LINUX INTERFACE FOR SIMPLIFIED HACKING

(HACKMATE)

ABSTRACT

- Kali OS includes over 300 security testing tools. A lot of the redundant tools from Backtrack have been removed and the tool interface streamlined. You can now get to the most used tools quickly as they appear in a top ten security tool menu. You can also find these same tools and a plethora of others all neatly categorized in the menu system.
- Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

KALI
BY OFFENSIVE SECURITY

INTRODUCTION

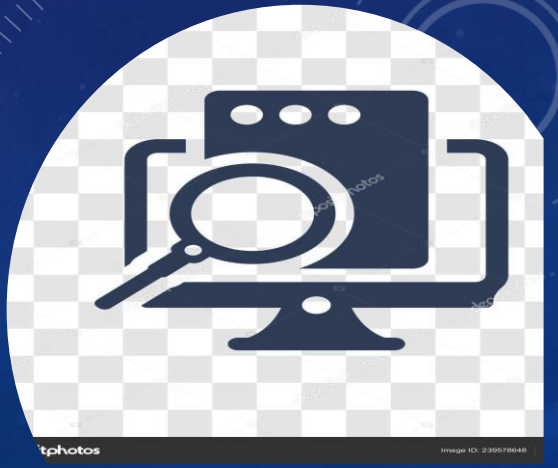
- Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.
- Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.
- In this project we have created a computer program using c++ which enables all the new **kali OS** users to use this obscure operating system with ease and hence enabling them to get a better view of all the hacking tools at a glance and giving them a better knowledge and experience in a very short period of time.this program is an attempt to simplify the new os . This program is named as **HACKMATE.**

HACKMATE (PROJECT OVERVIEW)

- This project is a C++ program providing simpler layout to new user about the various tools present in **kali os**
- Given in the flowchart are the various hacking tools that are covered under the project

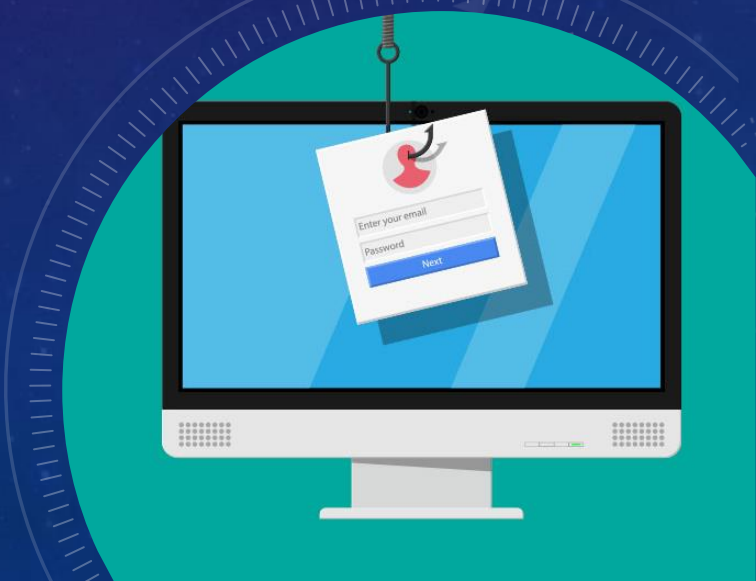
NETWORK SCANNING

- Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.
- **N map:-**Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.



