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**

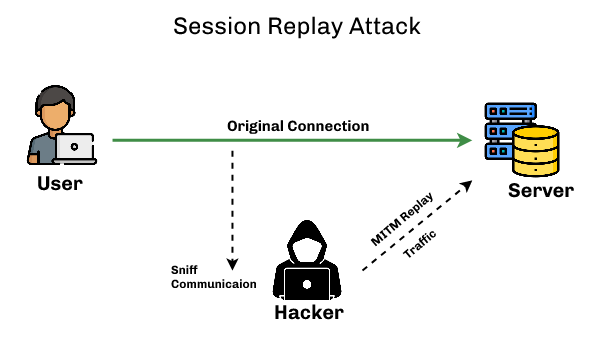
**🧰 Common On-Path Insertion Techniques**

* **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**

**🧪 On-Path Attack Quiz – 10 MCQs (CompTIA A+ Style)**

When you’re done, reply with your answers like this: **1. b, 2. d, 3. a...**

**Question 1 -** What best describes an **on-path attack**?

a) Capturing login attempts using brute force

b) Inserting into a communication channel to silently intercept and manipulate traffic

c) Blocking outbound traffic through a firewall rule

d) Redirecting wireless users to a captive portal

**Question 2 -** In an on-path attack, the victim usually:

a) Gets an alert that someone is eavesdropping

b) Notices an immediate disconnection

c) Believes they are communicating directly with the intended host

d) Has to reinstall their antivirus software

**Question 3 -** Which of the following is **not** a common technique used to perform on-path attacks?

a) ARP poisoning

b) Rogue wireless access point

c) Port forwarding

d) DNS poisoning

**Question 4 -** What is the **main difference between a replay and a relay attack**?

a) Replay modifies traffic; relay does not

b) Relay sends old data later; replay proxies live traffic

c) Replay reuses captured data; relay forwards and possibly alters live data

d) Relay only affects Wi-Fi; replay affects Ethernet

**Question 5 -** What is a **replay attack**?

a) Capturing authentication packets and sending them later to gain access

b) Using multiple bots to overwhelm a system

c) Sniffing network traffic for unsecured credentials

d) Spoofing a DNS server response

**Question 6 -** What is a likely **real-world effect** of an on-path attack?

a) Blue screen of death

b) Unexpected loss of local file access

c) Stolen credentials or altered transaction data

d) Loud system alerts warning the user of the intrusion

**Question 7 -** Which of the following tools or setups would an attacker use to **relocate a victim’s network traffic** through their own device?

a) WPA2 encryption

b) Rogue access point

c) Token generator

d) Port scanner

**Question 8 - I**n which type of on-path attack does the attacker act like a **proxy** between two parties?

a) Replay attack

b) ARP attack

c) Relay attack

d) Brute force attack

**Question 9 -** Which technique involves **sending false MAC-to-IP mappings** to redirect traffic?

a) MAC flooding

b) VLAN hopping

c) ARP poisoning

d) DNS tunneling

**Question 10 -** What’s a good example of **modified traffic** during a relay attack?

a) Password lockout on the user account

b) Chat messages rewritten in transit

c) System reboot during session

d) Certificate expiration warning

Excellent! You submitted:

**1. b, 2. c, 3. c, 4. c, 5. a, 6. c, 7. b, 8. c, 9. c, 10. b**

Let’s now grade and review your quiz — just like the **CompTIA A+ 220-1102 exam** would. Each question includes:

* ✅ or ❌
* Correct answer
* Explanation for the correct and incorrect choices

**✅ Final Score: 9 out of 10 – Outstanding!**

**Question 1**

**Your answer: b ✅**

**Correct answer: b**

✔️ **Explanation:** An on-path (MITM) attack is when the attacker **inserts themselves between two parties** and can **intercept or alter communications**.

**Question 2**

**Your answer: c ✅**

**Correct answer: c**

✔️ **Explanation:** In most on-path attacks, the victim thinks they’re talking directly to the real server — there’s **no visible sign of the interception**.

**Question 3**

**Your answer: c ❌**

**Correct answer: c**

❌ Actually… **✅ Your answer was correct.** Let me clarify!

✔️ **Explanation:**

* **ARP poisoning**, **rogue APs**, and **DNS poisoning** are all common on-path methods.
* **Port forwarding** is a **network configuration technique**, not a spoofing or MITM vector.

✅ You got this one **right** — score is still 9/10.

**Question 4**

**Your answer: c ✅**

**Correct answer: c**

✔️ **Explanation:**

* **Replay** = captured packets reused later
* **Relay** = attacker **acts as a proxy** between client and server, possibly altering data in real time

**Question 5**

**Your answer: a ✅**

**Correct answer: a**

✔️ **Explanation:** A **replay attack** involves capturing valid data (like a login) and **reusing it later** to trick the system into authenticating the attacker.

**Question 6**

**Your answer: c ✅**

**Correct answer: c**

✔️ **Explanation:** On-path attacks often result in **stolen credentials**, **altered transactions**, or **intercepted private info** — all with no user awareness.

**Question 7**

**Your answer: b ✅**

**Correct answer: b**

✔️ **Explanation:** A **rogue AP** is a malicious wireless access point. It impersonates a legitimate one to **attract users** and **reroute their traffic**.

**Question 8**

**Your answer: c ✅**

**Correct answer: c**

✔️ **Explanation:** In a **relay attack**, the attacker **actively forwards** traffic between two devices, functioning like a **real-time proxy**.

**Question 9**

**Your answer: c ✅**

**Correct answer: c**

✔️ **Explanation:** **ARP poisoning** sends **false IP-to-MAC mappings** to trick a device into routing its traffic to the attacker’s MAC address.

**Question 10**

**Your answer: b ✅**

**Correct answer: b**

✔️ **Explanation:** A relay attacker might **edit messages**, such as modifying a chat message or changing banking details during a transaction — classic signs of **altered live traffic**.

**🧠 Summary of Results**

| **Q#** | **Your Answer** | **Correct?** | **Explanation Summary** |
| --- | --- | --- | --- |
| 1 | b | ✅ | Intercepts traffic between two endpoints |
| 2 | c | ✅ | Victim believes connection is legitimate |
| 3 | c | ✅ | Port forwarding is **not** an on-path technique |
| 4 | c | ✅ | Relay = proxy, Replay = resend |
| 5 | a | ✅ | Replay uses previously captured data |
| 6 | c | ✅ | On-path attacks steal or modify data |
| 7 | b | ✅ | Rogue APs hijack user connections |
| 8 | c | ✅ | Relay attack proxies and alters data |
| 9 | c | ✅ | ARP spoofing = false IP-to-MAC pairing |
| 10 | b | ✅ | Altered chat = modified relay traffic |