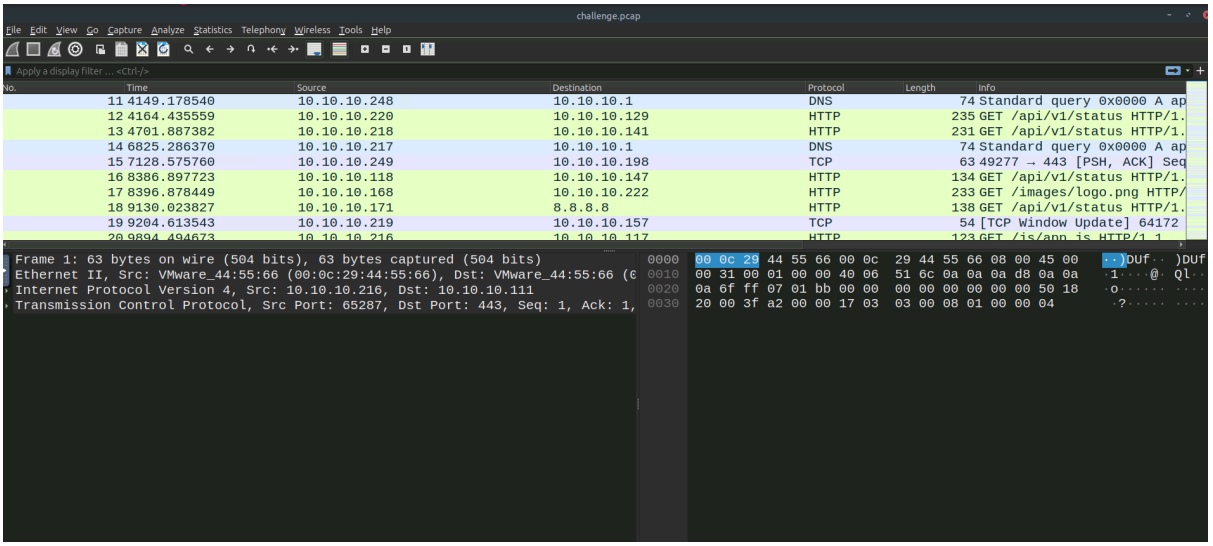
First Shift CTF Task 6: The Crown Jewel

Author: Ernest Nyabayo Osindo

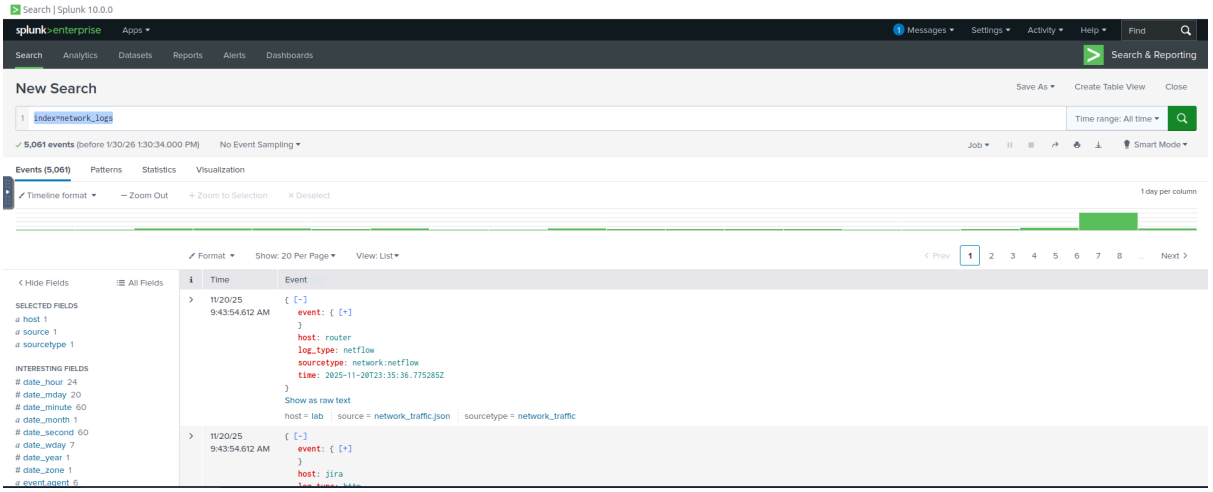
The Crown Jewel
You are on a shift, looking at the new alert coming from Imperium Labs - a company under MSSP monitoring long before you joined the team. It's hard to say what the company's primary focus is, but it has a global presence and undoubtedly has secrets to protect, especially those on heavily secured GitLab and Jira servers which store proprietary source code and project data.

