Privacy.** The length of the IV for a **WEP** key is 24 bits. There are 104 secret bits in a 128-bit **WEP key. WEP wireless** encryption technology uses **3-byte IV**.

WPA stands for **Wi-Fi Protected Access. WPA** attacks generally work by capturing the handshake for **password cracking**. **WPA** is based on the International Standard **802.11g.**

Temporal Key Integrity Protocol TKIP - is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). **TKIP** was an interim solution to replace WEP without the requirement of replacing legacy hardware.

RADIUS (RADIUS - Remote Authentication Dial-In User Service - rides on udp - **only encrypts the users password**) is an authentication technology which is sometimes combined with **WPA**

Reverse telnet is a specialized application of telnet, where the server side of the connection reads and writes data to a computer terminal line (RS-232 serial port), rather than providing a command shell to the host device.

> On the client, the command line for initiating a "reverse telnet" connection might look like this:
>
> telnet 172.16.1.254 2002
>
> (The syntax in the above example would be valid for the command-line telnet client packaged with many operating systems, including most Unix operating systems, or available as an option or add-on.)
>
> In this example, 172.16.1.254 is the IP address of the console device, and 2002 is the TCP port associated with a terminal line on the server.

TACACS - Terminal Access Controller Access-Control System (TACACS, /ˈtækæks/) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server

TACACS+ have largely replaced their predecessors- tcp based, full encryption.

SSID stands for Service Set Identifier.

OSMisc

The Solaris 10 operating system is most likely to be vulnerable to the TTYPROMPT vulnerability in the telnet service

Some methods to determine if a remote host is running an X Window server that allows remote connections from the local host are: **xterm -display remotehost:0.0**

The Control Program component of an **operating system** is responsible for controlling the execution of user programs and operations of I/O devices.

SE Linux offers Trusted OS capabilities by default (However many others also do these days)

On a **Solaris** system the CONSOLE setting in “**/etc/default/login**” controls if the superuser is allowed to login over **Telnet**.

On a **Solaris** system, 'showrev -p' returns a list of installed patches on the system.

Rexec uses port 512/tcp as standard

Rlogin uses port 513/tcp as standard

Using the **netstat -p** command in **UNIX** displays the program identifier / program name.

Using **traceroute -I** on a UNIX system uses ICMP ECHO requests instead of UDP as used by default.

The **rpm -qa** command can be used to list the installed packages on a **Redhat or Fedora** system.

Pkg info, pkg search, pkg list are all commands to list the installed packages on a Solaris system.

showrev -a or showrev -p are all commands to list the installed **patches** on a Solaris system.

The **CHMOD** command is used to change the permissions of the specified file(s) # OMG is anyone even reading this at this point **ffs**.

The function of the **/etc/ftpd/ftpusers** file on a Unix FTP server is to lists the users that are NOT I repeat NOT permitted to use the FTP server. **#you been denied mofo**

The often-problematic service **CUPS** is a Printing service on Unix. **#2 problems 1 cup**

The command "**finger 0@hostname**" (that is a zero) used against a **Solaris 8** system would display users with an empty **General Comprehensive Operating System** (**GCOS)** field in the password file. A GCOS field is typically used to record general information about the account or its user(s) such as their real name and phone number. - In most UNIX systems non-root users can change their own information using the ***chfn*** or ***chsh*** command.

When considering possible threats to a **UNIX Network File Share** Server the following should be noted - They are at risk of unauthorised data exfiltration, They can put the client at risk of subversion from a program on the share, Weak authentication can enable a masquerade of client or server

The encrypted passwords on a **FreeBSD** system are stored in the **/etc/master.passwd** file. #WHY_just_why???

Windows

A **domain controller** (DC) will usually have ports 88 389 and 53 open. You may also see 3389, or 22 and other services too.

In Windows the **Sc query** command (CLI) could be used to list the **running services**.

The command for doing a trace route in **Windows** is **“tracert”.**

The built-in administrator account in **Windows** will never be locked out even if an account lock out policy is in place.

In Active directory **FSMO** stands for **Flexible Security Master Operations**

In **Windows**, the **hardware abstraction layer** acts as a go intermediary between the hardware and the Kernel.

In **Windows** the administrators **RID** is always 500 (Guest is 501, Kerberos is 502).

On a **Windows System** the command "**netstat** -p udp –a" displays all listening and active UDP ports on the current machine.

