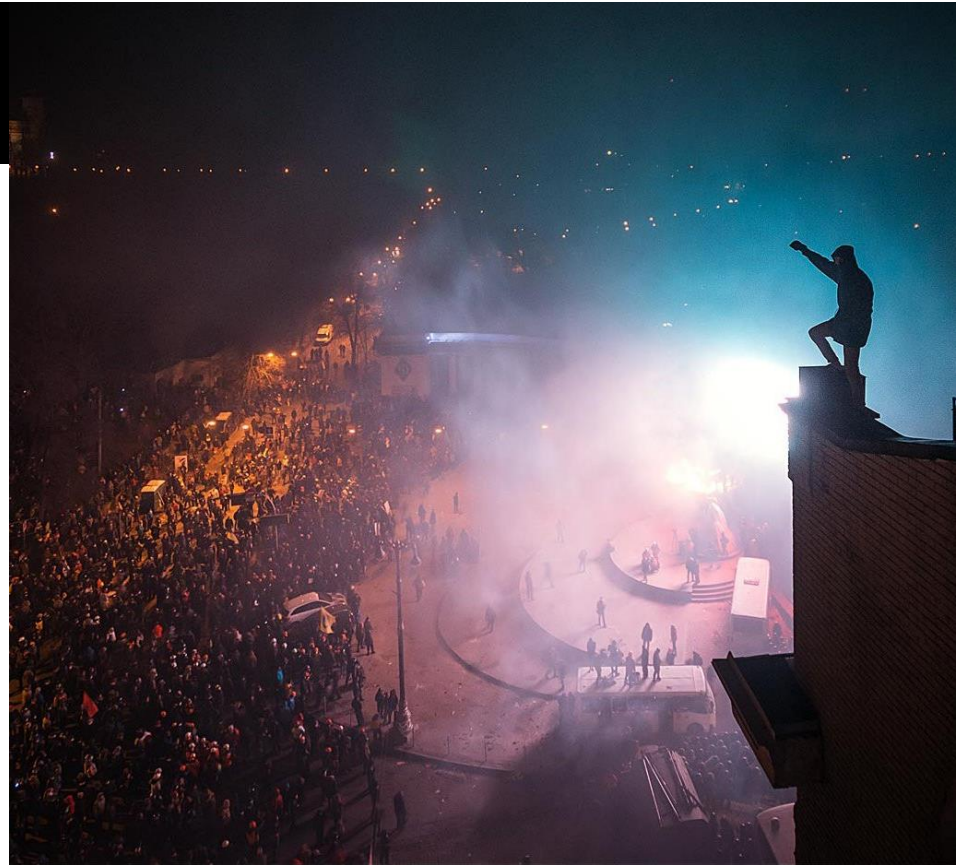


INFO-6065

*Ethical Hacking
& Exploits*

Course Introduction



Agenda

- Review Contact Information
- Online Content
- Test / Exam Information
- Lab Information
- Topics Covered and Tools Used
- Content
- Introduction to the tools we will be using
 - Talk about setting up your Kali VM
 - This is the primary focus for this week's lab

Contact Information

Email

- Use my FOL email address
- a_mackiewicz2@fanshaweonline.ca

Email sent Monday to Friday

- You can expect a turnaround of 24-48 hours or less

Email sent on the Weekend

- I usually check my email Sunday evening or first thing Monday morning

Email

Email Tips

- Use a relevant Subject
- Include the course number in the subject
- 6065 Question about test
- Keep it brief and to the point
- Don't be afraid to use point form
- Try not to wait until the last minute to send your email

General Information

- The course is a 4-credit course and is assigned 4 hours per week
- A lab session will follow the weekly lecture, unless you have a scheduled test that week
 - There are no labs on the weeks in which you have a theory test
- The labs will develop essential skills and reinforce the lecture content

Evaluation

Tests and Exams: (70%)

- Students need to write their exams in accordance with any protocols posted on FOL

Labs (30%)

