IP Address Classes

	Start address	End address
Class A	0.0.0.0	127.255.255.255
Class B	128.0.0.0	191.255.255.255
Class C	192.0.0.0	223.255.255.255
Class D	224.0.0.0	239.255.255.255
Class E	240.0.0.0	255.255.255

CIDR Address block	Description
0.0.0.0/8	current Network
10.0.0.0/8	Private Network
127.0.0.0/8	Loopback
169.254.0.0/16	Link Local
172.16.0.0/12	Private Network
192.0.0.0/24	Reserved (IANA)
192.0.2.0/24	TEST-NET-1
192.88.99.0/24	IPv6 to IPv_4 relay
192.168.0.0/16	Private Network
198.18.0.0/15	Network benchmark tests
198.51.100.0/24	TEST-NET-2

203.0.113.0/24 TEST-NET-3

224.0.0.0/4 Multicasts

240.0.0.0/4 Reserved

255.255.255.255 Broadcast

IPv_4 - 32 bits

IPv_6 - 128 bits

TCP works on Transport Layer

TCP - Establishes 3-way (3-step) handshake

TCP Security Problems

Denial of Service

* SYN Flood attack
* Sockstress
* TCP persistent Timer DOS

Connection Hijacking

* Attacker who is able to eavesdrop a TCP session and redirect packets can Hijack a TCP connection.
* TCP Sequence Prediction Attack
* Hunt and Juggernaut tools can be used to perform this attack.

Port Scanning

Port Open - SYN + ACK is returned

Port Close - RST is returned

User Datagram Protocol (UDP)

UDP Security Problems

UDP also works on Transport Layer

* DOS - UDP Flood attacks
* Spoofing / MITM

Port Scans

Port Open - reply / noreply

Port closed - ICMP desination unreachable + Port unreachable.

Internet Control Messaging Protocol (ICMP)

Security Problems in ICMP

* Easy to spoof since no src/dst checking is performed
* Subnet mask request reveals network topology
* Timestamp request can obtain the system time of a target for timing based attacks
* Redirect messages can leads to routing attacks

CAT 5 / Fibre - Category 5 cable

10/100/1000 baseT - supports half & full duplex communication.

Token ring - Token Ring Local Area Network in Datalink Layer

Wireless (802.11) - IEEE 802.11 is a set of standards carrying out wireless local area network (WLAN)

Encoding - preservation

Encryption - obfuscation

Symmetric key - It uses the same cryptographic keys for both the encryption of plaintext and decryption of plaintext.

Example: Twofish, Serpent, AES, Blowfish, CAST DES, RC4, TDES and IDEA.

Asymmetric key - It uses a pair of related key one public key and one private key. to encrypt and decrypt a message and protect it from unauthorised access of use.

Example: RSA

Algorithm	key size	Block size
DES	56 bits	64 bits
3DES	112 or 168 bits	64 bits
AES	128, 192, 256 bits	128 bits
RSA		214 bits
RC4	40-2048 bits	2064 (1684 effective)

SHA1 - Secure Hashing Algorithm 1

Its a cryptographic has function which takes an input and produces a 160 bits.

MD5 - Message Digest Algorithm is a cryptographic broken but still widely used hash function producing 128 bits

HMAC - Hash based Message Authentication Code

HMAC lets you verify both authenticity and origination of the data.

SSL - Secure Socket Layer (443)

IPSec - Internet Protocol Security (500 and 4500)
researchers had identified issues related to Internet Key Exchange protocol (IKEv1)

SSH - Secure Shell (22)
(or)
Secure Socket Shell.

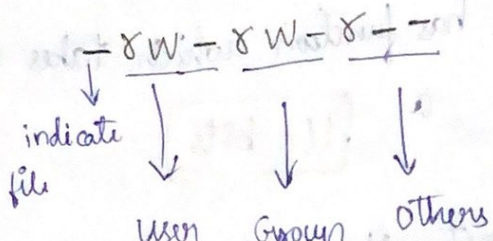
PGP - Pretty Good Privacy

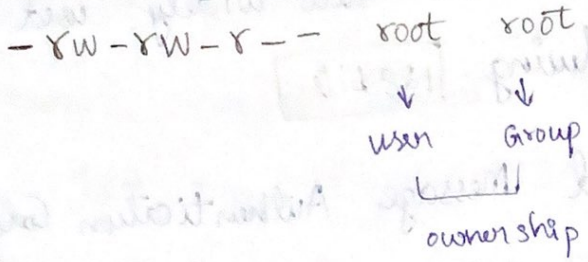
WEP - wired Equivalent Privacy (40bit Encryption)