On a **Windows system** the active directory database file is NTDS.DIT

The domain credentials of a user are cached in the following formats **MS-CACHE**

If the following command is executed on a **Windows** machine: ipconfig /renew Local Area Connection 1 this renews only the named connection that matches.

If the following command is used on a **Windows** machine: ipconfig /renew this renews all IP addresses.

If the following **Windows** command is run: **net user paul.richards pa55word123** this resets the user paul.richards password to pa55word123

The **lservers** command can be used to obtain a list of systems from a master browser together with details about the version and available services on a **Windows** system.

The '**RestrictAnonymous**' setting of **2** on a **Windows** system does not allow access without explicit anonymous permissions. The '**RestrictAnonymous**' setting of **1** prevents the enumeration of SAM accounts and names.

On a Windows system the term **SAM** stands for **LSA Security Account Manager**. - **LSA** stands for **Local Security Authority.**

The Kerberos ticketing system is used for authentication in a Microsoft Active Directory domain.

A change in the patching policy is the **mitigation** you should recommend for a missing Microsoft patch (or two), however patching the missing shiz is also a high priority.

On a **Windows** 2003 SP1 Server you attempt a **MS08-067** exploit. The most likely outcome is You will get a shell but regardless of the EXITFUNC setting the server service will crash when you quit the session.

You would find the **Security Accounts Manager (SAM)** file on a Microsoft **Windows** operating system in the "C:\Windows\system32\config\" folder.

Windows systems - In order to escalate your privileges to a SYSTEM level account you could try: - SQL Injection, exploit weak services running as SYSTEM or Crack stored passwords

Within a **Windows** domain the security implication of a **bi-directional** trust relationship between domain A and domain B, If the domain administrator account on domain A is broken into then the domain administrator account on domain B is also broken into.

The following **ping** command sent from a Windows system "**ping -r 5 fidusinfosec.com -n 2**" pings the awesome site of **FIDUS INFO SEC** with 2 echo requests while recording 5 count hops.

Linux

0 is the **UID** of a root user on a Linux system.

The 777 value denotes full access (read/write/execute) to all users and groups on a Linux system.

The purpose of the **reference monitor** and **security kernel** (in an operating system) is to intercept and mediate subjects attempting to access objects.

In **Linux** the **wheel group** is used as the Administrators group.

LUKS on a Linux server is a disk encryption specification.

The passwords in Linux are stored using a **Hash** function rarely with an encryption function and not asymmetrical encryption.

On a **Nix** system the **/etc/shadow** file is readable by the root user.

The **chage** command in **Linux** is used to set the password age

The **cron** service performs scheduled tasks in **Nix** systems.

Suid files, can be located with the **find / -perm -4000** command to privesc on Nix systems.

The **df** command on a Linux server can be used to check the remaining disk space.

The **uname -a** command could be used to examine the kernel version of a Linux host.

To update some Linux distros you can use **apt upgrade**, some use **Yum** and other methods are available.

/etc/shadow in **Linux** is used to store account passwords

Dirty Cow (copy on write) an example of a Linux ubiquitous exploit. It exploits a race condition to overwrite data in memory or on disk. It is an example of a kernel exploit.

Basics of the Linux filesystem

- / — The Root Directory
- /bin — Essential User Binaries
- /boot — Static Boot Files
- /cdrom — Historical Mount Point for CD-ROMs
- /dev — Device Files
- /etc — Configuration Files
- /home — Home Folders
- /lib — Essential Shared Libraries
- /lost+found — Recovered Files
- /media — Removable Media
- /mnt — Temporary Mount Points
- /opt — Optional Packages
- /proc — Kernel & Process Files
- /root — Root Home Directory
- /run — Application State Files
- /sbin — System Administration Binaries
- /srv — Service Data
- /tmp — Temporary Files
- /usr — User Binaries & Read-Only Data
- /var — Variable Data Files

The **lsof** Linux command is used to check files opened by current user.

The **iptables -F** Linux command is used to clear all the current iptables rules

The passwd root Linux command would reset the root users password

NFS mount options:- nfsvers, nolock, rw, ro, suid, nosuid, hard, soft, intr, nointrm fgm bgfm devsm nodevs, timeo, retrans , rsize, wsize (**Auto** is not a known option)

The **#** symbol is used to denote a comment in a shell script.

