Sathwik Admin

SathwikAdmin101409_EH AAT-1

My Files
My Files
University

Document Details

Submission ID
trn:oid:::3618:101024806

Submission Date
Jun 15, 2025, 10:47 PM GMT+5:30

Download Date
Jun 15, 2025, 10:50 PM GMT+5:30

File Name
SathwikAdmin101409_EH AAT-1.pdf

File Size
589.8 KB

13 Pages

1,984 Words

10,631 Characters

4% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- **9** Not Cited or Quoted 4%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

3% Internet sources
1% Publications
4% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **9** Not Cited or Quoted 4%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 3% Internet sources
- 1% Publications
- 4% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	University of Wales, Lampeter on 2025-04-25 <1%
2	Internet	www.zubairalexander.com <1%
3	Submitted works	University College Birmingham on 2025-05-07 <1%
4	Submitted works	Arab Open University on 2024-11-08 <1%
5	Internet	examnotes.net <1%
6	Internet	www.ipindia.nic.in <1%
7	Submitted works	University of Westminster on 2025-05-14 <1%

INSTITUTE OF AERONAUTICAL ENGINEERING

AN ASSIGNMENT REPORT OF

ETHICAL HACKING

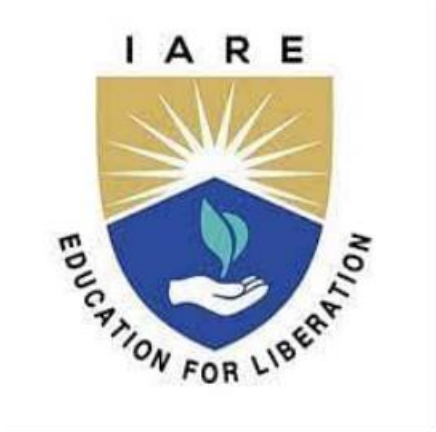
COURSE CODE-ACCD02

BY

VALGUNDAWAR SATHWIK

23951A62C8

CSE-CYBER SECURITY



6

INSTITUTE OF AERONAUTICAL ENGINEERING

DUNDIGAL, HYDERABAD-500 043, TELANGANA, INDIA.

1.Discuss about mitigation of hacking types

Ans)

1. Phishing – “They Pretend to Be Someone You Trust”

This is like someone calling you and pretending to be your bank or a friend to trick you into giving your password or clicking a fake link.

What you should do :If something feels off in a message or email, it probably is .Don’t click on links just because they look official — especially if they’re asking for passwords or money .If a message says “your account is blocked” or “urgent action needed” — pause and breathe. Go to the website yourself instead of clicking anything .Set up 2-step verification. It’s like a second lock on your front doo

2. Malware – “Sneaky Stuff That Gets in and Messes Things Up”This is like letting someone into your house who steals your stuff while you’re sleeping. You accidentally download malware from shady apps, dodgy websites, or even a bad USB.

What you should do: Don’t download random apps or files — especially if they sound too good to be true (like “free Netflix forever”).Keep your phone, laptop, and antivirus updated those little updates fix big problems.

Back up your important files (like photos and documents) just in case something goes wrong.

3. Password Hacking – “They Just Keep Guessing Until They Get It Right”

Hackers try a bunch of passwords over and over — or worse, use one leaked from another site you used the same password on.

What you should do :Use a strong password that’s hard to guess — like a phrase or sentence.

Example: “MangoLassi@3PM!” is better than “password123”.

Don’t use the same password for everything (yes, we’ve all done it).Use a password manager — it remembers everything for you.Turn on 2-factor authentication. It’s a small step that makes hacking a lot harder

2.Explain about importance of ethical hacking

Ans)

1. They Protect What Matters

Imagine someone trying to sneak into your home—but it’s not to steal anything. It’s your friend checking if your door lock is weak so you can fix it. Ethical hackers do that—but for your Instagram, your bank account, your personal info.

2. They Keep the Bad Guys Out

Cybercriminals are clever. They’re always looking for ways to steal data or cause chaos. Ethical hackers try to think like them, so they can stop them before the damage is done.

3. They Help Keep Life Going

When companies get hacked, everything can crash—apps stop working, hospitals lose data, even flights can be delayed. Ethical hackers help stop those disasters before they even happen.

4. They Make Us Feel Safe

When you know someone’s out there making sure things are secure, you feel more confident, right? Ethical hackers give us that sense of safety in an online world we can’t live without.