WPA - Wi-Fi Protected Access (TKIP Temporal Key Integrity Protocol)

WPA2 - Wi-Fi Protected Access 2
(uses AES) Asymmetric encryption

Unix file Permission





Analysing Registry ACL's

Query Value - Permission to read a entry from regis

Set Value - Permission to set entries in registry

Create Subkey - Permission to create subkeys on a selected registry key

Enumerate Subkey - identify the subkey of a registry ke

Notify - receive notification events from a key

Create link - create symbolic link

Delete - delete a registry object

Write DAC - write a discretionary access control list

Write Owner - change the owner of the selected key

Read Control - Open the discretionary access contro

Computer Misuse Act - 1990

Human Rights Act - 1998

Data Protection Act - 1998

Police and Justice Act - 2006

Microsoft windows Security Assessment

Identify windows domain/workgroups :

```
c:\ net view /domain
```

Domain Members

```
c:\ net view /domain:<domain Name>
```

Linux tool

```
nmbscan -d    domain list
nmbscan -m    domain list with master browsers
nmbscan -a    domain list, master browser, servers
```

Identify key servers within Target domains

```
netview /T /NTS /domain:<name>    servers
```

Identifying and analysing internal browse Lists

```
nbtstat -A <IP address>    Single host
```

<\\--__MSBROWSE__> Master Browse

Identifying and analysing accessible SMB shares

null sessions - net use \\<IP_address>\IPC "" /u:""

Active Directory

Active Directory stores information about objects on the network and makes the information easy for administrators and users to find and use.

Global Catalog

* It acts as a domain controller that stores object data and manage queries about objects and most common attributes (called Global Catalog Partial Attribute Set or PAS).
* It provides data that permits network log

Master Browser:

When a windows domain spans multiple subnet each of the subnet has an independ browser called Master Browser

FSMO:

specialized domain controller (DC) set of tasks where standard data transfer and update meth are inadequate.

Roles in FSMO

* Schema Master — one per forest
* Domain Naming Master — one per forest
* Relative ID Master — one per domain
* Primary Domain Controller — one per domain
* Infrastructure Master — one per domain

Group policy:

* A group Policy Object (GPO) is a virtual collection of policy setting.

* A GPO has a unique name, such as a GUID

Local Security Policy:

The local security Policy of system is a set of information about security of local Computers

Password Policies:

Enforce password history - 24 new password before reuse

Maximum Password age - 30 days - change every month

Minimum Password age - 2 days - can't change quickly

Minimum Password length - 8 characters - harder to bruteforce.

Password must meet Complexity requirements (min-1 upper, 1 lower, 1 number/special)

Account Lockout Policy

Duration - 30 minutes

Threshold - 5 attempts

Reset account lockout after - 30 minutes

Windows: Pre 2008 - no lockout applied

SID 500 - if account renamed.

Unix Security Assessment

rusers

port : 111 port

rusers -l <target>

[List of users logged on to remote machines]

rwho

port : 513 (UDP)

rwho -a

[List of current users who are logged into the all hosts]

SMTP

port - 25.

EXPN, VRFY, RCPT TO

finger

port - 79

It is used for querying host about the users that are logged on.

R* Services

rexecd - TCP port 512 - always require username and password

rlogind - TCP Port 513 - use hosts.equiv as r.host

rshell - TCP port 514 - use hosts.equiv as r.host

X11

X windows is commonly used for displaying graphical applications

Port - 6000 to 6063

xhost - host based authentication allows user to specify which IP addresses and hosts have access to the X-servers

xauth - most secure. The X server has a 'Cookie' (MIT-MAGIC-COOKIE-1)

RPC Services

Port : 111 (UDP, TCP)

rpcinfo -p <target>

SSH

Port : 22

Authentication mechanism in SSH

* Password based
* Public key
* keyboard Interactive
* GSSAPI Authentication