Introduction to Cyber Security and Ethical Hacking

Cybersecurity is a rapidly evolving field that involves protecting computer systems, networks, and data from a variety of threats. Ethical hacking, also known as penetration testing or white hacking, is the practice of identifying vulnerabilities and weaknesses in a system with the owner's permission to prevent them from being exploited by malicious individuals. This topic will provide an overview of basic commands, file management, system administration, networking, shell scripting, penetration, and other related topics in Cybersecurity and ethical hacking.

Basic Commands: Understanding basic command operations is critical to navigating the file system, performing tasks, and troubleshooting. Some basic commands include ls (list), cd (change directory), pwd (display current working directory), mkdir (create new directory), and rm (delete file). We have various cheatsheets in our repo to assist you with learning these.

File Management: Learn how to create, modify, and delete files and directories, and work with different types of file systems, such as NTFS, FAT, and EXT. Also, understand the concepts of access permissions, ownership, and privileges.

System Administration: Understand the basics of system administration, including installing and configuring operating systems, managing services and processes, and working with registries. Also learn about various system administration tools such as PowerShell and System Center Configuration Manager.

Networking: Study the network protocols, topologies, and services needed to connect and maintain networks. Also, understand network security concepts, including firewalls, VPNs, and encryption.

Shell Scripting: Learn how to automate repetitive tasks using shell scripts, which are programs written in languages such as Bash, Python, or Perl. These scripts can be used to perform tasks such as backups, deploying configurations, or monitoring the system.

Penetration: Learn techniques and tools for detecting vulnerabilities in computer systems and networks. This may include using tools such as Metasploit, Nmap, and Wireshark to scan, discover services, analyze traffic, and exploit known vulnerabilities.

Bug Hunting: Become proficient at finding and reporting bugs in software applications. This can include understanding different types of vulnerabilities such as SQL injection, cross scripting and authentication flaws.

Additional Topics: There are numerous other topics within Cybersecurity and ethical hacking that can be explored, such as data analytics, digital evidence forensics, and web application security.

By studying these topics, you'll gain a solid foundation in Cybersecurity and ethical hacking. With hands-on experience and continuous learning, you can further your career in this exciting field.