Absolutely — I’ll give you the **fully formatted version below** exactly as you’re seeing it now, so you can **copy and paste it directly into Word or Google Docs** with no cleanup needed. The formatting includes clear bullet points, headings, and tables, all designed for **study-readiness** without the need for reformatting.

**🛡️ On-Path Attack – Study Notes (CompTIA A+ 220-1102 Aligned)**

**✅ 1. Concept Overview: What Is an On-Path Attack?**

An **on-path attack** (formerly called **man-in-the-middle**) is when a hacker places themselves **between two devices on a network** to **intercept**, **monitor**, or **alter** the communication **without detection**.

**📘 2. Exam Relevance**

* **CompTIA A+ 220-1102 – Core 2**
* **Domain 2.0: Security**
* **Objective 2.5:** Common threats, vulnerabilities, and attacks

**You must understand:**

* What on-path attacks are
* How they are carried out
* The difference between **replay** and **relay**
* Methods used to insert into traffic
* Risks and defenses

**📋 3. Sentence-by-Sentence Breakdown**

**🔍 Definition of On-Path Attack**

* An on-path attacker **inserts their device into a communication session** between two hosts.
* They **intercept, monitor, and forward** data — all **without detection**.
* Both users (client and server) believe they’re talking directly to each other.

🧠 **Key Point**: The attacker is silently “on the path” between both parties.

**📡 Attacker Positioning in the Network**

* The attacker may be **logically inserted** between devices (e.g., on the same subnet).
* Once in place, they can:
  + **Capture authentication traffic**
  + **Hijack sessions**
  + **Eavesdrop or modify data**

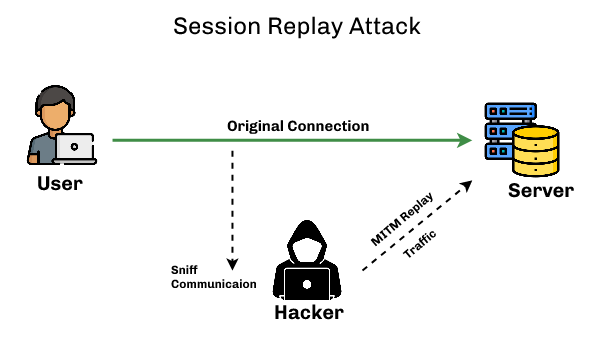
**🧰 Common On-Path Insertion Techniques**

* **ARP poisoning** – Sends false ARP replies to redirect traffic
* **DNS poisoning** – Redirects a domain name to a malicious IP
* **Rogue access point** – Tricks users into connecting to a fake Wi-Fi network
* **Rogue switch/hub** – Connects unauthorized hardware to manipulate traffic flow

**🔁 Replay vs. Relay: Two On-Path Techniques**

**🔄 Replay Attack**

* Attacker **captures valid data**, then **replays it later**.
* Often used to **re-send login credentials** or **session handshakes**.



Example:

An attacker captures a valid login attempt and **replays it** to gain access without a password.

🧠 **Key Point**: The attacker doesn’t change the data — they **re-use it**.

**🔁 Relay Attack**

* Attacker **actively proxies** communication between two users in real-time.
* May **intercept, read, or modify data** before passing it along.

Diagram of a computer network

AI-generated content may be incorrect.

Example:

Attacker sits between a user and a bank, capturing the login while relaying it to the real site — then changing transfer details in the process.

🧠 **Key Point**: The attacker **relays and alters** data between the client and server.

**🔓 Attacker Capabilities**

From the “middle,” an attacker can:

* Capture:
  + Login credentials
  + Bank account numbers
  + Session cookies
* Modify:
  + Redirect payments
  + Inject malware
  + Alter chat messages

**🧩 Summary Table**

| **Concept** | **Explanation** |
| --- | --- |
| **On-path attack** | Attacker silently sits between two hosts and intercepts their communication |
| **Replay attack** | Captured data is replayed without modification |
| **Relay attack** | Attacker proxies and can modify real-time communication |
| **ARP poisoning** | Spoofs MAC-to-IP mapping to reroute traffic |
| **DNS poisoning** | Redirects DNS queries to fake destinations |
| **Rogue access point** | Fake wireless access point used to capture data |
| **Rogue switch/hub** | Unauthorized physical device inserted into the network |

**🧾 4. Exam Inclusion Notification**

✅ **Yes – On-path attacks are directly included in the CompTIA A+ 220-1102 exam** under:

* **Domain 2.0: Security**
* **Objective 2.5: Threats and vulnerabilities**

You may be tested on:

* Identifying on-path attack examples
* Differences between replay and relay
* Common methods of executing them
* Impacts and basic mitigations

Let me know if you’d like this delivered in a downloadable **PDF or DOCX** format — or if you’d like a **follow-up 10-question quiz** to test your knowledge!

Based on your uploaded **On-Path Attack Notes**, here’s a **10-question multiple-choice quiz** crafted in the **style of the CompTIA A+ 220-1102 exam**, specifically targeting:

* **Domain 2.0: Security**
* **Objective 2.5: Threats and attacks**