CYBERSECURITY
RED TEAM, BLUE TEAM

OLLI Summer 2016

Tom Manteuffel

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

<table>
<thead>
<tr>
<th>Week I - How did we get here?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week II - Red Team: Hacking 101</td>
</tr>
<tr>
<td>Week III - Blue Team: Defending the home computers</td>
</tr>
</tbody>
</table>
TCP Stack

The basic plumbing of the Internet…
The web in turn enabled the greatest application of all: the search engine.
The Advantage of Layered Protocols

Secure Sockets Layer (SSL)

![Diagram showing layered protocols with HTTP and HTTPS protocols, and encrypted communication between a client and server.](image-url)
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
Red Team

Hacking 101

What does it mean to be hacked?

Attacker can run arbitrary programs on your machine

Attacker can send control messages to your machine

This is not detected on your machine
Cast of Characters
File Extensions…

File name

File extension

Rocky.exe
Executable Files

- Rocky.exe
- Rocky.doc
- Rocky.pdf
- Rocky.xls
- Rocky.jpg
- Rocky.gif
 executable

Rocky.exe
Rocky.pdf

To succeed, Boris must get Rocky to open an executable file on his machine...
Door Number One…

- Email attachments

To: Rocky
From: Boris
Subject: Hello
w/attachment: Rocky.exe
Door Number Two…

Wheresoe’er there be software, there shall also be found… Bugs

Tom’s Ironclad Rule of Software
How Bad Is It?

https://nvd.nist.gov
Door Number Two (cont’d)…

Boris installs malicious exploit on Rocky’s machine via a download from a sketchy website. This exploit is based on either an unpatched or an as-yet-unpatchable [zero-day] bug in some useful software.

This is every bit as effective as getting Rocky to execute a hostile file.
Once the door is breached…

Boris must still gain **persistence** onto Rocky’s machine.

Several ways:

- Windows Registry
- Run keys, search order, etc.
- Browser Helper Objects

An active area currently…
The Better the Attacker, the Slower the Attack

The most sophisticated attacks and attackers are all ‘low-and-slow’

The most sophisticated and professional attackers are known as APTs: Advanced Persistent Threats

These operations take months or even years to set up.
Phases in a Major Attack

- **Reconnaissance**
  - Open source investigation
  - Possible Google-hacking

- **Intrusion**
  - Acquiring persistence, command-and-control
  - Privilege escalation

- **Network Discovery**
  - Scanning
  - Footprinting

- **Host Capture**
  - Data capture and encryption

- **Exfiltration**
  - Data transfer to source
Phases in a Major Attack

Reconnaissance

- Open source collection
- ‘Google hacking’

By Johnnie Long, et al

By Michael Bazzell
Phases in a Major Attack

- Reconnaissance
- Intrusion
  - Persistence
  - Command channel
  - Privilege escalation
Phases in a Major Attack

- Reconnaissance
  - Footprinting
  - Discovery scanning
- Intrusion
- Network Discovery
  - Discovery scanning
  - Footprinting
Discovery Scanning
Footprinting

Windows 10

Windows Server 2003
Phases in a Major Attack

- Reconnaissance
  - Footprinting
  - Discovery scanning
- Intrusion
- Network Discovery
  - Footprinting
Phases in a Major Attack

- **Reconnaissance**
- **Intrusion**
- **Network Discovery**
- **Host Capture**

- Privilege escalation
- Admin credentials
Phases in a Major Attack

- Reconnaissance
- Intrusion
- Network Discovery
- Host Capture
- Data Exfiltration

- Possible encryption

- Jackpot!
The OPM Breach

In June 2015, 21.5 million personnel records were reported stolen from Office of Personnel Management.

Some of it was related to clearances.

The breach began apparently in March 2014. It was first noticed in April 2015.

It is suspected that Chinese initiated the attack.
The Target Attack

Hackers initially a small heating and air conditioning firm in Pennsylvania that worked with Target and had suffered its own breach via malware delivered in an email. In that intrusion, the thieves managed to steal the virtual private network credentials that the small company technicians used to remotely connect to Target’s network.

In December 2013 the data breach exposed 40 million customer debit and credit card accounts, and offered the attackers access to every single cash register in every Target store.

Total cost to Target: $150 million.  
Plus one CEO.
Major Breaches

For an animated visualization of recent data breaches by size:

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
3 Stolen Health Databases Reportedly for Sale on Dark Web

Marianne Kolbasuk McGee • June 27, 2016

A hacker is reportedly selling on the dark web copies of databases stolen from three unidentified U.S. healthcare organizations containing data on hundreds of thousands of patients. Why are such postings becoming more common, and what can organizations do to
20 Citing Attack, GoToMyPC Resets All Passwords

GoToMyPC, a service that helps people access and control their computers remotely over the Internet, is forcing all users to change their passwords, citing a spike in attacks that target people who re-use passwords across multiple sites.

Owned by Santa Clara, Calif. based networking giant Citrix, GoToMyPC is a popular software-as-a-service product that lets users access and control their PC or Mac. 

Owned by Santa Clara, Calif. based networking giant Citrix, GoToMyPC is a popular software-as-a-service product that lets users access and control their PC or Mac.
Verizon’s Annual DBIR

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
Faster, Faster, Faster

Most compromises now take place in minutes

Most exfiltrations now take place in days
THE YEAR IN FIGURES

- In 2015, there were 1,966,324 registered notifications about attempted malware infections that aimed to steal money via online access to bank accounts.
- Ransomware programs were detected on 753,684 computers of unique users; 179,209 computers were targeted by encryption ransomware.
- Kaspersky Lab’s web antivirus detected 121,262,075 unique malicious objects: scripts, exploits, executable files, etc.
- Kaspersky Lab solutions repelled 798,113,087 attacks launched from online resources located all over the world.
- 34.2% of user computers were subjected to at least one web attack over the year.
- To carry out their attacks, cybercriminals used 6,563,145 unique hosts.
- 24% of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US.
- Kaspersky Lab’s antivirus solutions detected a total of 4,000,000 unique malicious and potentially unwanted objects.
So What Can One Do to Protect Oneself?

That’s next week…
Questions

manteuf@verizon.net