





DAILY ASSESSMENT FORMAT

Date:	20 th June 2020	Name:	Soundarya NA
Course:	Ethical Hacking	USN:	4AL16EC077
Topic:	Ethical Hacking	Semester & Section:	8 th - B

FORENOON SESSION DETAILS

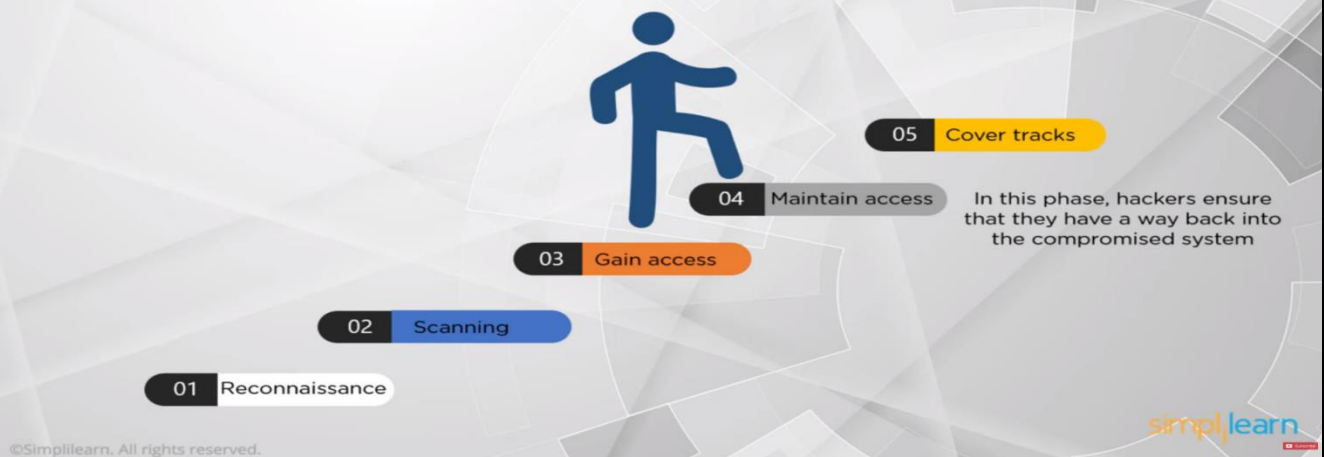
Image of session

Types of hackers

Black hat 	Grey hat 	White hat 	Suicide hacker 
<p>Individuals with extraordinary computing skills resorting to malicious or destructive activities</p>	<p>Individuals who work both offensively and defensively at various times</p>	<p>Individual professing hacker skills and using them for defensive purposes and also known as Security analyst</p>	<p>Individuals who aim to bring down critical infrastructure for a cause and are not worried about facing jail terms or any other punishment</p>

©Simplelearn. All rights reserved.

Phases of ethical hacking



Report:**Career and growth ladder in ethical hacking:**

As per the 2018 Hacker One report, internet users are already facing over 166,000 registered hackers. With stringent cyber laws, governments and various organizations are trying to make the internet a healthy place for its users.

Ethical hackers are those professionals who choose hacking methods to serve a greater purpose in the world with a good intent to benefit others. This guide is for those:

- With basic or no knowledge of ethical hacking
- With limited experience and waiting for an opportunity in ethical hacking

This guide will lead you through the beginner knowledge of ethical hacking, later acquiring expertise in the domain. One of the important requirements to become an ethical hacker would be your desire and intent to make a difference in the world.

If you want to try your hand at cybersecurity, then you must know that it is a vast industry with numerous domains such as application security, network security, and digital forensics which is sometimes further classified into other branches. So, you should be aware of your interest before you take your first step toward the industry. But if you have already made up your mind to become an ethical hacker, then stay with us.

Reasons to choose ethical hacking as career:

Ethical hackers always have a handful of roles and responsibilities to deal with. An ethical hacker not only safeguards the data and network of an organization but is also responsible for taking preventive measures to avoid a security breach via penetration testing or any other method. It does possess a great career scope. And, the salary package is another fascinating aspect of it. However, if you are still unsure of pursuing ethical hacking as a career, then the listed reasons will serve as food for thought.

1. **Scope for Career with Amazing Salary Trends:** The updated 2019 report by PayScale suggests the average salary of a certified ethical hacker is to be \$90k. The top employers of these certified hackers include:

- Booz, Allen, and Hamilton
- S. Army
- S. Air Force
- General Dynamics Information Technology Inc.

The scope for this career route is broadening with each passing year. It has been evidently noticed that government agencies (military, law enforcement department, and national intelligence departments) and private organizations both are hiring cybersecurity experts, though IT firms are primary recruiters of ethical hackers, usually under the title of a penetration tester, security analyst, cybersecurity engineer, network security administrator, and a few others. Apart from that, service providers like airlines, hotels, and financial institutions are also hiring certified ethical hackers to protect their sensitive data.