- Labs will be posted on FOL on a weekly basis
- Students have until 11:59 p.m. the night before the next lab assignment is posted to complete and submit their current lab

Typical Test Information

Tests will mainly consist of one or more of the following formats:

- Multiple Choice
- True False
- Ordering
- Matching
- Written answer

Topics

- Configure Windows and Linux VMs
- Perform scans with various tools
- Investigate the tools available in Kali and Metasploit
- Vulnerabilities, Weaknesses and Exploits
- Understanding them
- Finding them
- Exploiting them

Topics

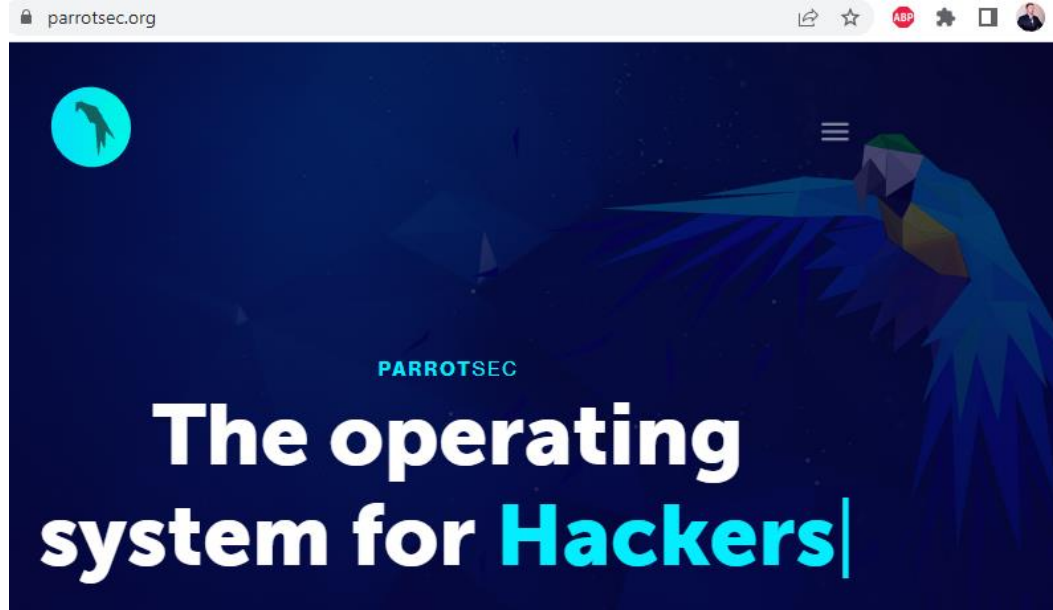
- Exploit Automation
- How hackers cover their tracks
- How hackers maintain access
- Investigate wireless vulnerabilities & exploits
- Investigate mobile vulnerabilities & exploits

