So, You Want to be a Hacker or Think like One?

For: NebraskaCert Conference

Authors: Luke Wentz
Jonathan Bender

Agenda

- Definition
- Capture the Flag frameworks
  - Remote
  - Local
- Competitions
  - Defcon
  - UCSB
  - Cipher 4
- Tools
  - Attack based
  - Defense based
- Educational Aspects

Definition

- Computer security War like game
- Each team gets a machine or small network
- Score
  - Success of defending assigned machine
  - Success of attacking other teams' machines
  - Flag
    - ECA+hWjCb8t8/FgbEg/mSm1hbU231kjg==
- Educational exercises

CTF Frameworks

- Remote
  - Normally played trough a VPN
  - 10 to 30 teams participate
  - Teams are 5 to 20 players per team
- Local
  - Co-located
  - 5 to 10 teams
  - 5 to 10 players per team

Competitions

- DEF CON
  - Held yearly at the DEF CON conference
  - Local
  - 7-8 teams
- UCSB
  - Remote
  - 5 international competitions
  - 30 teams per year
  - Based on DEF CON

Competitions[1]

- Cipher4
  - ***C**hallenges in **I**nformatics: **P**atching, **H**acking and **E**xploiting, a**R**rrrgh*
  - University Siegen & RWTH Aachen University.
  - 4th year
  - Remote

Tools

- Attack based
  - WireShark
  - Paros, Burp / Proxies
  - Reverse engineering programs
  - Nemesis
- Defense based
  - WireShark
  - TCP Wrapper
  - Firewalls

WireShark^2

- Packet Capture
- Sort Packets
  - Capture number
  - IP address
  - Traffic type

WireShark

- Filter Packets
  - Capture filters
    - Source / Destination Port Number
    - Traffic type
    - Source / Destination IP address
  - Display filters
    - Source / Destination Port Number
    - Traffic type
    - Source / Destination IP address

Paros[3], Burp[4]

- Proxy Server
- Evaluate web site security
- Intercepts all web traffic
  - Modify Requests, Response
    - Cookies
    - Fields

Reverse engineering programs

- Converts binaries to source code
- Helps debug programs
- Helps to find and exploit errors

TCP Wrapper[5]

- IP packet filtering tool
- Finer grain of filtering the iptables

Firewalls[6]

- Block Packets based on:
  - Single IP address
  - Range of IP addresses
  - Port Number
  - Packet Content
  - Packet Status
    - Related
    - New
    - Established

Educational Aspects

- Test Defensive techniques
- Learn and test offensive techniques
- Test web applications

Sources

1. http://www.cipher-ctf.org/cipher4.php?edit=0&include=cipher4.php
2. http://www.wireshark.org/
3. http://www.parosproxy.org/index.shtml
4. http://portswigger.net/proxy/
5. http://itso.iu.edu/TCP_Wrappers
6. http://www.netfilter.org/projects/iptables/index.html

Contact Information

- Luke Wentz
  - lwentz@nucia.unomaha.edu
- Jonathan Bender
  - jbender@nucia.unomaha.edu