TASK
1

ETHICAL HACKING AND CYBER SECURITY

BY:ST#IS#3235

CONTENTS:

BASIC TERMINOLOGIES

Vulnerabilities: faults in a software which are used to enter into the system.

Exploit: it is a piece of code which is used to attack the vulnerability .

Bot: it is an automated program which performs continuous attack on □(TARGET).

Backup: To store data in a secured way for future use in case if the data is missed.

Adware: It is a piece of code which displays ads on the web pages.

Anti-virus software: It is used to protect the system from virus and other mal wares.

Backdoor: It is a bypassing method of gaining access on computer without knowing to the user.

Broadband: It is a high speed network where the communication is shared between multiple users.

BYOD: It means "bring your own device" for security purposes.

Bug: it is an error or fault on a computer program that may cause different behaviour of the system.

Cache memory: It is a type of fast memory which stores the frequently searched data

Cookie: They are small files which are stored on a users computer.which are used to track sessions.

Cyber warfare: It is a cyber attacks between one nation to another to steal data and information.

Firewall: It is a piece of software that protects system from internet attacks.

Malware: It is used to attack the users system or server or computer network.

Phishing: It is a method of gathering person information through using spoofing.

Ransomware: It is a type of software used to block the users system until a sum of amount is paid.

Pen testing: hacking the users system with their permission.

Social Engineering: It is a type of manipulation technique to gather others information.

Spyware: It is a type of software it installs itself on a device and observers users actions.

Virus:A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

DIFFERENT TYPES OF CERTIFICATIONS

1. Certified Information Systems Security Professional (CISSP)

The CISSP certification from the cybersecurity professional organization (ISC)² ranks among the most sought-after credentials in the industry. Earning your CISSP demonstrates that you're experienced in IT security and capable of designing, implementing, and monitoring a cybersecurity program.

2. Certified Information Systems Auditor (CISA)

This credential from IT professional association ISACA helps demonstrate your expertise in assessing security vulnerabilities, designing and implementing controls, and reporting on compliance. It's among the most recognized certifications for careers in cybersecurity auditing.

3. Certified Information Security Manager (CISM)

With the CISM certification, also from ISACA, you can validate your expertise in the management side of information security, including topics like governance, program development, and program, incident, and risk management.

4. CompTIA Security+

CompTIA Security+ is an entry-level security certification that validates the core skills needed in any cybersecurity role. With this certification, demonstrate your ability to assess the security of an organization, monitor and secure cloud, mobile, and internet of things (IoT) environments, understand laws and regulations related to risk and compliance, and identify and respond to security incidents.

5. Certified Ethical Hacker (CEH)

Ethical hacking, also known as white hat hacking, penetration testing, or red team, involves lawfully hacking organizations to try and uncover vulnerabilities before malicious players do. The EC-Council offers the CEH Certified Ethical Hacker certification. Earn it to demonstrate your skills in penetration testing, attack detection, vectors, and prevention.

6. GIAC Security Essentials Certification (GSEC)

This certification from the Global Information Assurance Certification (GIAC) is an entry-level security credential for those with some background in information systems and networking. Earning this credential validates your skills in security tasks like active defense, network security, cryptography, incident response, and cloud security.

7. Systems Security Certified Practitioner (SSCP)

With this intermediate security credential from (ISC)², you can show employers that you have the skills to design, implement, and monitor a secure IT infrastructure. The exam tests expertise in access controls, risk identification and analysis, security administration, incident response, cryptography, and network, communications, systems, and application security.

8. CompTIA Advanced Security Practitioner (CASP+)

The CASP+ is designed for cybersecurity professionals who demonstrate advanced skills but want to continue working in technology (as opposed to management). The exam covers advanced topics like enterprise security domain, risk analysis, software vulnerability, securing cloud and virtualization technologies, and cryptographic techniques.

9. GIAC Certified Incident Handler (GCIH)

Earning the GCIH validates your understanding of offensive operations, including common attack techniques and vectors and your ability to detect, respond, and defend against attacks. The certification exam covers incident handling, computer crime investigation, hacker exploits, and hacker tools.

10. Offensive Security Certified Professional (OSCP)

The OSCP from Offensive Security has become one of the most sought-after certifications for penetration testers. The exam tests your ability to compromise a series of target machines using multiple exploitation steps and produce detailed penetration test reports for each attack.

TYPES OF HACKER

White Hat Hackers: White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity.They work under the rules and regulations provided by the government, that's why they are called Ethical hackers or Cybersecurity experts.

Black Hat Hackers: They are often called Crackers. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.

Gray Hat Hackers: Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers.

Script Kiddies: They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites.

Green Hat Hackers: They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers.

Blue Hat Hackers: They are much like the script kiddies; are beginners in the field of hacking. If anyone makes angry a script kiddie and he/she may take revenge, then they are considered as the blue hat hackers.

Red Hat Hackers: They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate.

State/Nation Sponsored Hackers: State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country.

Hacktivist: These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.

Malicious Insider or Whistleblower: A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

Password Policy:

The concept of username and passwords has been a fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity. The purpose of this policy is to determine a typical for the creation of strong passwords, the protection of these passwords, and therefore the frequency of change password must be followed.

Special access policy :

It defines a special access , a user can go anywhere and do anything until he had the special access policy.special Access Policy This policy provides a set of requirements for the regulation of special access use on the Montana Tech Computer System. This policy will provide a mechanism for the addition and removal of people from the special access database and a mechanism for periodic reviews of the special access status.

E-Mail Policy:

Email security may be a term for describing different procedures and techniques for shielding email accounts, content, and communication against unauthorized access, loss, or compromise. Email is usually wont to spread malware, spam, and phishing attacks. Attackers use deceptive messages to entice recipients to spare sensitive information, open attachments, or click on hyperlinks that install malware on the victim's device.

Access control policy:

The purpose of this policy is to stipulate the suitable use of computer devices at the corporate/company. These rules protect the authorized user and therefore the company also. Inappropriate use exposes the corporate to risks including virus attacks, compromise of network systems and services, and legal issues.

Data encryption policy:

The goal of an encryption policy is to encrypt data at the requisite times. For instance, IPSec and SSL provide encryption when data travels across a network but do little to protect data stored on disk or in a database. Similarly, encrypted fields in a database do nothing to protect information as it is accessed across the network.

THE END