A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

Host discovery

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

The Wireshark UDP Endpoints statistics show that the attacker (10.1.1.34) used source port 54628 to send 1000 UDP packets toward the target (10.1.1.36). Of these, only 4 replies were received in the form of ICMP “Port Unreachable” errors. This is a hallmark of a UDP port scan, where the attacker probes many ports, closed ports reply with ICMP errors, and open or filtered ports remain silent.

A screenshot of a computer

AI-generated content may be incorrect.

The TCP Endpoints statistics show that the attacker (10.1.1.34) used source port 60603 to transmit over 1000 TCP packets toward the target (10.1.1.36). The attacker received only 15 replies, which is consistent with a TCP SYN (half-open) scan: many SYN packets were sent to different ports, but only a small number responded with SYN/ACK (open) or RST (closed).

A screenshot of a computer

AI-generated content may be incorrect.

 Matches **SYN packets from attacker (10.1.1.34)** to the target (10.1.1.36).

 Confirms the attacker sent ~1000 TCP SYN probes across many ports

A screenshot of a computer

AI-generated content may be incorrect.

 Matches **SYN/ACK responses from the target (10.1.1.36)** to the attacker (10.1.1.34).

 Confirms some ports on the target were **open** because they replied with SYN/ACK.

A screenshot of a computer

AI-generated content may be incorrect.

Together, these two filters prove a **TCP SYN (half-open) scan**:

* The attacker sprayed SYN probes.
* The target replied with SYN/ACK on some ports → indicating they are open.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**TFTP Read (RRQ)**

* 10.1.1.36 → 10.1.1.34 requests post\_exploit.ps1.
* This means the attacker **pulled the PowerShell script** from the victim’s machine.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**TFTP Write (WRQ)**

* 10.1.1.36 → 10.1.1.34 initiates a **Write Request** for exfiltrate.txt.
* In TFTP, a **Write Request means the sender (attacker) wants to upload a file to the receiver (victim)**.

A screenshot of a computer

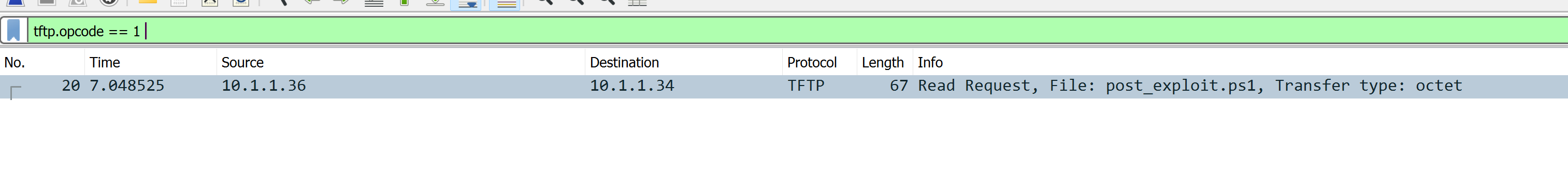
AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.