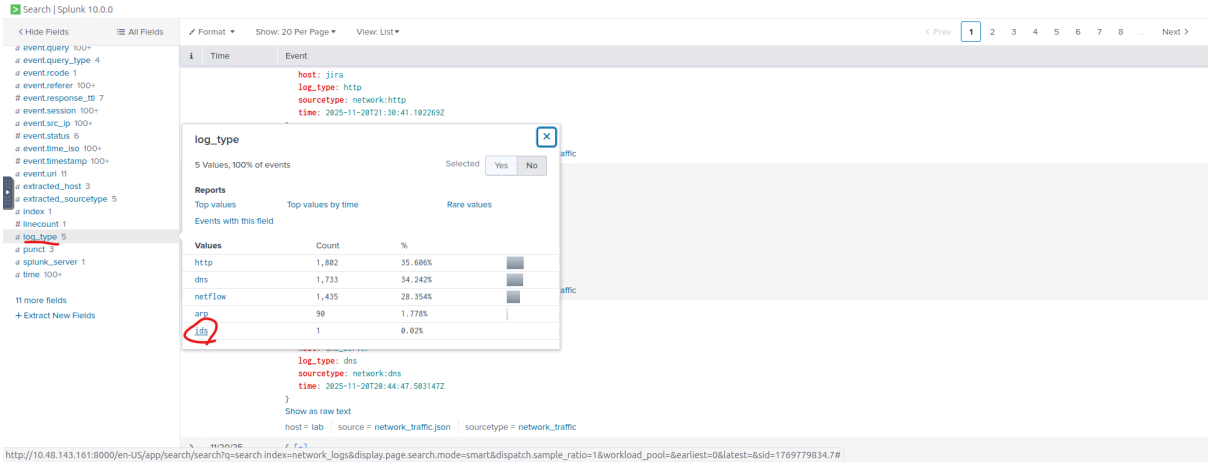
The Alert
The alert you are looking at is called Reverse Shell Outbound Connection Detected, not something you see every day. Fortunately, you were able to obtain the raw PCAPs and Splunk logs for this event. Can you analyze the network traffic and logs to reconstruct and stop a sophisticated attack aimed at stealing the "Crown Jewel" data?

- Detailed network traffic capture challenge.pcap that you can find on the network_traffic folder on the VM's Desktop
- Pre-ingested Splunk logs (index=network_logs), which can be accessed at 10.48.143.161:8000

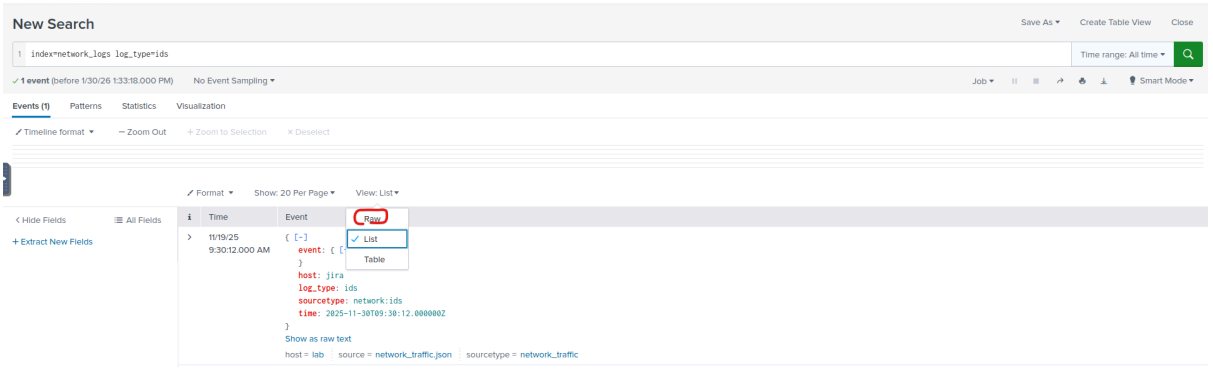


index=network_logs





http://10.48.143.161:8000/en-US/app/search/search?q=search index=network_logs&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1769779834.7#

