Algorithms			
Symmetric		**Asymmetric**	**Hash** (value output)
DES	56 Bits (8 bits for Parity)	**Diffie-Hellman**- Uses SSL & IPSec	**MD5** – 128bits
3DES	168 Bits	**ECC** – Uses points on curve, for encryption. Good for mobile.	**SHA-1** – 160-bits
AES	128,192,256 Bit Variation	**El Gamal** – No Prime #'s. Solves discrete logarithm problems.	**SHA-2** 224,256,384,512
IDEA	128 Bits	**RCA** – Achieves strong encryption using 2 large prime numbers	
TwoFish	Up to 256 Bits		
Blowfish	64 Bit block & key 32 - 448 Bits		
RC	(Variable) up to 2,040 Bits		

Hacking Steps	Pre-Attack Phase	Scanning Methodology
Reconnaissance – Gathering Evidence	Gather Info	Identify Live Systems
Scanning & Enumeration – Applying Tools	Determine Network Range	Discover Open Ports
Gaining Access – Attacking & Exploitation	Identify Active Machines	Identify OS & Services
Maintaining Access – Apply Backdoors	Find Open Ports & Applications	Scan For Vulnerabilities
Covering Tracks – Avoid Detection	Fingerprint OS	
	Fingerprint Services	
	Map the Network	

ICMP Message Type	Description & Codes
0: **Echo Reply**	Answer to a Type 8 Echo Request
3: **Destination Unreachable**	Error message indicating the host or network cannot be reached. **Codes:** 0—Destination network unreachable 1—Destination host unreachable 6—Network unknown 7—Host unknown 9—Network administratively prohibited 10—Host administratively prohibited 13—Communication administratively prohibited
4: **Source Quench**	A congestion control message
5**: Redirect**	Sent when there are two or more gateways available for the sender to use, and the best route available to the destination is not the configured default gateway. **Codes:** 0—Redirect datagram for the network 1—Redirect datagram for the host
8: **ECHO Request**	A ping message, requesting an Echo reply
11: **Time Exceeded**	The packet took too long to be routed to the destination (Code 0 is TTL expired).

Well Known Ports					
Port Number	**Protocol**	**Transport Protocol**	**Port Number**	**Protocol**	**Transport Protocol**
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP/UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP/UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP/UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP
• Well-known: 0–1023		• Registered: 1024–49151		• Dynamic: 49152–65535	

DNS RECORDS

Services (SRV)	**Defines the host name and port number of servers providing specific services.** (for example: a Directory Services server)
Start of Authority (SOA)	**Identifies the primary name server for the zone.** The SOA record contains the host name of the server responsible for all DNS records within the namespace, as well as the basic properties of the domain.
Pointer (PTR)	**Maps an IP address to a host name (providing for reverse DNS lookups).** You don't absolutely need a PTR record for every entry in your DNS namespace, but these are usually associated with e-mail server records.
Name Server (NS)	**Defines the name servers within your namespace.** These servers are the ones that respond to your clients' requests for name resolution.
Mail Exchange (MX)	**Identifies your e-mail servers within your domain.**
Canonical Name (CNAME)	**Provides for domain name aliases within your zone.** For example, you may have an FTP service and a web service running on the same IP address. CNAME records could be used to list both within DNS for you.
Address (A)	**Maps an IP address to a host name, and is used most often for DNS lookups.**

nmap Switch	Description	nmap Switch	Description
-sA	ACK scan	-PI	ICMP ping
-sF	FIN scan	-Po	No ping
-sI	IDLE scan	-PS	SYN ping
-sL	DNS scan (a.k.a. List scan)	-PT	TCP ping
-sN	NULL scan	-oN	Normal output
-sO	Protocol scan	-oX	XML output
-sP	Ping scan	-T paranoid or -T0	Serial, slowest scan
-sR	RPC scan	-T sneaky or -T1	Serial, slow scan
-sS	SYN scan	-T polite or -T2	Serial, normal speed scan
-sT	TCP Connect scan	-T normal or -T3	Parallel, normal speed scan
-sW	Windows scan	-T aggressive or -T4	Parallel, fast scan
-sX	XMAS tree scan	-T Sneaky	Parallel, fastest scan

Table 4-3 nmap Switches

Intense Scan: nmap -T4 -A –v <IP Address>

Intense Scan + UDP: nmap -sS -sU -T4 -A –v <IP Address>

Intense Scan all TCP Ports: nmap -p 1-65535 -T4 -A –v <IP Address>

Intense Scan no Ping: nmap -T4 -A -v –Pn <IP Address>

Ping Scan: nmap –sn <IP Address>

Quick Scan: nmap -T4 –F <IP Address>

Quick Scan Plus: nmap -sV -T4 -O -F --version-light <IP Address>

Quick Traceroute: nmap -sn –traceroute <IP Address>

Regular Scan: nmap <IP Address>

Slow Comprehensive Scan: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script all <IP Address>

Figure 4-6
UDP segment structure

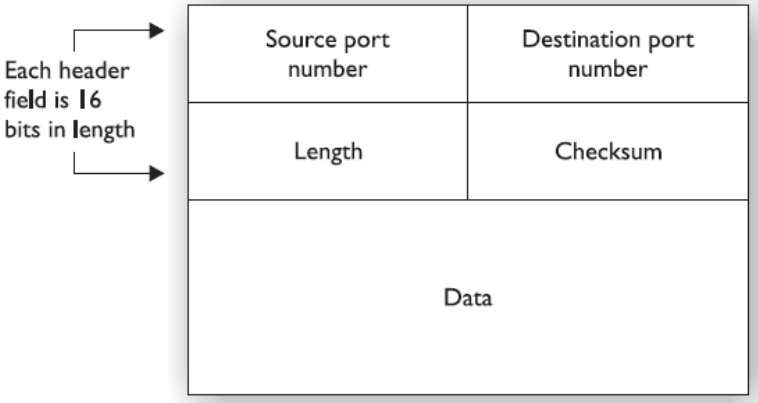
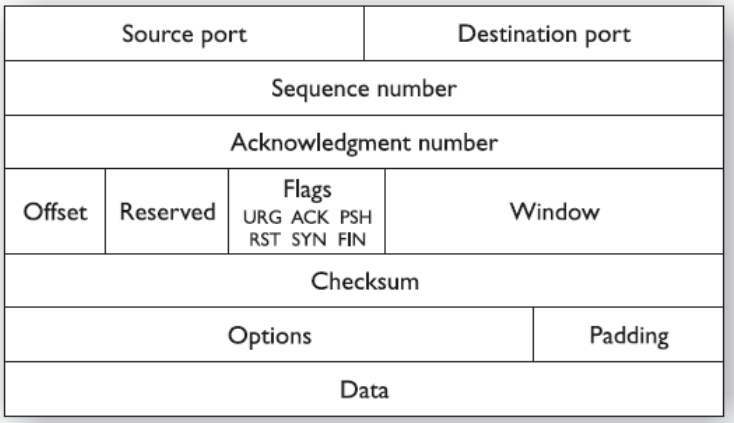


Figure 4-7
TCP segment structure



Trojan Ports

Trojan Name	**Port**
TCP Wrappers	421
Doom	666
Snipernet	667
Tini	7777
WinHole	1080–81
RAT	1095, 1097–8
SpySender	1807
Deep Throat	2140, 3150
NetBus	12345, 12346
Whack a Mole	12362, 12363
Back Orifice	31337, 31338