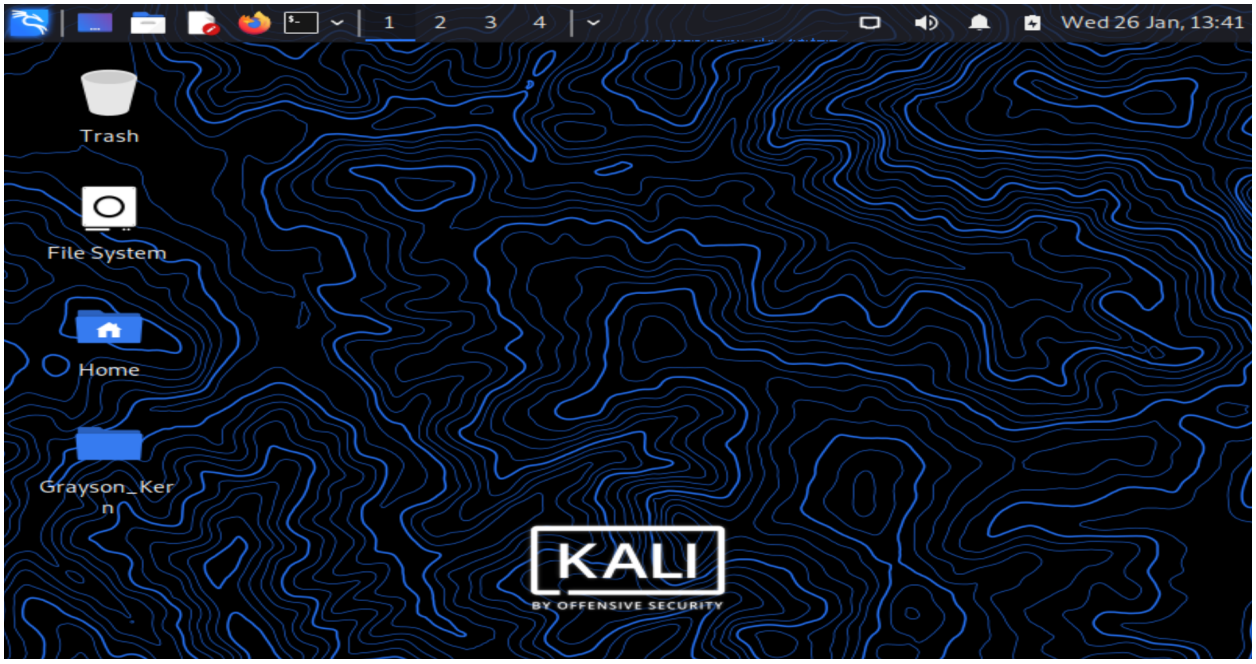
Lab 1: Introduction to Ethical Hacking

The art of hacking involves the exploitation of systems and their flaws. Though most commonly associated with computers, hacking can apply to all manner of machinery. Hackers themselves are divided into three camps: ethical white hat hackers, morally ambiguous gray hat hackers, and malicious black hat hackers. This course deals exclusively with white hat hacking and how it can be used for the betterment of information security.

Part 1: Installing The Virtual Machine

Virtualization technology and UNIX based operating systems have long since been mainstays of the ethical hacking trade. Together, they afford hackers a safe, and highly versatile environment to practice their craft. Though many virtualization platforms and Linux distributions exist, this course makes use of Oracle VM VirtualBox and a 64 bit Kali Linux virtual machine. The desktop of which is shown below.