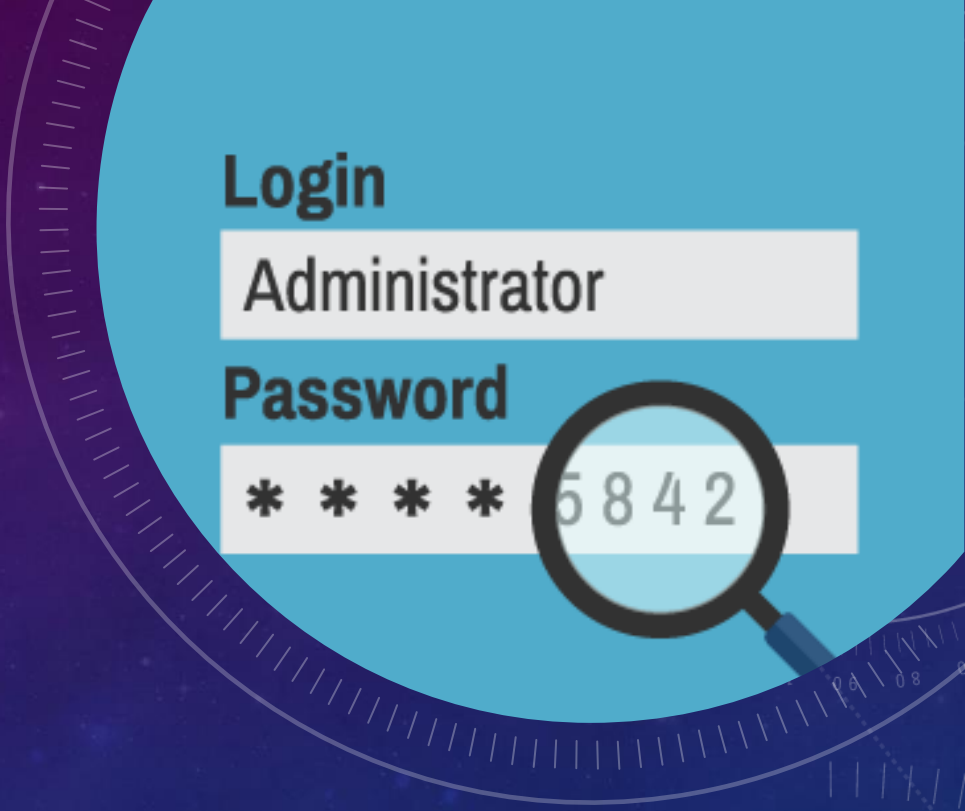
PHISHING ATTACK

- **Phishing** is a cyber **attack** that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.
- HIDDEN EYE:-Hidden Eye is an all in one tool that can be used to perform a variety of online attacks on user accounts. It's well loaded, therefore it can be used as keylogger (keystroke logging), phishing tool, information collector, social engineering tool, etc.



PASSWORD CRACKING

- Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it’s an art of obtaining the correct password that gives access to a system protected by an authentication method.
- **brut3k1t** is a security-oriented research framework for conducting brute force attacks against a multitude of protocols and services.



WI-FI HACKING

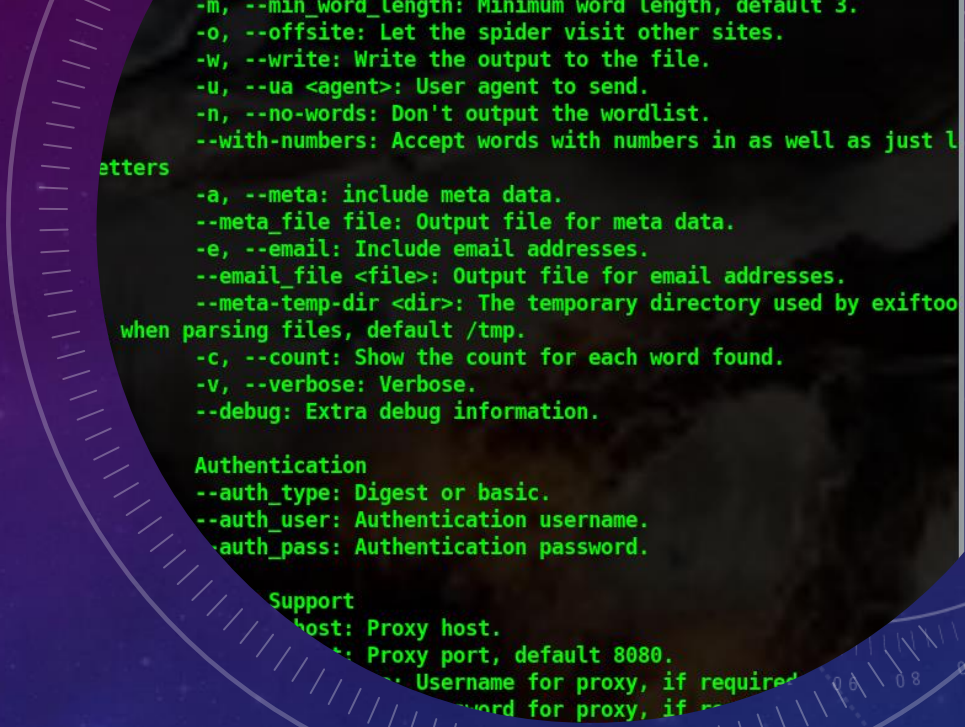
- **Wi-Fi hacking** is essentially cracking the security protocols in a wireless network, granting full access for the **hacker** to view, store, download, or abuse the wireless network.
- **Aircrack-ng** is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured

BACKDOOR ACCESS

- A backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.
- we use **msfvenom** to inject a meterpreter reverse payload into our executable, encode it and save the backdoored file into our webroot directory.
- The **Metasploit Project** is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

CUSTOM PASSWORD LIST

- Password cracking is a long-established art, relying on a combination of brute-force processing power and the ability to refine your list down to likely options based on what you know about a target. Many security protocols are vulnerable to brute-forcing attacks, which at its core relies on a few key principals.
- CUPP or the 'Common User Passwords Profiler' to generate custom password lists tailored towards individual targets. The application leverages user-supplied open-source intelligence (OSINT) information to compile an extensive and powerful password list. CUPP is written in Python and even provides an interactive interface to build its custom password lists.



THANK YOU!