



INTRO TO PEN TESTING AND KALI LINUX

Presenter Information

- ◆ William E. Bowen MSCIS, MCTS, C|EH, Security+
- ◆ E-mail: wbowen05@gmail.com
- ◆ University of Detroit Mercy Adjunct Professor
- ◆ IT Specialist for the Federal Government.
- ◆ Currently a member of the National Society of Black Engineers.



RECOMMENDED TEXT

KALI LINUX - AN ETHICAL HACKER'S
COOKBOOK: END-TO-END PENETRATION
TESTING PENETRATION TESTING
SOLUTIONS

AUTHOR: HIMANSHU SHARMA

ISBN-10: 9781787121829

ISBN-13: 978-1787121829



WHAT IS PEN TESTING?

- **Penetration test:** A penetration test, or sometimes pentest, is a software attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data. The process typically identifies the target systems and a particular goal. A pen tester then reviews available information and undertakes various means to attain the goal.
- **Pen Testing:** A method of testing, measuring and enhancing established security measures on information systems and support areas.
- **Pen Tester:** Someone who probes for and exploits security vulnerabilities in web-based applications, networks and systems. In other words, you get paid to legally hack.

KNOW YOUR OPPONENTS


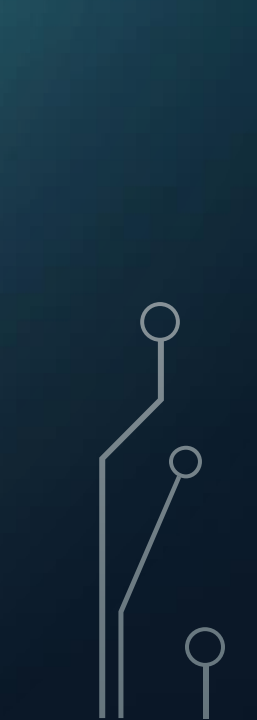
- **Script Kiddies:** Hackers who have limited or no training and know how to use basic tools or techniques. They may not even understand any or all of what they are doing.
- **White-Hat Hackers:** Hackers who think like the bad guys, but are really good guys. (ethical hackers and pen testers)
- **Gray-Hat Hackers:** Hackers that are between white and black hat hackers
- **Black-Hat Hackers:** Hackers who are the bad guys and normally break numerous laws and cause harm to individuals.
- **Cyberterrorists:** Attackers that try to knock out a target without regards to being stealthy.

PRESERVING CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

- For review the 3 pillars of IA are confidentiality, integrity, and availability
- Also be aware of the anti-CIA triad which includes
 - Improper Disclosure
 - Unauthorized Alterations
 - Disruption / Loss



RECOGNIZING HOW HACKING IS CATEGORIZED UNDER THE LAW

- Over the last 20+ years crimes associated with hacking have evolved tremendously and the following slides provide information regarding the different categories of cybercrime.
- 
- 

DIFFERENT TYPES OF CYBER CRIMES

- **Identity Theft:** The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.
- **Theft of Service:** unauthorized access accounts due to attacks such as stealing passwords and/or bypassing them all together, as well as back door access by exploiting existing vulnerabilities.
- **Network Intrusion or Unauthorized Access:** Unauthorized access to a network resource(s)

DIFFERENT TYPES OF CYBER CRIMES

- Posting and/or transmitting Illegal Material: Posting and streaming copyrighted or illegal material
- Fraud: Wrongful or criminal deception intended to result in financial or personal gain
- Embezzlement: Theft or misappropriation of funds placed in one's trust or belonging to one's employer

DIFFERENT TYPES OF CYBER CRIMES

- **Dumpster Diving:** A popular form of modern salvaging of waste discarded in large commercial, residential, industrial and construction containers.
- **Malicious Code:** The term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.
- **Unauthorized Destruction or Alteration of Information:**

DIFFERENT TYPES OF CYBER CRIMES

- **Denial of Service:** An interruption in an authorized user's access to a computer network, typically one caused with malicious intent.
- **Distributed Denial of Service:** An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
- **Cyberstalking:** The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.

DIFFERENT TYPES OF CYBER CRIMES

- **Cyberbullying:** The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature:
- **Cyberterrorism:** The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society:

OPERATING SYSTEM CONSIDERATIONS

- **Network Support:** Most modern operating systems not allow users to connect to networks with wired connections such as CAT-5 for Ethernet capabilities, but wi-fi, Bluetooth, 4G, ETC.
- **Multitasking:** The ability to run multiple applications at once. Keep in mind that too many applications open at once will hinder performance.
- **Application Support:** Are developers properly providing support for bug fixes and patches, especially in terms of security and working properly with other installed software.
- **Hardware Interface:** Ensure that the OS supports the hardware you plan on using.
 - EX. If you are video editor don't expect all OSX capture cards to work on Linux or even Windows.
- **Graphical User Interface (GUI):** Look and feel of what the user sees. Normally a desktop or a command prompt

CONSIDERATIONS WITH WINDOWS

- Numerous Updates and Patches
- Default Configurations (Especially older versions that had everything running at root level)
- Legacy Systems (Trying to make older applications run on newer versions of Windows)

CONSIDERATIONS WITH MAC OS

- Legacy Software(Trying to make older applications run on newer versions of Mac OS)
 - It's actually impossible to run most applications made before 2005 due to the switch from PowerPC chips to Intel based hardware
- Support
- Naivete (Can still be hacked and attacked even people think it's Indestructible)
- Features

CONSIDERATIONS WITH LINUX

- Open Source – Everyone can see the source code
- Flexibility
- Application Support for multiple variants

CONSIDERATIONS WITH UNIX

- Learning Curve
- Support
- Application Support can also be challenging since UNIX has been out since the 1960s and there are so many variants out there.

SECURING THE OPERATING SYSTEM SOFTWARE

Securing the operating system software includes the following steps:

1. Develop the security policy
2. Perform host software baselining
3. Configure operating system security and settings
4. Deploy the settings
5. Implement patch management

SCANNING AND ENUMERATION

- Once appropriate information is obtained for pen testing it's time to move onto scanning and enumeration.
- **Scanning** includes ping sweeping, port scanning, and vulnerability scanning.
- **Enumeration** is the process of extracting meaningful information from the openings and information you found during scanning, such as usernames, share data, group information, etc.

INTRODUCTION TO SCANNING

- **Ping Sweeps** check for live systems and are intended to search subnets or lists of IP addresses with the intent of identifying which addresses have a system that is powered on behind it.
- **Port Scanning** is a form of scanning that targets individual IP addresses and seeks to identify the ports that are open and closed on a specific system.
- **Vulnerability Scanning** finds weaknesses or problems in an environment and generates a report on its findings.

INTRODUCTION TO SCANNING

- When performing a scan you should retrieve the following information:
 - IP addresses of systems that are turned "live," which includes not just computers but tablets, mobile (cell) phones, printers, wireless access points, etc.
 - Lists of open and closed ports on targeted systems.
 - Operating system versions, which can be obtained in many cases during the scanning phase.
 - However one should exercise caution since attempting to identify a system may increase chances of detection
 - MAC addresses
 - Service information
 - Port data
 - Other network information depending on the situation

PINGING TO CHECK FOR LIVE SYSTEMS

- ***Pinging*** is a commonly used network diagnostic utility. However, firewalls and routers will quite frequently block it on the perimeter of a network where the outside world and the internal network meet.
 - The explains why some of you may have had issues with the ping command for random web sites with certain projects.

NMAP

- *Nmap*, or the "Network Mapper" is a free utility used for network discovery and is available on all major operating systems.

Nmap has both a command-line interface as well as a GUI interface known as Zenmap

BANNER GRABBING REVISITED

HTTP/1.1 200 OK

Date: Mon, 1 May 2017 22:10:40 EST

Server: IIS/7.0 (Windows Server 2012)

Last-Modified: Thu, 22 Feb 2015 11:20:14 PST

ETag: "1986-69b-123a4bc6"

Accept-Ranges: bytes

Content-Length: 1110

Connection: close

Content-Type: text/html

- I also received information about some of you having problems with ports and Telnet.
- If this is the case don't worry as long as your write up reflects that you understand how to do the commands and what they do.
- For future reference use port 21 or 22 when using Telnet.

TOOLS FOR BANNER GRABBING

- **Netcraft:** An online tool designed to gather information about servers and web servers.
- **IDServe:** A utility specifically designed to fingerprint web servers and can be obtained from <https://www.grc.com/id/idserve.htm>

ENUMERATION

- ***Network Enumeration*** is a computing activity in which usernames and info on groups, shares, and services of networked computers are retrieved. It should not be confused with network mapping, which only retrieves information about which servers are connected to a specific network and what operating system runs on them.

NULL SESSIONS

- A *null session* is an anonymous connection to an inter-process communication network service on Windows-based computers. The service is designed to allow named pipe connections but may be used by attackers to remotely gather information about the system.

Virtualization

- ◆ Allows users to run different operating systems on one computer without rebooting.
- It emulates certain hardware, but uses the actual CPU and therefore faster than emulation.

Virtualization

- ◆ Windows, Linux, and Mac OS X (Intel Only) users can also use VirtualBox from Oracle
 - www.virtualbox.org

Why Use Virtualization

- No matter how much some people praise an operating system, not every operating system is going to have every application that you want, or have the same performance for all tasks and applications across the board.

