Lec08: Remote Exploit

Taesoo Kim
Scoreboard
## NSA Codebreaker Challenges

<table>
<thead>
<tr>
<th>University</th>
<th>Task 0</th>
<th>Task 1</th>
<th>Task 2</th>
<th>Task 3</th>
<th>Task 4</th>
<th>Task 5</th>
<th>Task 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carnegie Mellon University</td>
<td>11</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Lafayette College</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Georgia Institute of Technology</td>
<td>29</td>
<td>18</td>
<td>15</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>University of Hawaii</td>
<td>20</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>University of Tulsa</td>
<td>14</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Pennsylvania State University</td>
<td>46</td>
<td>12</td>
<td>11</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Virginia Community College System</td>
<td>12</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Lesley University</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>University of Memphis</td>
<td>11</td>
<td>7</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Texas A&amp;M University - College Station</td>
<td>27</td>
<td>13</td>
<td>11</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Administrivia

- Hacking day on Oct 27 (No class)!
- If you are interested in, check out CTF Events
- One local CTF game (on 11/04/2017): Hungry Hungry Hackers 2017
- Due: Lab08 is out and its due on Nov 2 (two weeks!)
- NSA Codebreaker Challenge → Due: Nov 30
## Lab06: ROP

<table>
<thead>
<tr>
<th>Name</th>
<th>Points</th>
<th>Release</th>
<th>Deadline</th>
<th>Solved</th>
</tr>
</thead>
<tbody>
<tr>
<td>rop-basic</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>21</td>
</tr>
<tr>
<td>rop-64</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>21</td>
</tr>
<tr>
<td>pop</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>21</td>
</tr>
<tr>
<td>puzzle</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>21</td>
</tr>
<tr>
<td>upto-retaddr</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>21</td>
</tr>
<tr>
<td>find-gadget</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>20</td>
</tr>
<tr>
<td>sprintf</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>18</td>
</tr>
<tr>
<td>rop-sorting</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>20</td>
</tr>
<tr>
<td>inc1</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>18</td>
</tr>
<tr>
<td>fmtstr-retro</td>
<td>20</td>
<td>10-06-2017 00:00:00</td>
<td>10-20-2017 00:00:00</td>
<td>10</td>
</tr>
</tbody>
</table>
Best Write-ups for Lab06

- rop-basic: poning, carterchen
- rop-64: nagendra, carterchen
- pop: myao42, jallen309
- puzzle: nagendra, shudak3
- upto-retaddr: poning, dhaval
- find-gadget: N/A, N/A
- sprintf: markwis, jallen309
- rop-sorting: poning, brian_edmonds
- inc1: nagendra, carterchen
- fmtstr-relro: whuang328, jallen309
Discussion: Lab07

- What's the most "difficult" bug or challenge?
- What's the most "interesting" bug or challenge?
- So, ROP is too powerful?
Discussion: pop

- What was the challenging part?
- How did you solve?
Discussion: pop
Discussion: puzzle

• What was the problem?
• How did you solve?
Discussion: puzzle

• PALLET = "ALPHABETS : ABCDEFGHIJKLMNOPQRSTUVWXYZ_"
• → "ROP_ATTACK_SUCCESS"
Discussion: upto-retaddr

- What was the problem?
- How did you solve?
Discussion: upto-retaddr

- Stack pivoting
Discussion: find-gadget

- What was the problem?
- How did you solve?
Discussion: find-gadget
Discussion: sprintf

• How much did you try?
• Where did you stuck?
Discussion: sprintf
Discussion: sprintf
Discussion: rop-sorting

- How much did you try?
- Where did you stuck?
Discussion: inc1

- How much did you try?
- Where did you stuck?
Discussion: inc1
Discussion: fmtstr-retro

• What's special about this problem?
Discussion: fmtstr-relro

• RELRO: not able to overwrite got, but
  • atexit(), seen in previous lab?
  • real world: a bit complex
Discussion: fmtstr-relro
Discussion: fmtstr-relro

- PTR_MANGLE(func)?
Take-outs from ROP

- DEP/ASLR are not perfect solutions (pretty good mitigation?)
  - DEP: ret-to-lib, ROP
  - ASLR: code leakage
- What about stack canary? (what if we placed it together?)
- Lots of known defenses (e.g., CFI)
Today's Tutorial

• In-class tutorial:
  • Socket programming in Python
  • Your first remote exploit!
Remote Challenges

• Use techniques learned from Lab01-Lab07
• But targeting the remote server (e.g., online services)!
# Lab08: Remote Challenges

<table>
<thead>
<tr>
<th>Name</th>
<th>Points</th>
<th>Release</th>
<th>Deadline</th>
<th>Solved</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwd</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>2</td>
</tr>
<tr>
<td>mini-shellshock</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>2</td>
</tr>
<tr>
<td>obscure</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>1</td>
</tr>
<tr>
<td>diehard</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>2</td>
</tr>
<tr>
<td>array</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>2</td>
</tr>
<tr>
<td>fmtstr-heap2</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>1</td>
</tr>
<tr>
<td>memo</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>1</td>
</tr>
<tr>
<td>2kills</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>1</td>
</tr>
<tr>
<td>return-to-dl</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>1</td>
</tr>
<tr>
<td>2048_game</td>
<td>20</td>
<td>10-20-2017 00:00:00</td>
<td>11-03-2017 00:00:00</td>
<td>0</td>
</tr>
</tbody>
</table>
DEMO: about how remote challenges work

- nc
- exploit.py
In-class Tutorial

- Step1: nc
- Step2: brute force attack
- Step3: guessing attack

```bash
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2023
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2022
$ ssh YOURID@computron.gtisc.gatech.edu -p 2023
$ ssh YOURID@computron.gtisc.gatech.edu -p 2022

$ cd tut/lab08
$ cat README
```