CSEC-S

Introduction

Introduction

- Welcome to CSEC-S premiere meetup
- Space for practice, learning and relaxation
  - Every Friday 6 – 8pm unless otherwise notified by email or slack
  - Room: Announced weekly
  - Very technical and hands-on
  - Slides may be posted for reference
  - Screen recording may be available for reference
- 2017 Winter Syllabus
  - Focuses on learning Linux and Windows environment and C/Python programming
- Resources:
  - Required Books
    - Hacking; The art of exploitation [2nd Ed. Jon Erickson]
  - Recommended Books
    - C programming; A Modern approach [C.N.King]
  - Online resources
    - LiveOverflow www.liveoverflow.com etc.
- Challenge sites
  - OverTheWire www.overthewire.org
  - Exploit-Exercises www.exploit-exercises.com
  - Pwnable.kr etc.
- Record Keeping

  We encourage friendly competition. It forces us to find time to grow and learn personally.

  This will also allow us to form groups and distribute attention effectively.
  - WeChall www.wechall.net
  - OTW & wechall: overthewire.org/about/wechall.html
- Club forum
  - Slack channel: csec-s.slack.com.
  - Don't have an account? Request one by mailing Richard: richardmc.song – at – mail.utoronto.ca Kc: kc.udonsi – at – mail.utoronto.ca You'll also be added to the mailing list.
- Contact Us
  - Feel free to message I or Richard directly on slack.
  - Or via email. See above.
  - Actually, please use slack.

Setup & installations

OS: Windows

- Required Installations:
  - VMWare/VirtualBox/Vagrant
    - Demo installation of VirtualBox
  - Putty/OpenSSH for windows
- Required Downloads:
  - Ubuntu https://www.ubuntu.com/download/desktop
  - Python https://www.python.org/ftp/python/2.7.13/python-2.7.13.amd64.msi

C Programming

- The C programming language
- Allows low level manipulations of memory
- Programmers are responsible for memory management and type checking
- Must be used with caution
- Understanding the language is crucial before utilizing it. Careless use could result in vulnerabilities and undefined behaviour
- Every program in C has an entry point (function) called ‘main’
- Compile with: gcc –Wall –g <source> -o <executable>
- Resources:
  - Book: C programming; A modern approach C.N.King
  - Book: Hacking; the Art of Exploitation J.Erickson
  - Online environment: https://www.tutorialspoint.com/compile_c_online.php

- To understand how to write C programs (properly), we start by dissecting simple programs.
- Below is a basic C program utilizing control structures such as if-else, while/for loops and arithmetic operations.

```
# include <stdio.h>
int main (int argc, char * argv[]) {
  int i;
  for (i=0; i<argc; i++) {
    if (i % 2 == 0) {
      printf("arg %s is at even index\n", argv[i]);
    } else {
      printf("The %d argument is %s\n", i, argv[i]);
    }
  }
  return 0;
}
```

Python Programming & Bash scripting

- Python programming
- Python version 2.7/3.6
- Python for scripting
  - Quick networking tools
  - Exploit development etc.
- Resources
  - https://docs.python.org/2/library
- Bash scripting
  - Shell types: sh, bash, and ksh
- Resources
  - Book: Mastering UNIX Shell scripting 2ed R.K.Michael
  - Online: www.freeos.com/guides/lsst/
    etc.

```
#!/usr/bin/python
import socket as s
import sys
sock = s.socket(s.AF_INET, s.SOCK_STREAM, 0)

if len(sys.argv) == 3:
  host = sys.argv[1]
  port = sys.argv[2]

  sock.connect((host, int(port)))
  print sock.recv(1024)
else:
  print "Usage: ./client.py <host-name>
<port>"
sock.close()
exit(0)
```

Navigating the Linux File System 101

Man(ual) page is your best friend!

Remote connections: ssh, scp, telnet, nc

Playgorund: /tmp

Way-around-commands: ls, cd, cat, file, du, find

Interpreting `ls -lha` output:

```
total 80K
drwx------ 2 root root    0 Dec 31  1969 .
drwxr-xr-x 2 root root    0 Dec 31  1969 ..
-rw------- 1 root root 8.5K Feb 28 21:53 .bash_history
```

9 permission bits: divided into sections: user, group and other. 3 bits each from left to right read (r), write (w), execute (x) 1 leftmost bit: indicates if this entry is dir, symlink or file.

Files prefixed with a period indicate the file is hidden. “.” “..” mean current and parent directory respectively.

After the bits we have number of links (to be discussed later)

Followed by owner name, group name, size, last modified and name

Overthewire.org challenges 1 – 5 Notes: