Introduction to Ethical Hacking

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Discussed Vulnerabilities, Threat Vectors, Exploits and Attack detection + Responses

Objectives

- Learn what Ethical Hacking is and why it is important
- Explore the differences between Ethical and Malicious Hackers
- Discover Ethical hacking phases, techniques and Best Practices
- Know the different certifications for Ethical Hacking


When the free trial runs out so you make a new email account and reregister
donny drama
HACKERMAN


Police officer: So where did the hacker go?
Me : I don't know he just ransomware
HHAHA
HA HA
YELLOWJOKES.COM

What is Ethical Hacking

- Ethical hacking is the practice of identifying and exploiting vulnerabilities in computer systems and networks using the same methods and techniques as malicious hackers, but with the permission and knowledge of the system owner.

- The goal of ethical hacking is to proactively identify and address security flaws in order to improve the system's overall security posture. Ethical hacking is usually done by trained and certified professionals who follow a strict code of ethics and legal guidelines.

Ethical VS Malicious

Ethical Hacker/White Hat	Malicious Hacker/Black Hat
Hacks ***with*** authorization and on-behalf of an organization	Hacks ***without*** authorization
Shares information and issues uncovered for remedy to prevent future attacks	Takes advantage of vulnerabilities discovered within an organization's network
Penetrates networks and systems to evaluate potential vulnerabilities and exploits to provide actionable solutions	Seeks for personal gain to steal sensitive personal data, to install malicious software or "because they can."

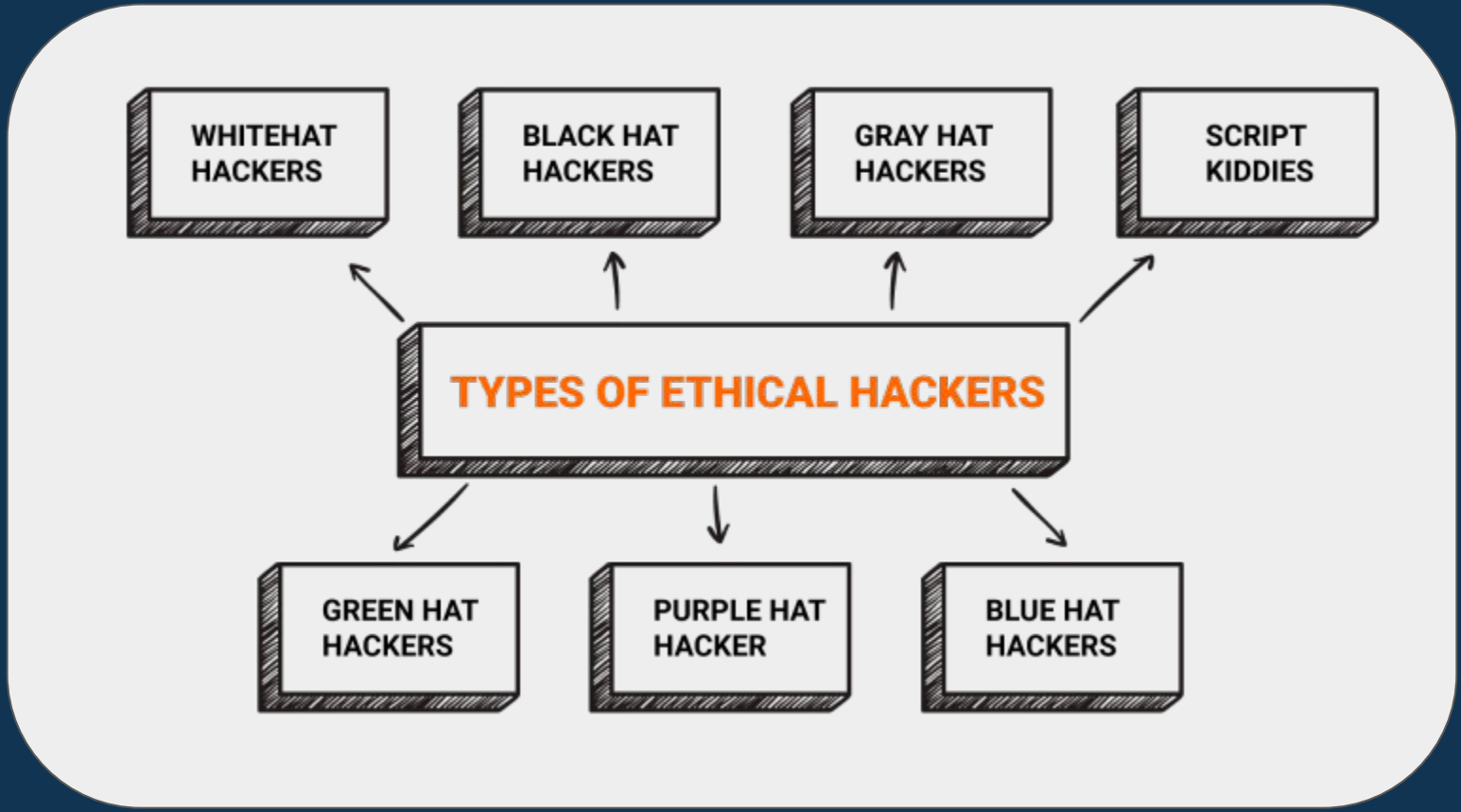
https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fstart.cybervista.net%2Fhubfs%2FHacker_Chart.png&f=1&nofb=1&ipt=c4a56f8bb2b92f8d78c776f833f92d413fea7123f0d4b8d387a81b4fc844cc50&ipo=images

Why is it Important?

- For starters, it identifies and exposes vulnerabilities in computer systems and networks before malicious hackers can exploit them.

