IOT & Cyber Security

Week 4-5 Kali Linux

What is Kali Linux and Why people use the Kali Linux?

Kali Linux is a free and open-source operating system designed for network security, digital forensics, and penetration testing. It is based on the Debian Linux distribution and comes pre-installed with a wide range of security tools that can be used for various purposes, such as identifying and exploiting vulnerabilities, creating and analyzing network traffic, and cracking passwords.

One of the main reasons people use Kali Linux is that it provides a comprehensive and convenient platform for conducting various kinds of security assessments and penetration tests. It allows users to easily access and use a wide range of security tools, without having to install and configure them individually. Additionally, Kali Linux is regularly updated with new tools and features, making it a valuable resource for security professionals and researchers.

Another reason people use Kali Linux is that it is specifically designed to be used in a forensic or penetration testing environment, and includes features such as live booting from USB or DVD, the ability

to run from a RAM disk, and support for remote SSH connections. This makes it a flexible and powerful platform for conducting various kinds of security assessments.

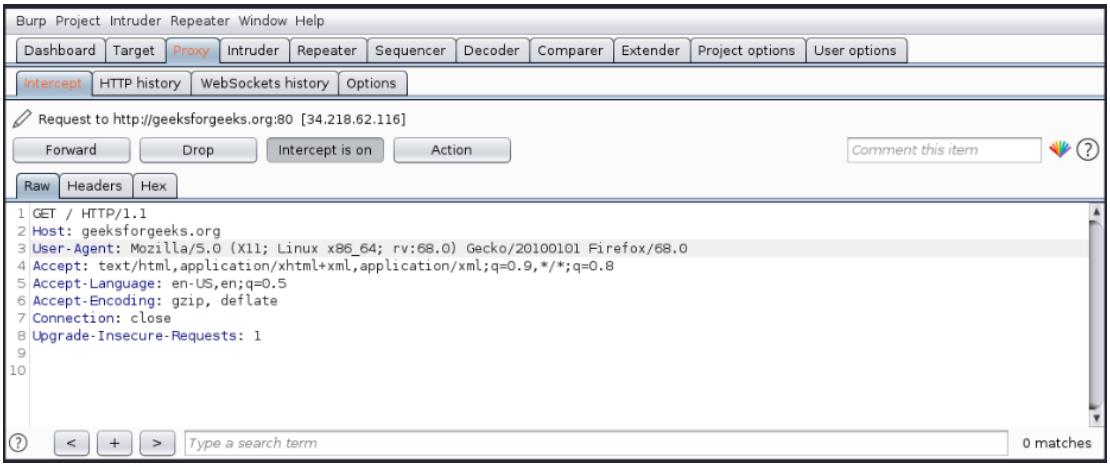
Why Kali?

- Includes more than 600 Penetration Testing Tools
- Free to use (if your time has no value)
- Operates on Open-Source Development Model
- Gives freedom to customize completely
- Developed in a secure environment
- Custom kernel, patched for injection
- ARMEL and ARMHF support
- Diverse and vibrant community

Top 10 Kali Linux Tools For Hacking

Here is a list of 10 popular tools that are commonly used in Kali Linux for hacking:

1. **Aircrack-ng:** a set of tools for assessing wireless network security
2. **Burp Suite:** a tool for performing web application security testing

