Rushi Admin

RushiAdmin102536_EH AAT2

My Files

My Files

University

Document Details

Submission ID

trn:oid:::3618:101026401

Submission Date

Jun 15, 2025, 10:56 PM GMT+5:30

Download Date

Jun 15, 2025, 10:59 PM GMT+5:30

File Name

RushiAdmin102536_EH AAT2.pdf

File Size

211.1 KB

11 Pages

3,184 Words

15,961 Characters

3% Overall Similarity

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

Match Groups

- **8** Not Cited or Quoted 3%
  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

0% Internet sources
1% Publications
3% 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

- **8** Not Cited or Quoted 3%
  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

- 0% Internet sources
- 1% Publications
- 3% 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	Liverpool John Moores University on 2024-03-06 <1%
2	Submitted works	Lakes College - West Cumbria on 2025-02-13 <1%
3	Submitted works	AlHussein Technical University on 2025-06-11 <1%
4	Submitted works	Community College System of New Hampshire on 2024-12-10 <1%
5	Publication	Fadele Ayotunde Alaba, Alvaro Rocha. "Chapter 2 Cyber Attacks", Springer Scienc... <1%
6	Internet	www.ipindia.nic.in <1%
7	Submitted works	University of Ghana on 2024-11-10 <1%

INSTITUTE OF AERONAUTICAL ENGINEERING

AN ASSIGNMENT REPORT OF

ETHICAL HACKING

COURSE CODE-ACCD02

BY

N. RUSHWITHA

23951A62A5

CSC-B

INSTITUTE OF AERONAUTICAL ENGINEERING

DUNDIGAL , HYDERABAD-500 043, TELANGANA, INDIA.

1. Impersonation on social networking sites?

Ans) Impersonation on social media is when someone pretends to be you or someone else by creating a fake account. They might copy your name, use your profile photo, and even take your personal information just to make the account look real. This might sound like a joke or prank, but it can actually be really harmful.

People impersonate others online for different reasons. Some might do it just to mess around, but others have more serious intentions like scamming people, spreading false rumors, or damaging someone's reputation. Imagine waking up one day and finding out someone is pretending to be you online—messaging your friends, posting things you never said, or asking for money in your name. It's not just creepy, it's dangerous too.

The scary part is that these fake accounts can look almost identical to real ones. So your friends or family might believe it's actually you. That's why impersonation can break trust, confuse people, and sometimes even lead to legal issues.

Thankfully, most social media platforms now allow you to report fake accounts. If you ever see someone pretending to be you or someone you know, you can report the profile, and the platform will usually take it down after reviewing it. It's also a good idea to keep your own account secure by using strong passwords, turning on two-factor authentication, and avoiding the sharing of too much personal info online.

Impersonation online isn't just a silly prank—it can seriously affect someone's life. Being aware and careful helps you stay protected in today's digital world

2. Explain types of footprinting.?

Ans)

---

3 Footprinting is like digital detective work. It's the process of gathering as much information as possible about a target system, network, or person—usually as a first step before a cybersecurity test or attack. Think of it as the research phase where someone tries to learn everything they can without actually interacting with the system directly. This step is important for ethical hackers, but it’s also a method used by attackers who want to plan out their next move. There are mainly two types of footprinting: passive and active.

Passive footprinting is all about quietly collecting information without alerting the target. In this type, the person gathering the data doesn't directly connect to the target system. Instead, they rely on public sources like websites, social media profiles, online forums, job postings, or even old press releases. For example, someone might look at a company’s LinkedIn page to find out what software they use, or they might scan WHOIS records to get domain registration info. Since there’s no direct contact, passive footprinting is harder to detect, which makes it sneaky but also useful for ethical hacking.

Active footprinting, on the other hand, is more direct. Here, the attacker or tester interacts with the target system to collect information. They might ping the network, perform traceroutes, or run port scans. These actions help them learn about IP addresses, open ports, services running, or even firewall details. Because active footprinting touches the target network directly, it can often be detected by security systems and alerts. That makes it riskier, but it also provides more detailed data.