Network Mapping

A Version scan (aka a service scan) is achieved by the flags -sV in **nmap**

Malware

Antivirus Heuristic scanning looks at the beginning and end of executable files for known virus signatures

A worm is **self-replicating,** but a **virus** isn't self-replicating

Trojans could inadvertently be installed with USB thumb drives

The **Sasser worm**:- MS04-011, starts an FTP server, it generates a list of IP addresses to target based on the infected host's IP addresses, it modifies the registry so that it runs on system start-up.

Worms are programs that can run independently, travel from system to system, and disrupt computer communications. They are self-replicating computer program that sends copies of itself to other computers on a network without any user intervention.

A **Boot Sector Virus** moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

A Virus is an application that requires a host application for replication

Enumeration

Active OS fingerprinting techniques sends specially crafted packets to the remote OS and analyze the received response.

You have become concerned that one of your workstations might be infected with a malicious program. The command **netstat -an** could help discover the issue.

Hardware

A **hard drive** is an example of **non-volatile** storage.

Databases

In the following **SQL Server** password hash, the salt value is 84449305: - 0x01008444930543174C59CC918D34B6A12C9CC9E.

Example SQL commands (note they end in a semicolon)

- mysql -h 10.0.0.1
- help;
- show databases;
- use staff;
- show tables;
- select * from passwords;
- select load_file('/etc/passwd');

Default database port numbers

- Oracle 1521
- Mysql 3306
- SQL server 1433 (and UDP port 1434) (TCP 2433 in hidden mode)
- Firebird / interbase 3050
- PostgreSQL 5432
- PervasiveSQL 5521
- MongoDB 27917 (Mongo is a no sql db)

In Microsoft SQL server using the "sa" account the stored procedure **xp_cmdshell** can be used to add user accounts and enumerate the system.

In **PostgreSQL**, a named collection of tables is called a Schema.

In **SQL**, the **SELECT DISTINCT** commands can be used to select only one copy of each set of duplicate rows

PostgreSQL is a relational database management system. Its an open-source ORDBMS developed at UC Berkley, which supports many modern features. It used a client/server model.

The command to remove a table customer from a database is: **DROP TABLE** <tablename>;

The extension used for data encryption/decryption within PostgreSQL is: **pgcrypto**

The **FROM SQL** clause is used to specify which table we are selecting or deleting data FROM.

The SQL condition for pattern matching is: **LIKE**

You can add data to PostgreSQL by using: **INSERT**

The **select @@version** command would display the version number of a Microsoft SQL Server database if you are connected with a command line client

Default database passwords

SYS in Oracle 10g: CHANGE_ON_INSTALL

SYS in Oracle 9: CHANGE_ON_INSTALL

SYS user on Oracle 9i: MANAGER

DBSNMP user on Oracle 9i: DBSNMP

sa (default password sa) – short for sysadmin - is the database administrator account on Microsoft SQL server

MONGODB has no enabled access control, so there is no default user or password. mongo.exe is the shell process and mongod.exe is the actual database process. It is written in javascript, C and C++

ALTER TABLE TableName DROP COLUMN ColumnName can be Used to delete columns from a SQL table.

Microsoft SQL Server enables **query stacking** (although so do most other SQL databases these days)

sysobjects is the default Microsoft SQL table

GROUP BY is an aggregate function in SQL

ORDER BY is a row sorting function in SQL

INSERT is a function in SQL to add a row.

DevSecOps

Basic python commands: -

- raw_input() – accept input from the user
- print("Hello, World!") - Display text
- python --version - find the python version
- #This is a comment - python programmers comment
- Python Variables
- x = str(3)   # x will be '3'
- y = int(3)   # y will be 3
- z = float(3) # z will be 3.0

Ansible by default uses **ssh** what to communicate with remote servers:

Ansible uses procedural syntax, **Terraform** does not

Dynamic analysis tools are useful for identifying **memory analysis.**

Static analysis tools are useful for identifying the use of **insecure functions.**

Terraform does not use procedural syntax.

Both **ansible** and **terraform** (Infrastructure as Code tools) use a masterless infrastructure architecture to store the state of infrastructure and updates (in a usual deployment case)

Key based authentication is the most secure, practical authentication option for Ansible to authenticate to the remote hosts.

"aws_secret_access_key" is the standard variable name for AWS API keys.

Branch policies can be used as a method to validate whether the code meets the company's quality standards and code review standards in **Azure DevOps**

The **.gitignore** file can be used within **Git** to ensure specific files are not tracked.