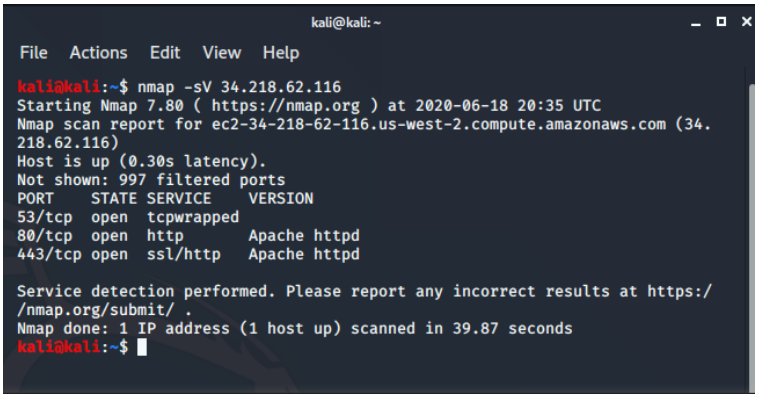


3. **Maltego**: a tool for information gathering and data visualization

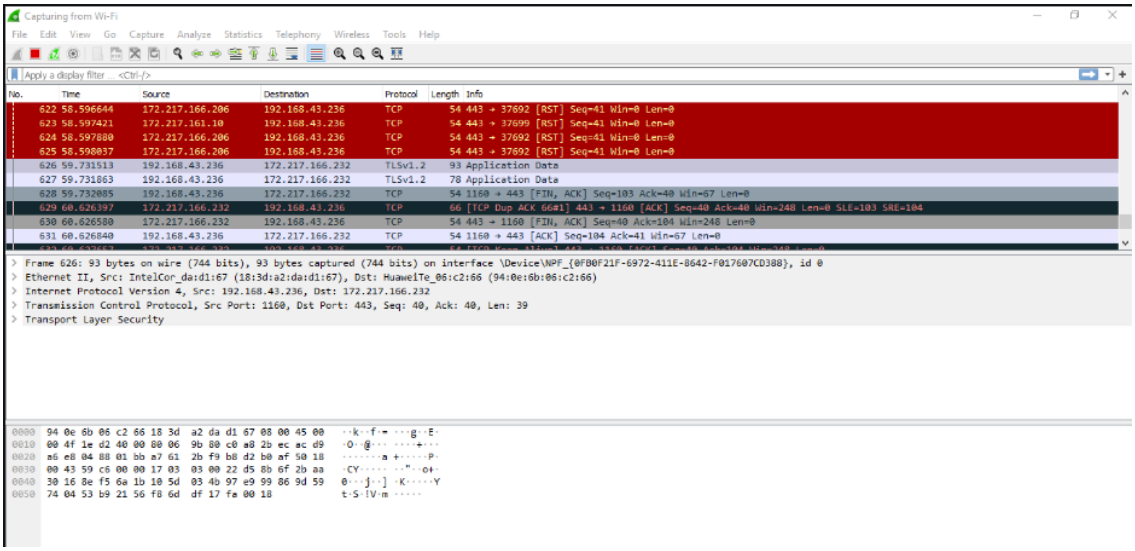
4. **Metasploit**: a tool for developing and executing exploit code

5. **Nmap**: a network mapping and scanning tool

```
nmap -sV ipaddress
```



6. **Wireshark**: a network protocol analyzer for analyzing network traffic



7. **Hashcat**: a password cracking tool
8. **John the Ripper**: another password cracking tool
9. **sqlmap**: a tool for automating SQL injection attacks
10. **Social Engineering Toolkit (SET):** a tool for carrying out social engineering attacks (e.g. phishing attacks).

Keep in mind that these tools can be used for both legitimate and malicious purposes, and it is important to use them responsibly and only with proper authorization.

Reflection about Kali Linux:

Kali Linux is a powerful and widely used operating system that has become an essential tool for many security professionals and researchers. It provides a comprehensive platform for conducting various kinds of security assessments and penetration tests, and is regularly updated with new tools and features.

One of the main benefits of Kali Linux is that it comes pre-installed with a wide range of security tools, which can be used to identify and exploit vulnerabilities, create and analyze network traffic, and crack passwords. This makes it a convenient and efficient platform for conducting security assessments, as users do not have to install and configure tools individually.

However, it is important to note that Kali Linux can also be used for malicious purposes, and it is crucial to use it responsibly and only with proper authorization. It is also worth considering that using Kali Linux may not be suitable or necessary in all situations, and other tools and approaches may be more appropriate depending on the specific goals and requirements of a given security assessment.

Overall, Kali Linux is a valuable resource for security professionals and researchers, and can be an effective tool for conducting various kinds of security assessments and penetration tests. However, it is important to use it responsibly and appropriately, and to consider its limitations and potential risks.

References:

https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/

https://medium.com/analytics-vidhya/a-comprehensive-guide-to-kali-linux-essentials-and-beyond-ae29298c3be3