Both types are often used together. First, someone gathers as much as they can passively to avoid raising suspicion. Then, if needed, they move on to active methods to fill in the gaps. Whether done by ethical hackers or malicious attackers, footprinting is a powerful way to understand a target—and knowing how it works is the first step in protecting against it.

3. Stages of footprinting?

3 Ans) Footprinting is the process of gathering information about a target, and like any proper investigation, it happens in stages. These stages help someone, whether an ethical hacker or a cybercriminal, slowly build a picture of the target system, network, or person. It's like piecing together clues before deciding how to move forward.

The first stage is information gathering. This is where the person starts collecting all the basic, public data about the target. They might look up the company's website, find employee names on LinkedIn, or use search engines to see what kind of technology is mentioned in blogs or job postings. This stage is all about being quiet and unnoticed, gathering as much useful info as possible without interacting with the target directly.

Next comes the determination of network range. Now the focus shifts toward understanding the scope of the target's digital presence. This means finding out the IP address range the target uses, checking which domains they own, or what servers they run. This helps narrow down the space that needs to be analyzed or attacked later.

Then we move into identifying active machines. Once the network range is known, the person tries to find out which machines or systems are actually up and running. This usually involves pinging different IP addresses or scanning the network to see what responds. This gives a clearer picture of what's online and potentially vulnerable.

After that, it's time for port and service detection. The goal here is to see which doors, or ports, are open on those machines and what kind of services are running behind them. For example, is a web server running? Is there a file-sharing service active? This information helps the person figure out how the system is being used and what might be weak.

Finally, there is OS and system information fingerprinting. This stage digs deeper to figure out which operating system the machine is using, like Windows, Linux, or Mac, and even which version. That's important because different systems have different vulnerabilities. Knowing the system details makes it easier to plan the next steps.

4. Role of Hypertext Transfer Protocol HTTP in web services?

Ans) The Hypertext Transfer Protocol, or HTTP, plays a huge role in how we experience the internet today. It's basically the language that web browsers and servers use to talk to each other. Whenever you open a website, click a link, submit a form, or watch a video online, HTTP is working behind the scenes to make sure everything gets to you properly.

HTTP acts like a messenger. When you type a web address into your browser, your device sends a request to the website's server using HTTP. The server then replies with the content you asked for—like a webpage, an image, or a video. This back-and-forth communication happens very quickly, and it all relies on HTTP to make sure the messages are understood clearly.

In web services, HTTP does more than just show you websites. It also allows different applications and systems to connect and exchange data, even if they are built in different languages or hosted on different platforms. For example, when a weather app pulls data from a weather server, or when a payment gateway processes your order, HTTP is the protocol making that exchange possible. It helps developers create systems that can talk to each other smoothly.

One of the best things about HTTP is that it's stateless. This means that every time a request is made, it doesn't remember past interactions. While this might sound like a limitation, it actually helps web services scale better and handle more users at once. To manage information across sessions, things like cookies or tokens are used alongside HTTP.

In summary, HTTP is like the digital handshake that keeps the web connected. It makes sure that your browser and web services can communicate clearly and reliably, making the internet experience seamless and interactive for all of us

5. How to install anti-theft software on mobile phone?

Ans) Imagine you're opening your favorite website on your phone or laptop. As soon as you hit enter, something important happens behind the scenes—your browser starts talking to the website's server using something called HTTP, or Hypertext Transfer Protocol. It's kind of like a language or set of rules that helps devices communicate on the web. Without it, websites simply wouldn't load.

HTTP's job is pretty simple but powerful. It sends your request to a server (like when you click on a webpage), and the server responds by sending back the content you asked for, such as text, images, or videos. It's this smooth back-and-forth communication that makes browsing the internet feel instant and easy.