Pentest Distros

Parrot

Parrot O/S

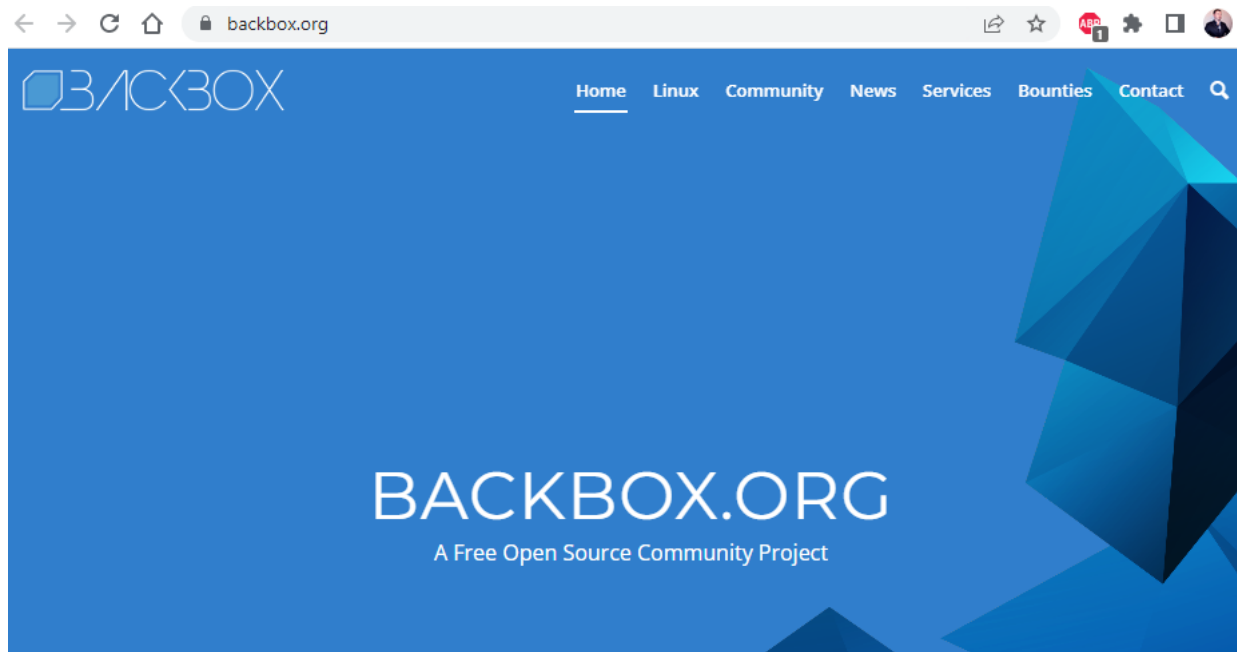
- Linux distro based on Debian
- The Parrot team is comprised of independent developers



Backbox

BackBox

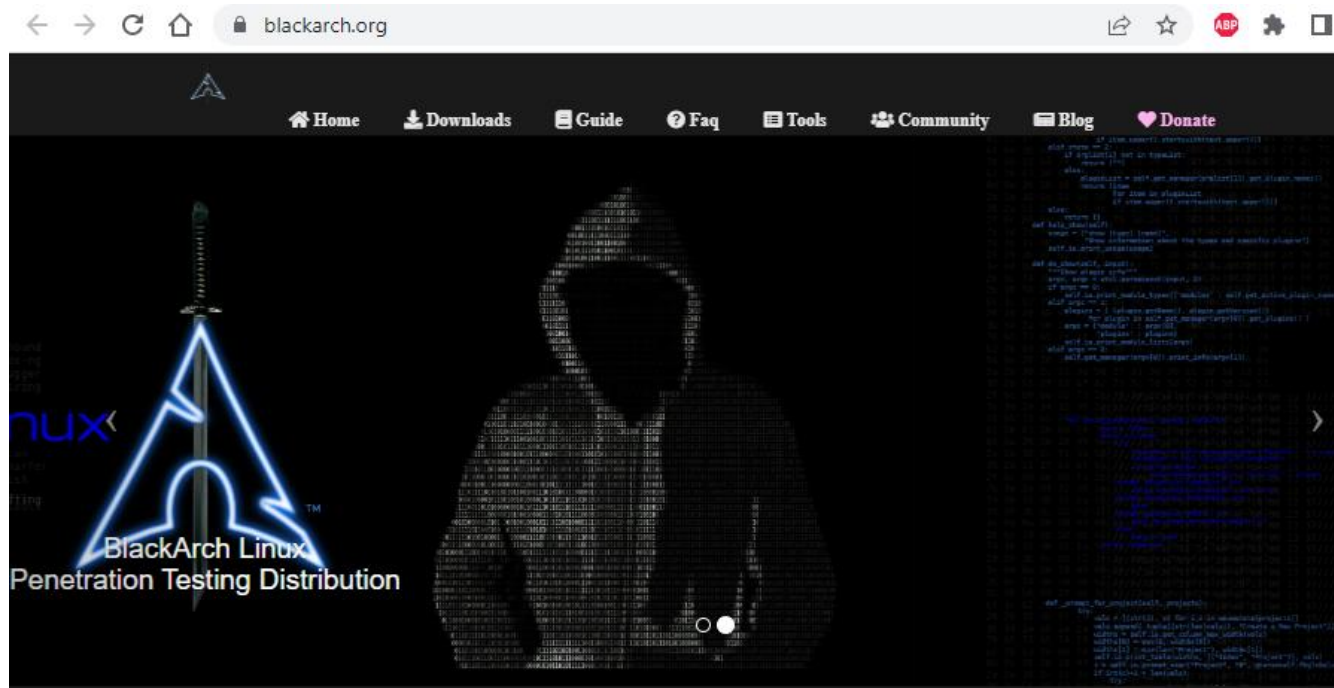
- Based on Ubuntu LTS
- Great for forensics



