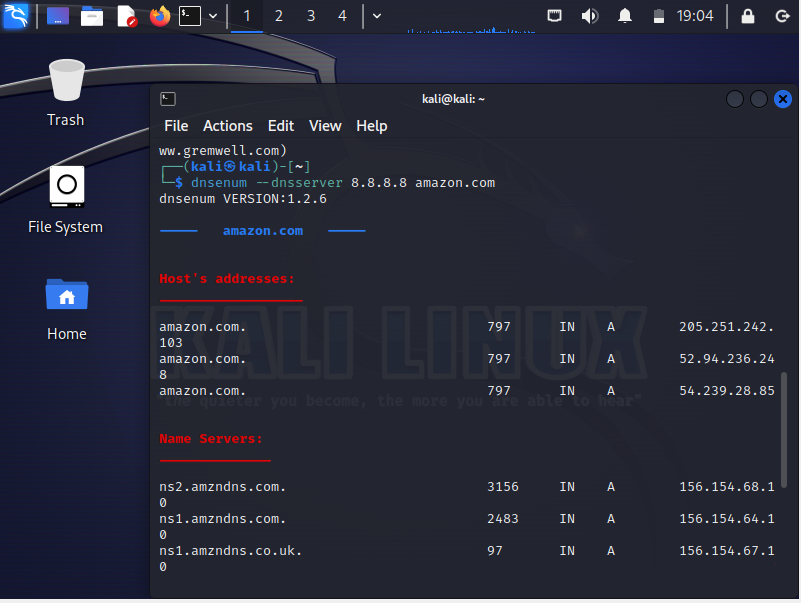
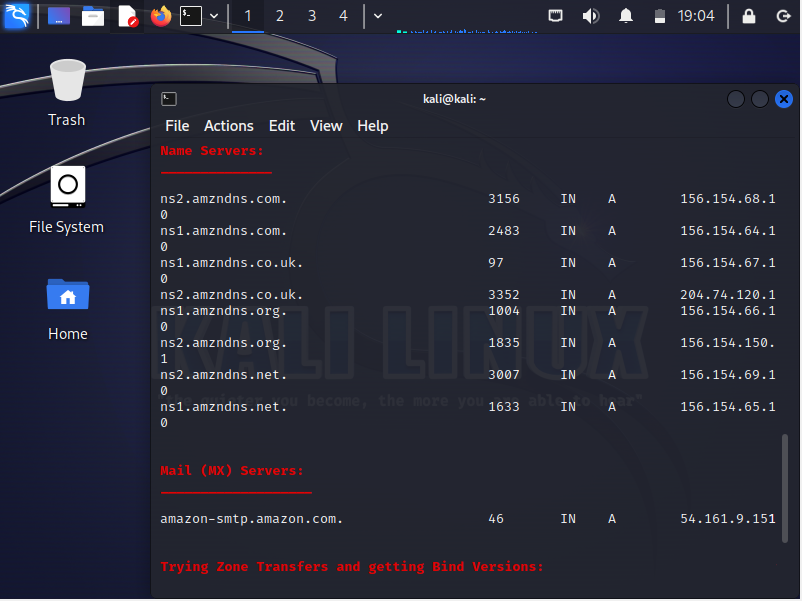
**Assignment 2**

**Information Gathering - dnsenum**





Tools used for everything from identifying all the devices on a network -- enumerating -- to linking a network interface controller's [media access control address](https://www.techtarget.com/searchnetworking/definition/MAC-address) with an IP address to identifying open ports on targeted servers. Kali Linux information gathering tools include scanners, such as [Nmap](https://www.techtarget.com/searchsecurity/feature/How-to-use-Nmap-to-scan-for-open-ports) and [Wireshark](https://www.techtarget.com/searchsecurity/tip/Wireshark-tutorial-How-to-sniff-network-traffic), as well as information planning platforms that integrate the leading tools, often with GUIs for more comprehensive functionality.

**Wireless attacks**

This category includes a broad range of utilities to carry out cybersecurity exercises -- or hack attacks -- against wireless systems, including those connected by Bluetooth and Wi-Fi. The top Kali wireless utility is [Aircrack-ng](https://www.computerweekly.com/tip/Step-by-step-aircrack-tutorial-for-Wi-Fi-penetration-testing), a software suite that includes a network detector, wireless packet sniffer and credential cracking tools used to attack wireless [authentication](https://www.techtarget.com/searchsecurity/definition/authentication) protocols, such as Wired Equivalent Privacy ([WEP](https://www.techtarget.com/searchsecurity/definition/Wired-Equivalent-Privacy)) and [Wi-Fi Protected Access](https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access).

**Web applications**

This category covers a lot of ground, and like everything in Kali, tools exist for almost any pen testing or [red-teaming exercise](https://www.techtarget.com/whatis/definition/red-teaming) involving web applications. While [OWASP](https://www.techtarget.com/searchsoftwarequality/definition/OWASP) is a rich cybersecurity platform for network attacks and defenses included with Kali, [OWASP Zed Attack Proxy](https://www.zaproxy.org/docs/developer/) is just one of the many utilities available for attacking web apps.

**Password attacks**

This category includes standalone password cracker tools, such as [Hydra](https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-Hydra-password-cracking-tool), Ncrack, Hashcat and [John the Ripper](https://www.techtarget.com/whatis/definition/John-the-Ripper). It also includes utilities that help increase the effectiveness of any password cracker, such as Crunch, a program for generating wordlists; [Ophcrack](https://www.techtarget.com/searchsecurity/tip/Ophcrack-Password-cracking-made-easy), a program that uses rainbow tables to crack Windows passwords; and more.

**Exploitation Tools:**

 These are tools used to exploit vulnerabilities found in systems. Usually, a vulnerability is identified during a Vulnerability Assessment of a target.

**Examples: –** Armitage, Metasploit Framework, SET, Router Sploit, Yersinia etc…

**Sniffing and Spoofing:** These are tools used for network packet captures, network packet manipulators, packet crafting applications, and web spoofing. There are also a few VoIP reconstruction applications.

**Examples: –** Burp Suite, Responder, Ettercap, SSLStrip, Dsniff, Wireshark etc…

**Maintaining Access:** Maintaining Access tools are used once a foothold is established into a target system or network. It is common to find compromised systems having multiple hooks back to the attacker to provide alternative routes in the event a vulnerability that is used by the attacker is found and remediated.

**Reverse Engineering:** These tools are used to disable an executable and debug programs. The purpose of reverse engineering is analyzing how a program was developed so it can be copied, modified, or lead to development of other programs. Reverse Engineering is also used for malware analysis to determine what an executable does or by researchers to attempt to find vulnerabilities in software applications.

**Examples: –** Dex2jar, Ollydbg, Smali, Yara, Apktool etc…

**Stress Testing:** Stress Testing tools are used to evaluate how much data a system can handle. Undesired outcomes could be obtained from overloading systems such as causing a device controlling network communication to open all communication channels or a system shutting down (also known as a denial of service attack).

**Examples: –** iaxflood, DHCPig, t50, Termineter, ipv6-toolkit etc…

**Hardware Hacking:** This section contains Android tools, which could be classified as mobile, and Ardunio tools that are used for programming and controlling other small electronic devices.

**Examples: –** Android-sdk, Apktool, Arduino, Sakis3G etc…