But HTTP isn't just for viewing websites. It's also how apps and services talk to each other behind the scenes. For example, when a weather app shows your local forecast, or when an online store processes your payment, it's HTTP that's helping those systems connect and exchange data. It allows different platforms—no matter how they were built—to work together.

One interesting thing about HTTP is that it doesn't remember your past activity. Every time you visit a webpage, it treats it like a fresh request. This helps websites run faster and handle more people at once, but when needed, things like cookies or tokens are added to help remember who you are.

So in simple terms, HTTP is like the invisible delivery guy of the internet. It picks up your requests, brings back exactly what you asked for, and keeps everything running smoothly. Without it, the web wouldn't work the way we know it today.

6. Wireless intrusion prevention system WIPS?

Ans) Whenever we browse the internet, click on a link, or open a website, something really important happens in the background—even if we don't see it. That something is called **HTTP**, or **Hypertext Transfer Protocol**. It might sound technical, but it's actually the reason websites and web services work as smoothly as they do.

Think of HTTP as the middleman between your browser and the web server. When you type in a website address or click a link, your browser sends out a request saying, "Hey, can I have this page?" The server receives that request, finds the page or data, and sends it back to your screen. All of this happens in just seconds, and it's HTTP that makes this conversation possible.

But HTTP doesn't just help with websites—it's also how different apps and online services talk to each other. For example, when your weather app shows you the forecast, it's actually using HTTP to ask a server for the latest data. Or when you place an order online, the details go back and forth between your browser, payment system, and seller's site using HTTP.

One of the unique things about HTTP is that it doesn't keep track of previous requests—it treats every new interaction like it's the first one. That helps websites respond faster and manage more people at once. And if something needs to be remembered, like a login or shopping cart, websites use cookies or sessions alongside HTTP to keep track of you.

In simple terms, HTTP is what keeps the web connected. It's the reason you can load a blog, stream a video, or use a web app without thinking twice. It quietly handles the communication between your device and the online world, making the internet experience feel smooth, fast, and effortless

5

7. Understanding the Cisco Adaptive Security Appliance Firewall?

Ans) The Cisco Adaptive Security Appliance, or ASA for short, is one of the most trusted tools for protecting computer networks. Think of it like a highly trained security guard for your digital space. Its job is to monitor everything that comes in and goes out of a network, making sure only the right data gets through while keeping the harmful stuff out.

Cisco ASA is more than just a basic firewall. It's actually a combination of several security tools rolled into one device. At its core, it blocks unwanted traffic and prevents unauthorized access—just like any good firewall. But it also includes extra features like VPN support, intrusion prevention, and content filtering, which means it offers a full package of protection for businesses and organizations.

One of the key things about Cisco ASA is that it's adaptable. That's even part of its name—Adaptive Security Appliance. It adjusts to different needs and can handle both small office networks and large enterprise systems. Whether a company has just a few computers or hundreds, the ASA can scale its protection accordingly.

Let's say someone tries to access private company data from the outside. The ASA firewall can detect that this isn't normal behavior and immediately block the attempt. If someone inside the company accidentally clicks a suspicious link, the ASA can inspect that traffic and stop any harmful content from spreading. And if employees need to access work files from home, the ASA also supports secure VPN connections to make that possible safely.

In short, Cisco ASA is a powerful, all-in-one firewall solution that keeps networks safe from attacks, both from outside threats and internal mistakes. It's reliable, flexible, and smart enough to handle modern cybersecurity challenges without slowing down the network. That's why it's widely used by businesses around the world.

8. Network Address Translation process?

Ans) Have you ever wondered how all your devices like your phone, laptop, or even your smart TV connect to the internet at the same time using just one Wi-Fi connection? That's made possible by something working quietly in the background called Network Address Translation or NAT.

Let's imagine your home as a little neighborhood. Inside this neighborhood, every device has its own unique house number which we call a private IP address. These addresses are only recognized within your local network and they don't work outside your home. But the internet is like a big city that only recognizes public addresses. So how do your devices communicate with the internet if their addresses aren't even visible? That's where NAT steps in.