BlackArch

BlackArch

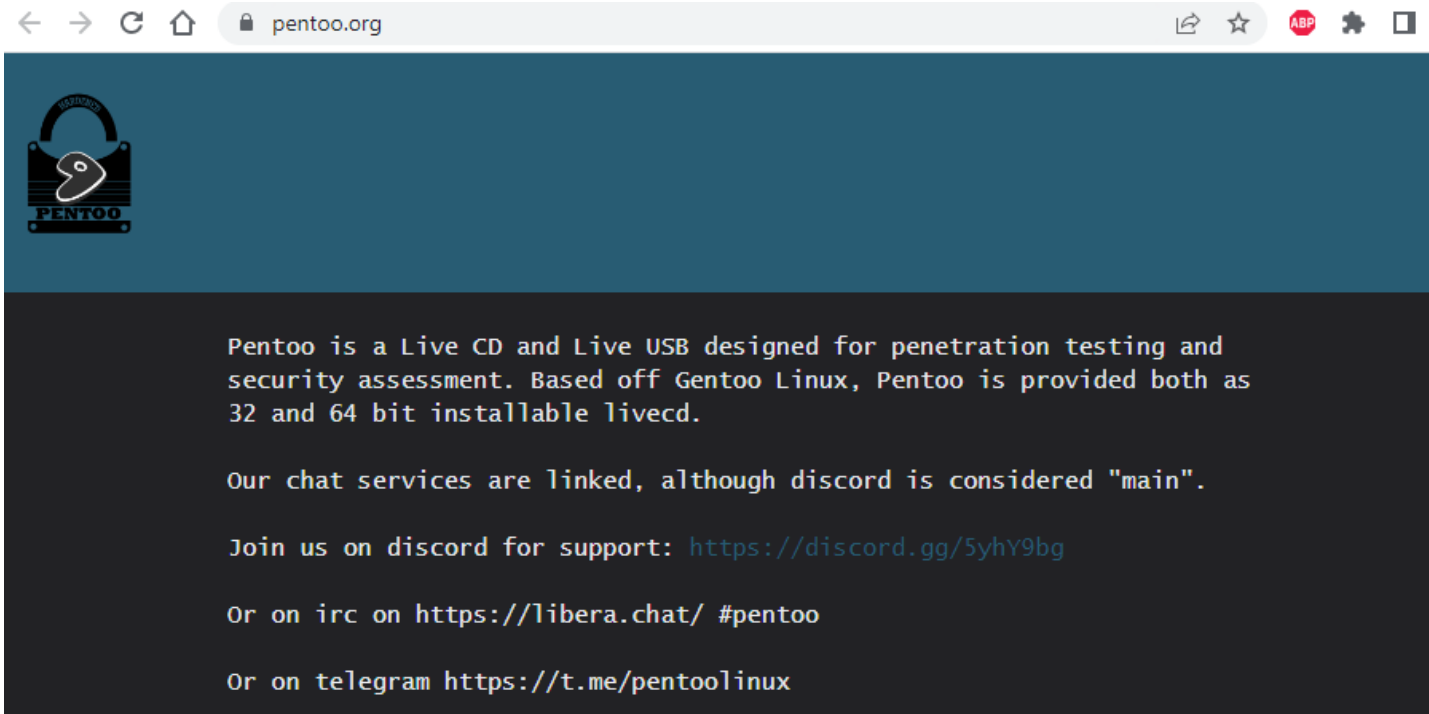
- Based on Arch Linux
- Full ISO contains over 2800 tools (22 GB in size)