- Secondly, ethical hacking is crucial for adhering to a variety of laws and industry standards, including the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS).

- Lastly, ethical hacking is critical for retaining the trust of customers and stakeholders. A data breach or other security incident can cause significant financial and reputational harm to a company, and ethical hacking can help prevent these incidents from happening.



https://www.testbytes.net/wp-content/uploads/2020/10/Types-of-Ethical-Hackers-768x432.png

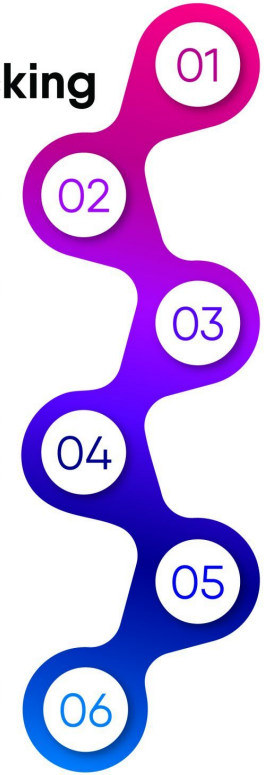
Ethical Hacking Phases

- Reconnaissance: Gathering information about the target, such as IP addresses, open ports, and operating system.
- Scanning: By actively probing the target to find vulnerabilities like open ports, services, and software versions, scanning involves actively examining the target.
- Gaining Access: Exploiting the vulnerabilities that have been found will allow access to the target system or network.
- Maintaining Access: Establishing a consistent presence on the target system or network is necessary for maintaining access.
- Covering Tracks: Removing traces of the ethical hacking activity is known as "covering tracks."

It is absolutely crucial to be aware of the importance of obtaining permission before conducting an ethical hacking engagement, and the potential legal consequences of conducting illegal hacking activities.

MYCAPTAIN

Phases of Ethical Hacking



Reconnaissance

The first step is to gather data and information about the target system. This is so that we can easily gain control of the system.

Scanning

This is the phase where the hacker recons the entire system to find vulnerabilities and security loopholes. This phase includes using port scanners, net mappers, and other such

Gaining Access

The vulnerabilities found in the previous phase are used at this point to gain access and enter the target system without raising any suspicions.

Maintaining Access

In this phase the hacker uses measures like installing backdoors and payloads into the system to maintain access to the system.

Clearing Tracks

As the name suggests, this is the phase of clearing all signs of any malicious activities performed in the system. Despite it being an unethical process, ethical hackers still have to perform it to help understand how a cracker might do these activities.

Reporting

This is the phase that differentiates an ethical hacker from others. In this phase, the hacker compiles a report of the vulnerabilities found (if any), tools used in each process, success rate, and the pro-

Learn what you Love!

LIVE and Online with Young Professionals

www.mycaptain.in

Hyperiondev

https://blog.mycaptain.in/wp-content/uploads/2020/02/Ethical-hacking-Phases-of-Ethical-hacking-1568x2040.jpg

Ethical Hacking Techniques

- Cracking passwords with software tools in order to gain access to a target system or network is known as password cracking.

- Social engineering is the practice of tricking people into disclosing private information, like usernames and passwords.

- Exploiting vulnerabilities entails locating and taking advantage of hardware or software flaws to access a target system or network.

As an Ethical Hacker it is just as important to ensure that you remain up-to-date with the latest ethical hacking techniques and tools.

Tools and Techniques

- Vulnerability Scanners: Automated tools called vulnerability scanners search target networks or systems for known vulnerabilities.(OpenVAS, Nessus)

- Packet Sniffers: Packet sniffers are devices that intercept and examine network traffic; they are frequently used to find and take advantage of network vulnerabilities.(Wireshark)

- Exploit Frameworks: Frameworks for automating the process of exploiting vulnerabilities are known as "exploit frameworks" and are groups of software tools and scripts.(BeEF)

Ethical Hacking Best Practices:

1. Getting written consent before carrying out any ethical hacking activities.
2. Keeping all information about the target and the engagement strictly confidential.
3. Keeping abreast of the newest tools and techniques for ethical hacking.
4. Recording all actions taken and results obtained during the engagement.
5. Making sure that all discovered vulnerabilities are reported to the appropriate parties.

Ethical Hacking Certification:

- **Certified Ethical Hacker (CEH)**
- **Offensive Security Certified Professional (OSCP)**
- **CompTIA PenTest+**
- **GIAC Penetration Tester (GPEN)**

A professional's knowledge and abilities in the field are validated by certification, which also shows that person is committed to using hacking techniques that are morally and responsibly.

Ethical Hacking Certification:

- Furthermore, in the field of cybersecurity and ethical hacking, it is critical to emphasize the importance of education and continuous learning. As technology advances and new threats emerge, ethical hackers must stay current on the latest tools, techniques, and best practices.

- Ethical hackers can improve their skills and knowledge while also demonstrating their commitment to the highest ethical and professional standards by investing in education and professional development.

Hyperiondev

Wrapping Up.

- Ethical hacking should always be conducted with the permission and knowledge of the target organization. Any unauthorized or illegal hacking can result in serious consequences, both legally and morally. It is important to remember that the goal of ethical hacking is to improve the security of a system and protect against potential threats, not to cause harm or disruption.

- While ethical hacking tools are designed to identify vulnerabilities and potential attack vectors, they are not foolproof and can miss critical vulnerabilities

- it's important to have a comprehensive methodology in place that takes into account the unique aspects of each engagement. A good methodology should include various phases such as planning, reconnaissance, vulnerability assessment, exploitation, and post-exploitation.

Next up

- Penetration Testing

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"