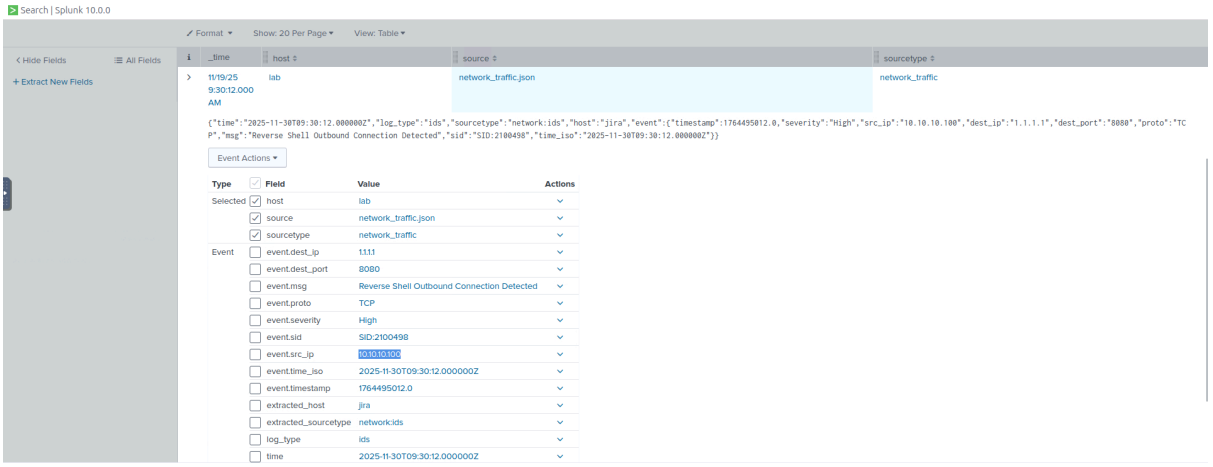


http://10.48.143.161:8000/en-US/app/search/search?q=search index=network_logs log_type=ids&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1769779998.10#