Figure 1: VM Desktop

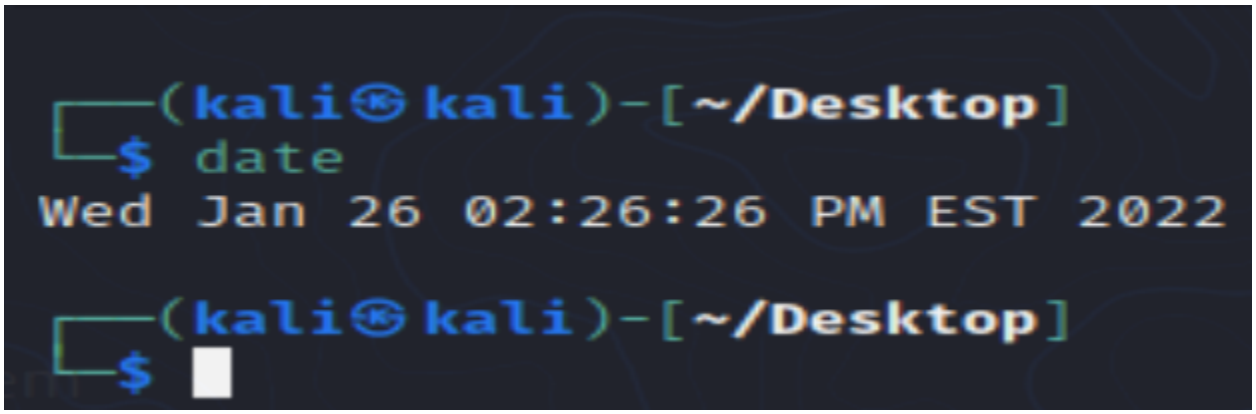


Part 2: Practicing Common Commands

The UNIX command line or shell is an extremely powerful program that provides access to a seemingly infinite array of system level functionalities. Any ethical hacker worth his or her salt should be intimately familiar with it. To this end, screenshots of 20 common commands are shown below.

Figure 2: Common Linux Commands

Print the Current Date and Time



Print the Current Year's Calendar

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cal
     January 2022
Su Mo Tu We Th Fr Sa
                   1
 2  3  4  5  6  7  8
 9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Display the Current Username

```
┌──(kali㉿kali)-[~/Desktop]
└─$ whoami
kali

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Print Working Directory

```
┌──(kali㉿kali)-[~/Desktop]
└─$ pwd
/home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$
```

List All Files and Permissions in the Current Directory

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -al
total 12
drwxr-xr-x  3 kali kali 4096 Jan 26 14:38 .
drwxr-xr-x 16 kali kali 4096 Jan 26 14:39 ..
drwxr-xr-x  2 kali kali 4096 Jan 26 14:38 Grayson_Kern

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Change Directory

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd Grayson_Kern

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Make New Directory Here

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ mkdir Lab 1

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Concatenate File(s) to Standard Output

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ cat HelloWorld.txt
Hello World
```

Copy File(s) to Target Directory

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ cp HelloWorld.txt /home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Move File(s) Between Directories

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mv HelloWorld.txt /home/kali/Desktop/Grayson_Kern

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Remove File From Directory

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ rm HelloWorld.txt

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Print Various System Information

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ uname -a
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05) x86_6
4 GNU/Linux

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Display the Uptime of the Machine

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ uptime
 15:08:09 up 47 min,  1 user,  load average: 0.17, 0.20, 0.15

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Display a List of Users

```
┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$ users
kali

┌──(kali㉿kali)-[~/Desktop/Grayson_Kern]
└─$
```

Show Output One Screen at a Time

```
8.0K    ./.config/qt5ct
8.0K    ./.config/dconf
8.0K    ./.config/powershell
8.0K    ./.config/gtk-3.0
84K     ./.config/pulse
8.0K    ./.config/qterminal.org
8.0K    ./.config/xfce4/desktop
4.0K    ./.config/xfce4/xfwm4
16K     ./.config/xfce4/panel/launcher-7
8.0K    ./.config/xfce4/panel/launcher-5
8.0K    ./.config/xfce4/panel/launcher-6
48K     ./.config/xfce4/panel
68K     ./.config/xfce4/xfconf/xfce-perchannel-xml
72K     ./.config/xfce4/xfconf
136K    ./.config/xfce4
272K    ./.config
4.0K    ./Documents
4.0K    ./Pictures
4.0K    ./Downloads
8.0K    ./.cache/sessions/thumbs-kali:0
12K     ./.cache/sessions
4.0K    ./.cache/mozilla/firefox/zoeo8y9x.default
260K    ./.cache/mozilla/firefox/veckhj92.default-esr/OfflineCache
4.0K    ./.cache/mozilla/firefox/veckhj92.default-esr/cache2/doomed
12M     ./.cache/mozilla/firefox/veckhj92.default-esr/cache2/entries
12M     ./.cache/mozilla/firefox/veckhj92.default-esr/cache2
--More--
```

Sort File(s)

```
┌──(kali㉿kali)-[~]
└─$ sort -n text.txt
a
b
c
1
2
3
```

Vi Text Editor

```
Hello World
~
~
~
~
~
```

Display Free Memory

```
┌──(kali㉿kali)-[~]
└─$ free
              total        used        free      shared  buff/cache   availa
ble
Mem:        2029520      782920      684820       23208      561780     1076
680
Swap:        998396           0      998396
```

Display Command History

```
 132   free -g
 133   free -m
 134   clear

┌──(kali㉿kali)-[~]
└─$
```

Part 3: Determining the Corporate Need for Security Professionals

Nearly every sector of the modern economy relies on computing technology in some way shape or form, opening a world of possibilities for cyber attacks. As such, qualified penetration testers and security professionals are highly sought after by many companies. A sampling of information security related job offerings from monster.com is shown below.