KALI LINUX

- Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd. Mati Aharoni, Devon Kearns and Raphaël Hertzog are the core developers.
- It includes some of the most commonly known/used security and analysis tools, aiming for a wide spread of goals, ranging from web application analysis to network analysis, stress tests, sniffing, vulnerability assessment, computer forensic analysis, automotive and exploitation. It has been built on Ubuntu core system yet fully customized, designed to be one of the best Penetration testing and security distribution and more.
- <https://www.kali.org/>

PREPPING TOOLS

- Today we will be looking at the following tools:
 - Dnscan
 - Subbrute
 - Dirsearch

DNSCAN

- Dnscan is a Python tool that uses a wordlist to resolve valid subdomains.
- At this point we will pull it down from the git repository with the following command:
- `git clone https://github.com/rbsec/dnscan.git`
- You can also download and save it from <https://github.com/rbsec/dnscan> .
- Afterwards from within the command line browse to the directory where it was saved.
- Run this command `./dnscan.py -h` to see the different options

SUBBRUTE

- Subbrute uses public resolvers to brute force the subdomains to provide an extra layer of anonymity.
- Download it using the following command:
 - `git clone https://github.com/TheRook/subbrute.git`
- Alternatively you can download it via a browser at this link:
 - <https://github.com/TheRook/subbrute>
- For this example we can use the dnspop wordlist from:
 - <https://github.com/bitquark/dnspop/tree/master/results>

SUBBRUTE

- A wordlist is needed after installation is complete for it to run.
- Once everything is set up browse to the subroute's directory and run it using this command:
 - `./subroute.py`
- Finally to run it against a domain with our wordlist use the following command:
 - `./subroute.py -s /path/to/wordlist hostname.com`

DIRSEARCH

- Dirsearch is a command-line tool that can be used to brute force the directories.
- Install with the following command:
 - `git clone https://github.com/maurosoria/dirsearch.git`
- Alternatively you can download it through a browser at:
 - `https://github.com/maurosoria/dirsearch`
- Once the download is complete browse to the directory where it was downloaded and run it with this command:
 - `/dirsearch.py -u hostname.com -e aspx,php`

HAVING FUN WITH SHODAN



SHODAN

- Shodan is the world's first search engine to search for devices connected to the internet. It was launched in 2009 by John Matherly.
- Shodan can be used to look up webcams, databases, industrial systems, video games, and so on.
- Shodan mostly collects data on the most popular web services running, such as HTTP, HTTPS, MongoDB, FTP, and many more.
- It's a great tool for use with Kali and other Pen Testing Distros and can be found here:
<https://www.shodan.io/>

The background is a dark teal gradient. In the four corners, there are white, stylized circuit board traces. These traces consist of straight lines of varying lengths and angles, ending in small white circles, resembling a network or data flow diagram.

OTHER DISTROS FOR SECURITY AND PEN TESTING

PARROT SECURITY OS

- Parrot Security OS, also known as ParrotSec, is a Linux distribution based on Debian with a focus on computer security. It is designed for penetration testing, vulnerability assessment and mitigation, computer forensics and anonymous web browsing. It is developed by the Frozenbox Team.
- ParrotSec is intended to provide a penetrating testing tools equipped with many different kinds of tools for user to be test on their lab.
- <https://www.parrotsec.org/>

PARROT SECURITY OS

- Parrot Full is the complete all-in-one environment for pentesting, privacy, digital forensics, reverse engineering and software development.
- The system includes a full arsenal of security oriented tools to cover many categories of the work of a pentester.
- Parrot Lite is a special edition of Parrot designed for daily use, and it targets regular users who need a lightweight, always updated and beautiful system on their laptops or workstations.

PARROT SECURITY OS

- The distribution has the same look and feel of a regular Parrot environment and includes all the basic programs for daily work. Parrot Lite also includes programs to chat privately with people, encrypt documents with the highest cryptographic standards or surf the net in a completely anonymous and secure way.
- The system can also be used as a starting point to build a very customized pentesting platform with only the tools you need, or you can use it to build your professional workstation by taking advantage of all the latest and most powerful technologies of Debian without hassle.

BACKBOX LINUX

- A penetration testing and security assessment oriented Linux distribution providing a network and systems analysis toolkit. It includes some of the most commonly known/used security and analysis tools, aiming for a wide spread of goals, ranging from web application analysis to network analysis, stress tests, sniffing, vulnerability assessment, computer forensic analysis, automotive and exploitation. It has been built on Ubuntu core system yet fully customized, designed to be one of the best Penetration testing and security distribution and more.
- <https://linux.backbox.org/>