Pentoo

Pentoo

- Based on Gentoo Linux
- Uses a custom Kernel



BackTrack and Kali Linux

BackTrack

- Project was funded by Offensive Security
- Extremely versatile security distribution
- Last version was BackTrack 5

Kali

- Kali Linux, also developed by Offensive Security, has replaced BackTrack
- Both Kali and BackTrack are Open Source
- Although they are both targeted at security professionals, these tools are used by black hat hackers as well

Kali Linux

Kali Versions

- Support for 32 bit, 32 bit PAE, 64 bit and ARM architectures
- Support for a wide variety of desktop environments
- GNOME, KDE, LXDE, XFCE, I3WM, MATE, etc
- Personal preference
- We are using the GNOME version
- Versions like LXDE are designed to use fewer resources
- Lightweight X11 Desktop Environment
- Useful for installing on low power devices

Kali Linux

Kali Versions

- 2023.1 also has a “Purple” version for blue teams
- Contains over 600 tools
- Can be set up as lightweight without the desktop (using SSH access)
- Recommended to have 8GB of RAM

Kali Linux

Kali Features

- Information Gathering
- Vulnerability Analysis
- Web Application Attacks
- Exploitation Tools
- Sniffing and Spoofing
- Maintaining Access
- Stress Testing
- Privilege Escalation
- Forensics

Wide Variety of Tools

Kali Tools

Well over 600 individual tools

- We will only be able to touch a fraction of them in this course
- We will use some of these tools in later labs
- There is a wide variety of online tutorials for Kali Linux

Feel free to explore the many tools available in Kali

- Just take snapshots if you are modifying your configurations

To install all packages in Kali Linux use: **apt-get install kali-linux-all**

For more info see: <https://www.kali.org/blog/kali-linux-metapackages/>

Metasploit

Metasploit Basics

- HD Moore created the Metasploit Project in 2003
- This led to the development of the Metasploit Framework
- Framework for writing security tools and exploits
- Project was taken over in 2009 by Rapid7
- Open Source

Metasploit

Rapid7 has continued to develop the project

- They have committed to keeping an open source version

There are now free and paid versions

- Metasploit Pro
- Metasploit Framework
 - This is the one we will be using

Metasploit

RAPID7


PRODUCTS ▾

SERVICES ▾

SUPPORT & RESOURCES ▾

COMPANY ▾

RESEARCH

EN ▾  SIGN IN

Metasploit Pen Testing Tool



TRY NOW

Choose the edition that's right for you

Metasploit Pro, recommended for penetration testers and IT security teams, offers a comprehensive set of advanced features. If you're simply looking for a basic command-line interface and manual exploitation, check out Metasploit Framework. Scroll down for a full feature comparison.

Recommended

Pro

For penetration testers and IT
security teams

CONTACT SALES

Buy Now

Compare Features

Framework

For developers and security
researchers

FREE DOWNLOAD

Compare Features

Alternatives

Metasploit is arguably the most popular pen-test framework, however there are other options

- PTF (The PenTesters Framework)
- Exploit Pack
- Social-Engineer Toolkit
- OWTF (Offensive Web Testing Framework)
- RouterSploit

Nmap & Zenmap

- Network Mapper
- nmap is run from the command line
- Zenmap is a GUI version of nmap

Features:

- Host discovery
- Port Scanning and version detection
- OS detection

Autoscan

Network discovery tool

- Provides you with a list of connected equipment

Requires very little configuration

- You basically need to point it at your network

Features:

- Multithreaded Scanning
- Automatic Network Discovery
- Much more

Wireshark

- Graphical network protocol analyzer
 - If you want a GUI, this is your choice
- Originally name Ethereal
- Similar functionality to the command line tool tcpdump
- You can filter the live view of the data to see just what you want
 - Allows you to filter for specific frames that are required to crack protocols like WPA2 (EAPoL)

Maltego

- Forensics and data mining application
- Queries public data sources
- Graphically presents relationships between:
 - People
 - Companies
 - Websites
 - Etc.

Nessus

Vulnerability Scanning Tool from Tenable

- Free for personal use in a non-enterprise environment

Features:

- Vulnerability Scans
- Finding Identifying Misconfigurations
- Looking for Default Passwords
- Much More

OpenVAS

- Open Source Vulnerability Scanner
- We will use this tool instead of Nessus
- Similar features to Nessus
- Forked from the last truly free version of Nessus in 2005
 - Feeds are free
 - Over 100,000 network vulnerability tests
 - Each feeds look for a specific vulnerability

NetCat

- Swiss-Army Knife Utility for TCP/IP
- Designed to read and write data across TCP and UDP connections
- Works as a standalone tool and as a back-end tool for other programs
- You may need to shut down your AV to use it
- We will also use Ncat, a revision of netcat that adds more functionality
 - Developed by the same people who created nmap

Password Cracking

CeWL

- Gathers keywords for an URL
- Keywords can be used by password crackers

PWDump

- Hash dumping
- Offline attacks

John the Ripper

- Combination of a few different password crackers
- Works with a wide variety of hashes

Hydra

- Online password attacks

Images and VMs

We will be using a variety of images in this course

- Turn off automatic updates, so you are using the same software version (same patch / upgrade level)

Exploits are very sensitive to a variety of factors

- OS Version
- Service Pack
- Updates and Patches

Warning

- This course is **NOT** designed to teach you how to be a hacker
- You are **NOT** allowed to use the tools and techniques we will be covering outside of the isolated lab environment
- Use of these tools on the rest of the College's network would constitute an **Academic Offence**
- The College has full packet capture capabilities to track down illegal activity

So Why Use These Tools?

- Understand the tools used by attackers
- Learn what attacks look like
- Learn how test your own networks
- Understand the risks that come with running these tools
- You need to understand the techniques hackers will be using if you want to implement an effective approach to defense

Lab 01: Details

Lab 01 Details

- Login and Confirm Basic Functionality
- Confirm Network Setup
- Confirm VMware Setup
- Confirm DHCP Functionality
- Change hostname
- Navigate Menus
- Regenerate SSH Keys
- Basic Configuration

Lab Commands

Apt Commands

Note: Only run these when asked

The first time you run the updates it will take a while

apt-get update

- Updates packages listings from the repo, should be run at least once a week

apt-get upgrade

- Upgrades all currently installed packages with those updates available from the repo. should be run once a week

You may need to turn off your Anti Virus

Apt Commands

apt-cache search <pattern>

- Searches packages and descriptions for <pattern>

apt-get install <package>

- Downloads <package> and all its dependencies, and installs or upgrades them

Software Update

- GUI tool to update your distribution
- This tool catches some of the upgrades that don't work properly with apt-get upgrade

Terminal commands

locate

- The locate command can be used to find files
- *locate hosts*

updatedb

- Updates the database of files on the system

grep

- grep can be used to parse the output of another command
- *locate hosts | grep etc*
- This would locate all the files named “hosts”, where “etc” is in the directory path

Lab Expectations

Submission guidelines:

- Submit your work prior to the posted deadline on FOL
- *Verify your submission!*
- *Number your slides*
- *Ensure that your submission is in .pptx format*
- *Ensure that you include all requested information in your screenshots*

Work submitted has to be yours!

Wrapping up...

- Questions...?