Figure 3: Information Security Jobs In The Chicago Area

Salesforce Administrator

Ace Hardware

Oak Brook, IL

Network Engineer

Alexander Technology Group

Schaumburg, IL

Cyber Security

Creative Financial Staffing

Chicago, IL

Network Specialist
Village of Oak Park
OAK PARK, IL

Part 4: Top 25 Most Dangerous Software Flaws

Software vulnerabilities, especially those at the system level, are often used by black hat hackers as avenues of attack. Sans.org maintains a list of the 25 most prominent exploits along with a wealth of information on each one.

Figure 4: CWE Top 25 Exploits

The CWE Top 25

Rank	ID	Name
1	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3	CWE-20	Improper Input Validation
4	CWE-200	Information Exposure
5	CWE-125	Out-of-bounds Read
6	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
7	CWE-416	Use After Free
8	CWE-190	Integer Overflow or Wraparound
9	CWE-352	Cross-Site Request Forgery (CSRF)
10	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
11	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
12	CWE-787	Out-of-bounds Write
13	CWE-287	Improper Authentication
14	CWE-476	NULL Pointer Dereference
15	CWE-732	Incorrect Permission Assignment for Critical Resource
16	CWE-434	Unrestricted Upload of File with Dangerous Type
17	CWE-611	Improper Restriction of XML External Entity Reference
18	CWE-94	Improper Control of Generation of Code ('Code Injection')
19	CWE-798	Use of Hard-coded Credentials
20	CWE-400	Uncontrolled Resource Consumption
21	CWE-772	Missing Release of Resource after Effective Lifetime
22	CWE-426	Untrusted Search Path
23	CWE-502	Deserialization of Untrusted Data
24	CWE-269	Improper Privilege Management
25	CWE-295	Improper Certificate Validation

CWE-125: Out-of-bounds Read

Weakness ID: 125 **Status:** Draft
Abstraction: Base
Structure: Simple

Presentation Filter: Complete

Description

The software reads data past the end, or before the beginning, of the intended buffer.

Extended Description

Typically, this can allow attackers to read sensitive information from other memory locations or cause a crash. A crash can occur when the code reads a variable amount of data and assumes that a sentinel exists to stop the read operation, such as a NUL in a string. The expected sentinel might not be located in the out-of-bounds memory, causing excessive data to be read, leading to a segmentation fault or a buffer overflow. The software may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent read operation then produces undefined or unexpected results.

This particular vulnerability exists primarily within programs written in low level programming languages with direct access to memory. Namely C, and C++. It occurs when software reads data from before or beyond the intended buffer, usually due to boolean logic or pointer arithmetic errors. Often this will simply cause the program to terminate with a segmentation fault, but will sometimes read from sensitive or reserved memory addresses. Attackers can therefore exploit this vulnerability to bypass ASLR, and view the memory address of system level executables.

Part 5: Local Cyber Crime Laws

Laws pertaining to cyber crime vary widely between States and are all relatively novel. Ethical hackers and penetration testers should be aware of their State's legal statutes to avoid running afoul of the law. One such statue from the State of Illinois is shown below.

Figure 5: Illinois State Computer Fraud Laws

CRIMINAL OFFENSES
(720 ILCS 5/) Criminal Code of 2012.

(720 ILCS 5/Art. 17, Subdiv. 30 heading)
SUBDIVISION 30. COMPUTER FRAUD
(Source: P.A. 96-1551, eff. 7-1-11.)

(720 ILCS 5/17-50) (was 720 ILCS 5/16D-5 and 5/16D-6)
Sec. 17-50. Computer fraud.

(a) A person commits computer fraud when he or she knowingly:

(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data, with the intent of devising or executing any scheme or artifice to defraud, or as part of a deception;

(2) Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme or artifice to defraud, or as part of a deception; or

(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection with any scheme or artifice to defraud, or as part of a deception.

(b) Sentence.

(1) A violation of subdivision (a)(1) of this Section is a Class 4 felony.

(2) A violation of subdivision (a)(2) of this Section is a Class 3 felony.

(3) A violation of subdivision (a)(3) of this Section:

(i) is a Class 4 felony if the value of the money, property, or services is $1,000 or less; or

(ii) is a Class 3 felony if the value of the money, property, or services is more than $1,000 but less than $50,000; or

(iii) is a Class 2 felony if the value of the money, property, or services is $50,000 or more.

(c) Forfeiture of property. Any person who commits computer fraud as set forth in subsection (a) is subject to the property forfeiture provisions set forth in Article 124B of the Code of Criminal Procedure of 1963.
(Source: P.A. 96-712, eff. 1-1-10; 96-1551, eff. 7-1-11.)