CYBERSECURITY GUIDE

Here is a cybersecurity study guide that you can follow to get started in the field:

****Foundation****

*** **Linux: **** Linux is a free and open-source operating system that is widely used in cybersecurity. It is important to have a good understanding of Linux in order to work in this field.
*** **Bash: **** Bash is a shell scripting language that is used to automate tasks on Linux. It is important to learn Bash scripting in order to be able to automate common tasks in cybersecurity.
*** **Windows PowerShell: **** Windows PowerShell is a scripting language that is used on Windows systems. It is important to learn Windows PowerShell in order to be able to automate common tasks on Windows systems.
*** **Networking: **** Networking is the study of how computers communicate with each other. It is important to have a good understanding of networking in order to work in cybersecurity.
*** **VIM: **** VIM is a text editor that is used by many cybersecurity professionals. It is important to learn VIM in order to be able to edit files and scripts on Linux systems.
*** **Programming Languages: **** There are many programming languages that are used in cybersecurity. Some of the most common programming languages include Python, C/C++, JavaScript, and HTML.

****The Basics****

*** **OWASP Framework: **** The OWASP Framework is a set of security controls that can be used to improve the security of software applications.
*** **OSINT: **** OSINT stands for Open-Source Intelligence. It is the process of collecting information from publicly available sources.
*** **Recon, Scanning & Enumeration: **** Recon, Scanning, and Enumeration are all steps in the process of gathering information about a target system.
*** **Exploitation & Attacking Vectors: **** Exploitation is the process of using a vulnerability to gain access to a system. Attacking vectors are the ways that attackers can gain access to a system.
*** **Privilege Escalation: **** Privilege escalation is the process of gaining elevated privileges on a system.
*** **Windows Active Directory: **** Windows Active Directory is a directory service that is used to manage users, computers, and other objects in a Windows environment.
*** **Exploit Dev & Payloads: **** Exploit development is the process of creating an exploit that can be used to exploit a vulnerability. Payloads are the code that is executed when an exploit is successful.

****Advanced****

*** **Malwares, Rootkits, Reserve Engineering: **** Malware is software that is designed to harm a computer system. Rootkits are tools that are used by attackers to gain root access to a system. Reverse engineering is the process of taking apart software to understand how it works.

CYBERSECURITY GUIDE

* **Pivoting and Persistence (Post Exploitation): ** Pivoting is the process of moving from one system to another. Persistence is the process of maintaining access to a system after the initial exploit has been successful.

Tools to Master (Must Learn)

* **Nmap: ** Nmap is a network scanner that can be used to gather information about a target system.
* **Burp Suite: ** Burp Suite is an integrated platform for web application security testing.
* **Wireshark: ** Wireshark is a network protocol analyzer that can be used to capture and analyze network traffic.
* **Metasploit: ** Metasploit is a framework for developing and using exploits.

***Nessus: ** Nessus is a vulnerability scanner that can be used to identify security weaknesses in systems and applications.

***Splunk: ** Splunk is a data analytics platform that can be used to collect, store, and analyze security logs.

***IBM QRadar: ** IBM QRadar is a security information and event management (SIEM) platform that can be used to collect, correlate, and analyze security events from across an organization.

***SIEM: ** SIEM stands for security information and event management. A SIEM is a software platform that collects, stores, and analyzes security logs and events from across an organization. SIEMs can be used to identify security threats, investigate security incidents, and improve security posture.

**OS: ** Kali Linux

Kali Linux is a penetration testing distribution of Linux that is used by many cybersecurity professionals. It comes pre-installed with a wide variety of tools that can be used for penetration testing.

Resources

There are many resources available to help you learn about cybersecurity. Some of the most popular resources include:

* **YouTube: ** There are many cybersecurity channels on YouTube that offer free tutorials and courses.
- the cyber mentor
- PhD security
- Chris Greer
- freecodecamp
- life overflow
- hackersploit
- john Hammond
-- null byte
- masters in it

CYBERSECURITY GUIDE

- bitten tech
- the hackers world
- Tec chop net

* **Paid Courses: ** There are many paid courses available that can teach you about cybersecurity.
-- on Udemy
-- tcm security
-- Chris Greer
David bombal
-- My Guidance - Join Https://T.Me/+Tbgktul0nc05njk1

* **Playgrounds: ** There are many cybersecurity playgrounds that allow you to practice your skills.
try hack me
Hack the box
Cybrary

* **Certifications: ** There are many cybersecurity certifications available that can demonstrate your skills.
Ceh master
Pentest+
Security+
ejpt

Additional Subjects

There are many additional subjects that you can learn about in order to improve your skills in cybersecurity. Some of the most popular additional subjects include:

* **MITRE ATT&CK: ** The MITRE ATT&CK framework is a taxonomy of attack techniques that is used by many cybersecurity professionals.
* **NIST Framework - GRC: ** The NIST Framework for Information Security Management is a framework that can be used to improve the security of an organization.
* **ISO 27001 - GRC: ** ISO 27001 is an international standard for information security management.

Introducing Sanskrit's Cyber Security Guidance, your gateway to cyber security success! Join our Telegram group to discover more and embark on your cyber security journey today.
https://t.me/+TbGktUl0nc05Njk1

Conclusion

CYBERSECURITY GUIDE

Cybersecurity is a complex and ever-changing field. However, by following this study guide, you can gain the foundational knowledge that you need to get started in this field.

In addition to these resources, it is also important to have a strong understanding of cybersecurity principles and best practices. There are many resources available to help you learn about cybersecurity, including books, articles, online courses, and training programs.

By mastering the tools and principles of cybersecurity, you can help to protect your organization from cyberattacks.

Here are some additional tips for mastering cybersecurity:

*** **Start with the basics. **** Before you can master any tool, you need to have a good understanding of the basics. This includes understanding the tool's features and capabilities, as well as the terminology used in cybersecurity.
*** **Practice regularly. **** The best way to learn how to use a tool is to practice using it regularly. This will help you to become familiar with the tool's interface and learn how to use it effectively.
*** **Get help from others. **** There are many resources available to help you learn how to use cybersecurity tools. These resources include online tutorials, forums, and user groups.
*** **Stay up-to-date. **** Cybersecurity tools are constantly being updated with new features and capabilities. It is important to stay up-to-date with the latest updates so that you can use the tool to its full potential.