NAT lives in your router and acts like a helpful receptionist. When your device wants to visit a website or watch a video online, NAT changes the private address to a public one, sends the request out to the internet, and waits for a reply. When that reply comes back, NAT knows exactly which device asked for it and sends it to the right place. It's like sorting the mail, making sure each package reaches the correct door.

This system is super useful because the world doesn't have enough public IP addresses for every single device. NAT allows multiple devices to share one public IP address while keeping everything organized and working smoothly. It also adds a bit of privacy and protection because devices from the outside world can't directly access your private network, they have to go through NAT first.

So even though we don't see it happening, NAT is always there, quietly making sure that all your online activities stay connected, safe, and simple

9. Understanding Honeypots?

Imagine setting a trap—not to catch someone and punish them, but to understand how they think and what they're planning. That's basically what a honeypot does in the world of cybersecurity. A honeypot is a specially designed system that looks like a real computer or server, complete with fake data and weak spots. It's made to attract hackers and trick them into interacting with it. But the goal isn't to stop them right away—it's to quietly observe what they're trying to do.

Now, when we talk about **open-source honeypots**, we're referring to tools that anyone can use, modify, or improve because the code is publicly available. These honeypots are especially helpful for learning and research. Security professionals, ethical hackers, and even students use open-source honeypots to better understand how attackers behave, what tools they use, and which vulnerabilities they try to exploit.

One great thing about open-source honeypots is that they can be set up with relatively low cost and effort. You don't need to be part of a big company or spend a fortune. There are plenty of well-known options like **Cowrie**, which pretends to be a vulnerable SSH server, or **Dionaea**, which is great for catching malware. When someone tries to break into these fake systems, the honeypot records every move they make—just like a hidden camera in a store.

This information helps security teams stay one step ahead. By studying real-world hacking attempts, they can build stronger defenses, fix weak points, and protect real systems more effectively. And since the honeypot isn't connected to any actual sensitive data, there's no real harm done when attackers poke around.

In simple terms, an open-source honeypot is like a decoy that helps us learn. It's not just a fake computer—it's a tool for watching, understanding, and improving cybersecurity. And the fact that it's open-source means the community can come together to keep making it better

10. Best Practices for Protecting Embedded Oss?

Ans) Embedded operating systems are kind of like the quiet workers behind the scenes. They're in our cars, washing machines, medical devices, and even traffic lights. We don't usually notice them, but they're constantly doing their job, keeping everything running smoothly. But just like any part of technology, they can be vulnerable to cyber threats, which means we need to take steps to protect them.

The first step is to keep things simple. These systems are built for specific tasks, so it's best not to overload them with extra features or software they don't need. The more basic the system, the fewer chances there are for something to go wrong or for someone to break in.

Another really important part is updates. We're used to updating our phones or computers when there's a new version available, but we often forget that smart devices need the same attention. If an embedded system is using old software, it might have security gaps that hackers know how to take advantage of. Keeping things up to date helps close those gaps.

Then there's the issue of passwords. A lot of devices come with default login details that are easy to guess. Changing those to strong, unique passwords is a quick and simple way to make your device safer. And if you can use two-factor authentication where you need a password and a second step like a code sent to your phone that's even better.

We should also think about the information these devices handle. Even if it doesn't seem sensitive, encrypting the data helps keep it private and safe from tampering. Encryption basically scrambles the data so only the right person or system can understand it.

Finally, it helps to keep an eye on the device from time to time. Monitoring its activity or checking logs can help spot anything unusual early on before it turns into a serious problem.

At the end of the day, protecting embedded systems doesn't have to be complicated. A few smart habits like keeping things updated, using good passwords, limiting what the system can do, and paying attention can make a big difference. These little systems do a lot for us, so it's only fair we take good care of them too.