CYBERSECURITY
RED TEAM, BLUE TEAM

OLLI Summer 2016

Tom Manteuffel

Slides: http://www.olligmu.org/~docstore
Plan of The Course

Week I - How did we get here?

Week II - Red Team: Hacking 101

Week III - Blue Team: Defending the home computers
Chapel Hill, 1976
Revolution #1

KIM-1 Microcontroller

Certified Brilliant Idea™

$245
Revolution #2

Computer networking
## Layered Protocols – 1970s

For a time, chaos reigned. Then a new standard appeared…

<table>
<thead>
<tr>
<th>Proprietary</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM’s SNA &amp; SDLC</td>
<td>ISO’s HDLC</td>
</tr>
<tr>
<td>DEC’s DDCMP</td>
<td>ITU’s X.25</td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
</tbody>
</table>

Certified Brilliant Idea™
TCP/IP

TCP

IP

Applications

Responsible for reliable transmission and connections

Responsible for ultra-fast routing
Each layer has its own data
Routing is thus faster…

108.17.34.12

IP Address
TCP Stack

The basic plumbing of the Internet…
Adding Applications
Adding Applications

File Transfer Protocol

FTP
TCP
IP
LINK

FTP
TCP
IP
LINK

ftp://ftp.microsoft.com
Adding Applications

The web in turn enabled the greatest application of all: the search engine.
Second Advantage of Layered Protocols

Secure Sockets Layer (SSL)

Page layout

HTTPS
TCP
IP
LINK

Page Server

HTTPS
TCP
IP
LINK

ENCRYPTED
Second Advantage of Layered Protocols

VPNs

TCP

IP

IPSEC

LINK

Encrypted IP Tunnel

TCP

IP

IPSEC

LINK
Every so often, someone will ask, who’s the idiot who designed it so the internet only has 32 bit addresses…

Yeah, that would be me…
Why Hasn’t IP Address space run out?

Because within private networks, only private addresses are used, and hence can be re-used elsewhere…

Network Address Translation

Certified Brilliant Idea™
Public Key Cryptography

Prior to 1976, all encryption was based upon using the same key to encrypt and decrypt.
With Public Key Cryptography, keys come in *pairs*, mathematically related so that if you have one, you can’t deduce the other. And *if you encrypt with one, you can only decrypt with the other*.

“Public key” known to all

“Private key” known to only one person.

Certified Brilliant Idea™
Public Key Encryption

A. Lincoln encrypts with Stanton’s Public Key

Only Stanton can decrypt, with his Private Key
Digital Signing

A. Lincoln signs with his Private Key

Anyone can verify, with Lincoln’s Public Key

Four score ...

4c10de7

Four score ...

4c10de7

Four score ...

4c10de7

Four score ...

SENDERR

RECEIVER
Public Key Cryptography

Public key cryptography is used to:

- To authenticate patches from vendors
- For SSL (but only verifies server!)
- Digitally signed PDFs
- For securing internet name servers (DNS)
- For securing remote admin access (SSH)
Wake-Up Call

On November 2, 1988, a young Cornell graduate student, Robert Tappan Morris, launched a small proof-of-concept program on an MIT computer connected to the Internet. He wanted, he said, to gauge the size of the Internet at the time, so he made it replicate itself to other machines.

The ‘Morris’ Worm
Wake-Up Call

• The computers cleaned had to be partitioned off to prevent further contamination from still-infected machines.

• Systems were still being taken down for clean-up days later.

• Possibly 6,000 computers, including some of the largest, were disabled for a time.

In response, the government established the Computer Emergency Response Team (CERT) at Carnegie-Mellon. Morris was convicted of a felony.

(He later joined the faculty at MIT.)
On the analogy with physical ports, TCP was designed to utilize up to 65000 virtual ‘ports’. Each port is a TCP connection.
First Generation Intrusion Detection

Ca. 1989

Designed to look for signs (signatures) of hostile activity and send an alarm when detected.

Has evolved in many directions

- Host-based
- Network-based
- Anomaly-based
- Antivirus
- Endpoint protection
Questions

manteuf@verizon.net