3.List out common malware attacks and their characteristics

1. Virus

Nature: Attaches itself to clean files or programs.

Spread: Activates when the host file runs.

Effects: Can corrupt or delete data, slow down systems, or cause total failure.

2. Worm

Nature: Standalone software.

Spread: Self-replicates and spreads across networks without human action.

Effects: Consumes bandwidth, crashes systems, or creates backdoors.

3. Trojan Horse

Nature: Disguised as legitimate software.

Spread: Requires the user to install it.

Effects: Provides backdoor access, steals data, or downloads additional malware

4. Ransomware

Nature: Encrypts user data.

Spread: Through malicious attachments, links, or exploits.

Effects: Demands payment (usually in cryptocurrency) to unlock files.

5. Spyware

Nature: Secretly gathers user information

Spread: Often bundled with free software or via malicious ads.

Effects: Tracks activities, steals credentials, and may result in identity thef

6. Adware

Nature: Displays unwanted ads.

Spread: Bundled with freeware or malicious downloads.

Effects: Slows down systems and invades user privacy.

4.Describe some certifications and skills needed for ethical hackers

Ans)

Top Certifications for Ethical Hackers

1. CEH (Certified Ethical Hacker)

Offered by: EC-Council

Focus: Hacking tools, techniques, and methods used by real hackers.

Why it's useful: It's one of the most recognized certifications in the cybersecurity world.

2. OSCP (Offensive Security Certified Professional)

Offered by: Offensive Security

Focus: Hands-on penetration testing.

Why it's useful: Known for its difficulty—it proves you can hack under pressure.

3. CompTIA Security+

Offered by: CompTIA

Focus: Basics of security, network attacks, and risk management.

Why it's useful: Great for beginners stepping into cybersecurity.

4. CISSP (Certified Information Systems Security Professional)

Offered by: ISC²

Focus: Advanced security strategy and management.

Why it's useful: Ideal for experienced professionals in security leadership roles.

Essential Skills Every Ethical Hacker Needs

1. Networking Knowledge

Understand how computers communicate (TCP/IP, firewalls, routers).

Helps identify how attackers move through networks.

2. Operating Systems (Linux, Windows, macOS)

Hackers often use Linux tools (like Kali Linux), and many exploits target Windows.

3. Programming Skills

Common languages:

Python (automation, scripting)

JavaScript (web vulnerabilities)

5.How osint framework provides information gathering

What is OSINT Framework?

Imagine you're a detective—but instead of sneaking around, you use the internet to find clues. The OSINT framework is like your organized toolkit. It helps you find public information that’s already out there on the web—like social media posts, website details, leaked data, or even where a photo was taken.

How It Helps with Information Gathering:

1. Everything in One Place:

It brings together tons of online tools.

You don’t need to Google everything—you just click through categories (like “email,” “social media,” “phone numbers”) and it shows you tools to use.

2. Step-by-Step Clues:

You start with one small detail (like a name or email).

Then you follow links and tools to uncover more, like a puzzle unfolding.

3. No Hacking Involved:

You’re not breaking into anything.

OSINT only finds info that people or websites have already made public—like LinkedIn profiles, old blog posts, or leaked data online.

4. Tracks a Lot of Things:

You can search for people, websites, phone numbers, usernames, locations, and more.

6.Describe various types of trojan malware

Ans)

1. Backdoor Trojan

Purpose: Gives hackers remote access to your device.

What it does: Lets attackers control your system, steal files, install more malware, or even spy on you.

Example: A fake software installer that opens a hidden door into your system.

2. Downloader Trojan

Purpose: Downloads and installs other malware.

What it does: Acts like a delivery guy—it sneaks into your device, then fetches other malware like ransomware or spyware.

Example: Comes hidden inside pirated software or suspicious attachments.

3. Banking Trojan

Purpose: Steals your financial information.

What it does: Watches what you type or redirects you to fake banking pages to steal login details.

Example: Fake banking apps or links that mimic your bank's website.

4. Remote Access Trojan (RAT)

Purpose: Full control over your system from a distance.

What it does: Hackers can view your screen, control your mouse, activate your webcam, and more.

Example: Often spread through phishing emails or fake software.

5. Spyware Trojan

Purpose: Secretly spies on your activities.

What it does: Tracks what you type, sites you visit, or collects passwords.

Example: Can come bundled with "free" tools or mobile apps.

