Algorithms			
Symmetric		Asymmetric	Hash (value output)

Hacking Steps	Pre-Attack Phase	Scanning Methodology

ICMP Message Type	Description & Codes
0:	
3:	Error message indicating the host or network cannot be reached. **Codes:** 0— 1— 6— 7— 9— 10— 13—
4:	
5	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— 1—
8:	
11:	

Well Known Ports					
Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21		TCP	110		TCP
22		TCP	135		TCP
23		TCP	137–139		TCP/UDP
25		TCP	143		TCP
53		TCP/UDP	161/162		UDP
67		UDP	389		TCP/UDP
69		UDP	443		TCP
80		TCP	445		TCP
• Well-known: 0–1023		• Registered: 1024–49151		• Dynamic: 49152–65535	

DNS RECORDS

	Defines the host name and port number of servers providing specific services. (for example: a Directory Services server)
	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.
	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.
	Defines the name servers within your namespace. These servers are the ones that respond to your clients' requests for name resolution.
	Identifies your e-mail servers within your domain.
	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.
	Maps an IP address to a host name, and is used most often for DNS lookups.

nmap Switch	Description	nmap Switch	Description
-sA		-PI	
-sF		-Po	
-sI		-PS	
-sL		-PT	
-sN		-oN	
-sO		-oX	
-sP			Serial,slowest scan
-sR			Serial,slow scan
-sS			Serial,normal speed scan
-sT			Parallel,normal speed scan
-sW			Parallel,fast scan
-sX			Parallel,fastest scan

Table 4-3 nmap Switches

Intense Scan: nmap

Intense Scan + UDP: nmap

Intense Scan all TCP Ports: nmap

Intense Scan no Ping: nmap

Ping Scan: nmap

Quick Scan: nmap

Quick Scan Plus: nmap

Quick Traceroute: nmap

Regular Scan: nmap

Slow Comprehensive Scan: nmap

Figure 4-6 UDP segment structure

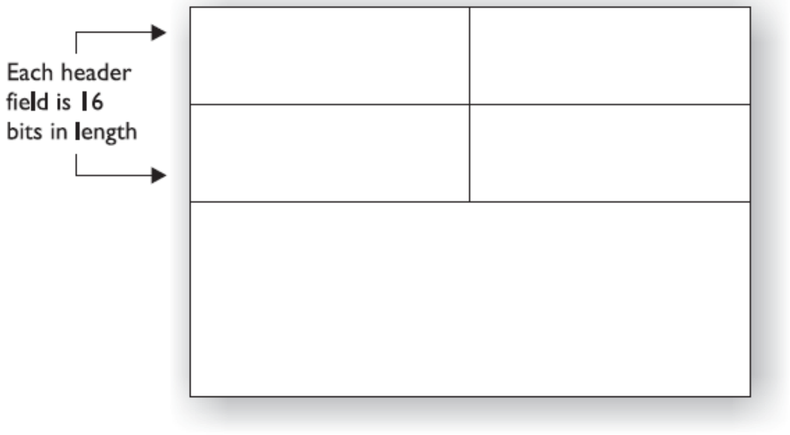
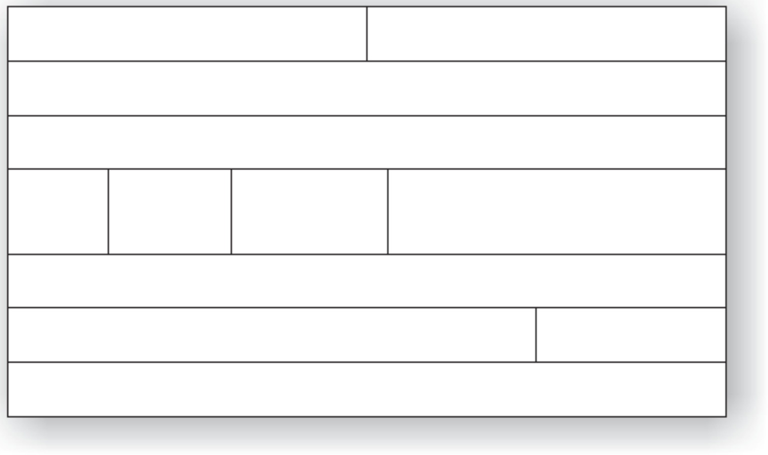


Figure 4-7 TCP segment structure



Trojan Ports

Trojan Name	Port
TCP Wrappers	
Doom	
Snipernet	
Tini	
WinHole	
RAT	
SpySender	
Deep Thr oat	
NetBus	
Whack a Mole	
Back Orifice	