2. **Growing Job Market for Certified Ethical Hackers:** Job lift, a UK-based job search platform, reported in 2018 that there are around 3240 job vacancies for ethical hackers. The report analyzed data for the past 24 months and declared that these job vacancies are increasing at an average of 4% per month. Another interesting calculation of the same platform mentions that 7 of every 10 job vacancies are looking for candidates with accredited credentials.

3. **Perfect Way to Enter Other Domains of Cybersecurity:** An ethical hacker possesses thorough knowledge of network security, application security, information security, and a lot more. There are organizations looking for professionals with specialized knowledge making it convenient for certified ethical hackers to take up other cybersecurity jobs, too, such as:

- Network administrator/manager
- Security investigator
- Penetration tester
- Web security administrator/manager
- Data security analyst/specialist

- Computer/digital forensics investigator
- IT security administrator/consultant/manager
- Network defense technicians

Program Relevance:

Cybercrimes have cost the world \$2 trillion so far in 2019, according to recent research. Cybersecurity Ventures predicted in 2017 that damages would hit \$6 trillion by 2021, prompting global spending of roughly \$10 billion in cyber-security measures by 2027 to protect against these catastrophic losses.

But it's not just the big companies and organizations that get hit. Average, everyday consumers experience phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses. For instance, it takes just five minutes to hack an internet-connected device, which includes your smartphone, smartwatch, on-board automobile computer, smart television, and home control systems, according to a Netscout report.

This means the more we rely on the internet, the more we need good cybersecurity in all its forms. But first, let's see what we're up against.

The Different Forms of Cybersecurity Threats:

When it comes to infiltrating your system, hackers have an entire toolbox worth of tricks at their disposal. For instance:

Denial-of-service (DoS) Attacks:

Hackers flood a network with requests to exhaust bandwidth. In many cases, DoS attacks are meant to be more of a nuisance than anything else.

Man-in-the-middle (MitM) Attack:

This attack happens when hackers insert themselves into a two-party communication. Once they're in, they can steal data.

Phishing Attacks:

Phishing uses fake emails and text messages to get people to give hackers access to private information. It is one of the most regular attacks, especially against the general public.

Malware:

This attack method is broken down into spyware, ransomware, worms, and viruses. Emails or downloads usually deliver these attacks from suspicious sites.

SQL Injection Attack:

Hackers insert malicious code onto an SQL-using server, usually via a vulnerable website search box. Once carried out successfully, the attack lets the hacker see information otherwise kept off-limits.

Password Attack:

Just what it sounds like. Hackers try to crack a password, usually a poorly chosen one and gain network entry.

Considering the dizzying number of cyber-attacks mentioned previously, you can see the importance of employing active cybersecurity measures. Fortunately, there are many useful cybersecurity methods that you can practice both at home and at work. Keep these in mind, and you'll reduce the likelihood of having a cybercrime on your hands.

Practice Good Password Selection:

Do you still have a "password" as your default password? If so, then shame on you! The ideal strong password is between 8 and 12 characters and includes upper- and lower-case letters, at least one number, and a unique character (such as !?, @). Don't use simple passwords, and don't use anything based on easy to find information about yourself.

Keep Your Wi-Fi Secure:

Speaking of passwords, don't forget to protect your Wi-Fi network. Use WPA2 (Wi-Fi Protected Access version 2) for your security method.

Install Antivirus Software:

Fortunately, many internet providers bundle in some halfway decent antivirus software with their service. If your provider doesn't, then pick up something from Norton, McAfee or Symantec; it's not expensive, and it'll pay for itself in the long run. Also, when you install the program, make sure it's running.

Avoid Suspicious Emails and Texts:

Don't recognize the email address or the phone number of the text sender? Don't open it up, don't reply. Don't do anything other than deleting it! Many of these are the opening gambit in a phishing scam or identity theft attempt.

Use Firewalls and Encryption:

Firewalls help regulate network traffic, both inbound and outbound. That includes blocking off certain sketchy websites. Encryption is essential if you're dealing with financial transactions, especially if you're a business owner. Encryption software scrambles the data so that even if the information falls in the wrong hands, it's useless unless the crooks also have access to the encryption key.

Don't Lose Track of Mobile Devices:

One of the easiest yet most successful ways for hackers to get into your network is to just physically grab your laptop, tablet, or smartphone and log in. That's why you should always make sure your devices never leave your sight when you go out. Never leave them unattended in public or alone with people you don't know or trust. Furthermore, don't forget to lock them with strong passwords.

Practice Good Bluetooth and GPS Usage:

Hackers can penetrate your system by using your GPS or Bluetooth connection. Your GPS lets people know where you are, so turn it off if you don't need it. The same goes for Bluetooth; hackers can use it to gain access to your phone.

Take Courses Related to Cyber-Security:

The more you know about cybersecurity, the more secure you can make your network, and the greater the peace of mind you will have. There are a host of online courses you can take to become better informed.