6. Rootkit Trojan

Purpose: Hides other malware so it's hard to detect.

What it does: Makes sure other viruses stay hidden deep in your system.

Example: Can disguise keyloggers or ransomware by modifying system files.

7.Discuss how sniffing attacks work for hackers

Ans)

What is a Sniffing Attack?

A sniffing attack is when a hacker secretly "listens in" on network traffic—like eavesdropping on a conversation between two people. The hacker captures data being sent over a network and then analyzes it to steal sensitive information like:Passwords,Emails,Credit card numbers,Login sessions

How Hackers Perform Sniffing Attacks:

1. Network Access

First, the hacker connects to the network—either by physically plugging in or joining a Wi-Fi network (like public Wi-Fi at a café).

If the network isn’t secured properly, they’re in.

2. Packet Sniffing Tools

Hackers use tools like Wireshark, Tcpdump, or Cain & Abel to capture data packets.

These tools allow them to see the raw data flowing through the network, like usernames, search history, or even live messages—especially if the data isn’t encrypted.

3. Promiscuous Mode

On normal systems, a network card only reads data meant for it.

Hackers switch the network interface to promiscuous mode, which means it starts capturing everything, even traffic not meant for them.

4. Reading the Traffic

Once the data is captured, the hacker looks through it for anything useful:

Unencrypted passwords

Login sessions

Browsing activity

8.Explain how to defend against password cracking of systems

Ans)

How to Defend Against Password Cracking:

1. Use Strong Passwords

Long (at least 12 characters)

Mix of uppercase, lowercase, numbers, and symbols

Avoid names, birthdays, or real words

2. Enable Account Lockout Policies

Lock the account after a certain number of failed login attempts (e.g., 5 tries).

This stops brute-force attacks dead in their tracks.

3. Use Multi-Factor Authentication (MFA)

Even if someone gets your password, they need a second form (like a code on your phone).

Tools: Google Authenticator, Authy, Microsoft Authenticator

4. Hash Passwords (Securely)

Systems should never store raw passwords.

Use strong hashing algorithms like bcrypt, scrypt, or Argon2.

These slow down cracking tools and make leaks less dangerous.

9.Demonstrate the steps to building cyber security strategy

Steps to Building a Cybersecurity Strategy:

1. Understand What You're Protecting (Asset Identification)

First, figure out:

What systems do you use?

What data is sensitive (customer info, passwords, money, etc.)?

What would hurt most if stolen or damaged?

Example: Identify all computers, servers, cloud services, and critical data.

2. Assess the Risks

Ask:(What are the most likely threats? (Hackers, malware, insider threats, etc.)What are your weak points? (Outdated software, weak passwords, open ports?)

Tools like vulnerability scanners or audits can help here.

3. Set Clear Security Goals

Decide what you want to achieve:

Prevent unauthorized access

Protect customer data

Detect and respond to attacks quickly

This guides the whole plan.

4. Define Policies and Rules

Create guidelines for how things should be done:

Strong password policies

Who gets access to what (access control)

Rules for using personal devices (BYOD)

These policies are like the “house rules” for your digital environment.

10.Explain about trojan horse working process

Ans)

Working Process of a Trojan Horse: Step-by-Step

1. Disguised Entry:The Trojan comes disguised as a legitimate-looking file or program.You might download it from a fake website, open it from an email attachment, or install it thinking it’s a free app or update.

Example: A file named FreeMoviePlayer.exe might really be a Trojan.

2. User Installs or Runs the File:

Trojans don’t spread on their own—they need you to install or open them.Once you run the file, the malicious code activates silently in the background.

3. Silent Execution:

The Trojan starts running its hidden functions without alerting the user.It may do things like:Open a backdoor to let hackers in,Steal your passwords,Log your keystrokes (keylogger),Download more malware

,Spy through your webcam or mic

4. Communication with Hacker (Command & Control):

Many Trojans connect to the hacker’s remote server (called a C&C server).They wait for instructions—like:Send stolen data

Install ransomware,Join a botnet to attack other systems

5. Data Theft or Damage Begins:

The Trojan may start:Copying your files,Watching what you type,Encrypting your data (in case of ransomware),Slowing your system or crashing it,And the worst part? You might not even notice anything wrong—until it’s too late. Example in Real Life:

1. You get an email that says, “Here’s your invoice. Please review.”
2. You open the attached .doc file and enable macros.
3. That macro runs a Trojan in the background.