Clear Text Protocols

Nic Maurel

Introduction

- Once upon a time the internet was a friendly place.
- Most communications used clear text authentication, and usernames and passwords were sent over networks with no intention to hide them.
- This is no longer appropriate!

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2005

Year	2000	2001	2002	2003	2004	1Q,2005
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	1,220

Total vulnerabilities reported (1995-1Q,2005): **17,946**

Statistics Taken from www.cert.org

What are clear text protocols?

- Clear Text Protocols are Protocols that speak in a language that is “Human readable”.

- Many companies still use these protocols today.

IP Header	Clear text Data
Source IP Destination IP Port	

Which are the clear text Protocols?

Port 20/21	FTP
Port 23	TELNET
Port 25	SMTP
Port 80	HTTP
Port 110	POP3
Port 143	IMAPv4
Port 139/445	NETBIOS
Port 161/162	SNMP
Port 1521	SQLnet

Http

- Webmail – can expose usernames, passwords and email content.
- Cookies – carry individual user information, and browsing habits. Used for shopping carts ect.
- Alternatives to HTTP is using HTTPS (SSL 3 or TLS)

SMTP, POP3 & IMAP

- Mail servers transfer email with the de facto standard protocol SMTP.
- POP3 and IMAP are uses to access email from the mail server with usernames and passwords.
- PGP and S/MIME are alternatives but not all mail servers support encryption.

Telnet & ftp

- Telnet is used for terminal sessions with servers.
- Ftp – used for upload and download of files between 2 hosts.
- The alternative is SSH & SFTP

Wireless Networks

- Clear text protocols on wireless networks, bring back a threat that was once alleviated with a choke point on wired Networks.
- What ever encryption used at this stage can be broken.
- Networks can be pin pointed with GPRS.

Threats of Clear Text Protocols

- Good password policy doesn't help.
- Same passwords for everything are a threat.
- Is it really okay to use Telnet or Ftp internally?
- ID Theft.
- Confidentiality becomes a major problem, using ftp, telnet and smtp.
- You are only as strong as your weakest link.
- Switched networks do not prevent sniffing.
- Where ever you go wireless networks can be detected.
- War driving could become a major issue.

Sniffing Tools

- How important is our personal information to us?
- There are many sniffing tools out there that are freely downloadable, and becoming easier to use eg. Ethereal, Ngrep, Ettercap, Kismet, Dsniff, Driftnet.
- The Problem arises when someone is not using them for the good of analysing a network.

Encrypting Traffic – SSL/TLS

HTTP	80	443
NNTP	119	563
FTP-data	20	989
FTP-control	21	990
Telnet	23	992
IMAP	143	993
POP3	110	995
SMTP	25	465 (revoked)

What can we do ?

- Hackers are opportunistic don't give them a "sniff"
- Security Awareness
- Start using encrypted protocols such as SSH, SFTP, HTTPS.
- Don't Use Clear Text protocols on Wireless Networks
- Encryption is good but fails without good policy.
- IP Version 6 has built in security.

- Seventh Commandment of System Administration : Thou shalt use encryption for insecure services

Thank you for listening,
Please stay for the demonstration.