1. From which internal IP did the suspicious connection originate?

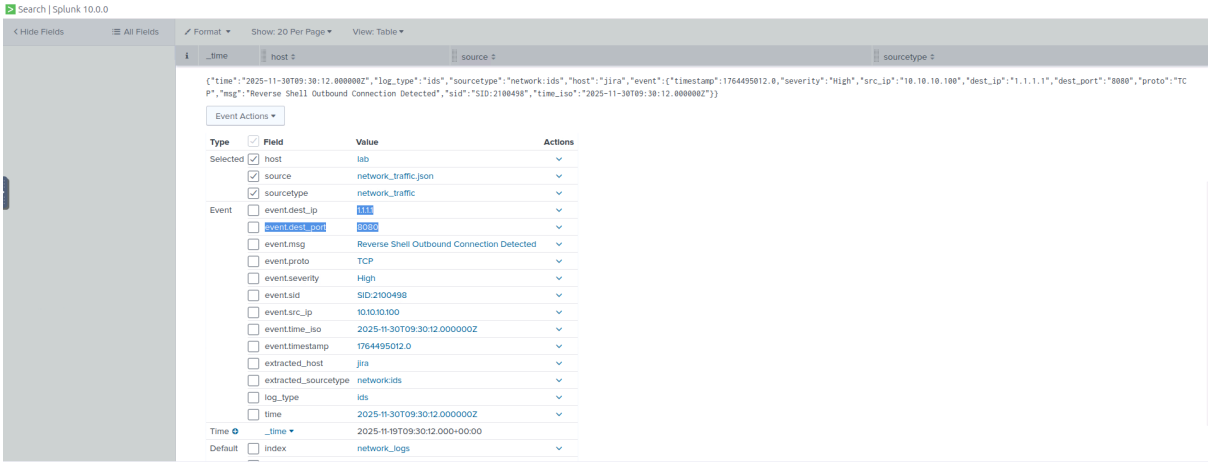
index=network_logs log_type=ids

View table



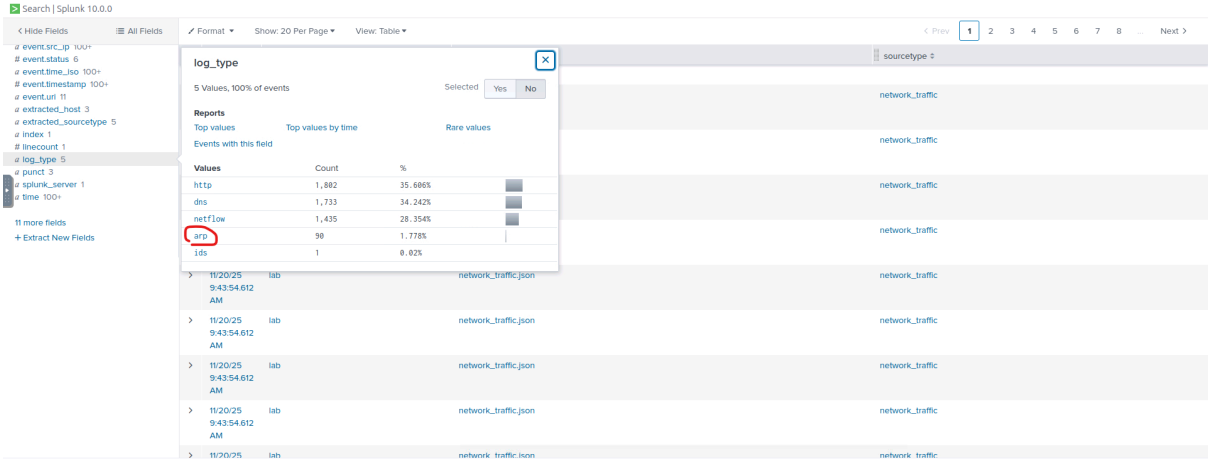
Answer: 10.10.10.100

2. What outbound connection was detected as a C2 channel? (Answer example: 1.2.3.4:9996)

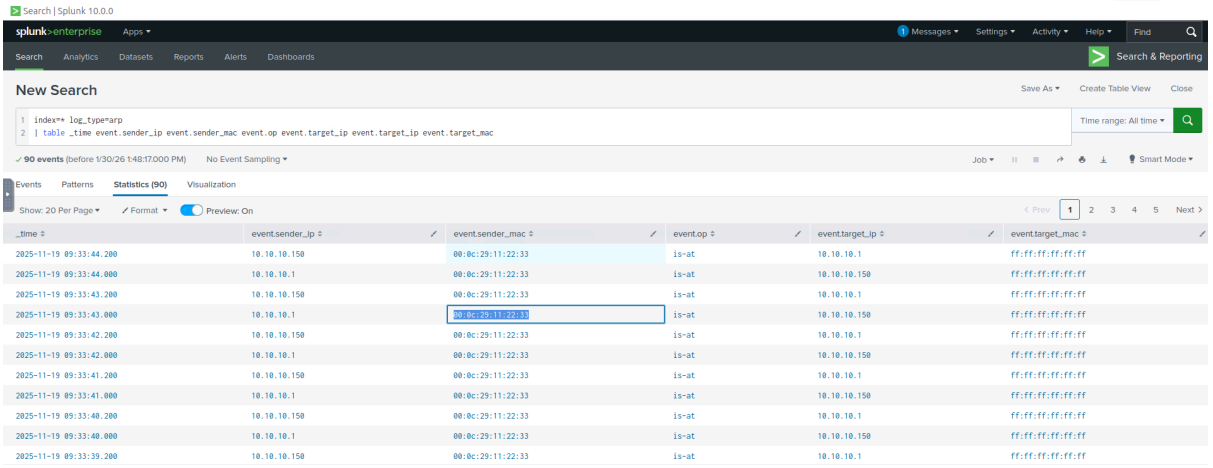


Answer: 1.1.1.1:8080

3. Which MAC address is impersonating the gateway 10.10.10.1?



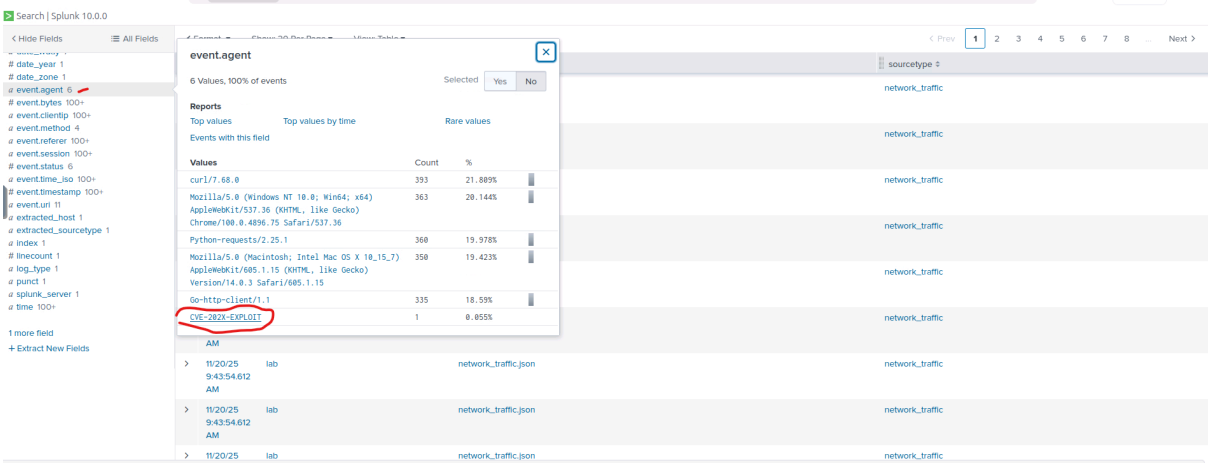
index=* log_type=arp
| table _time event.sender_ip event.sender_mac event.op event.target_ip event.target_ip event.target_mac

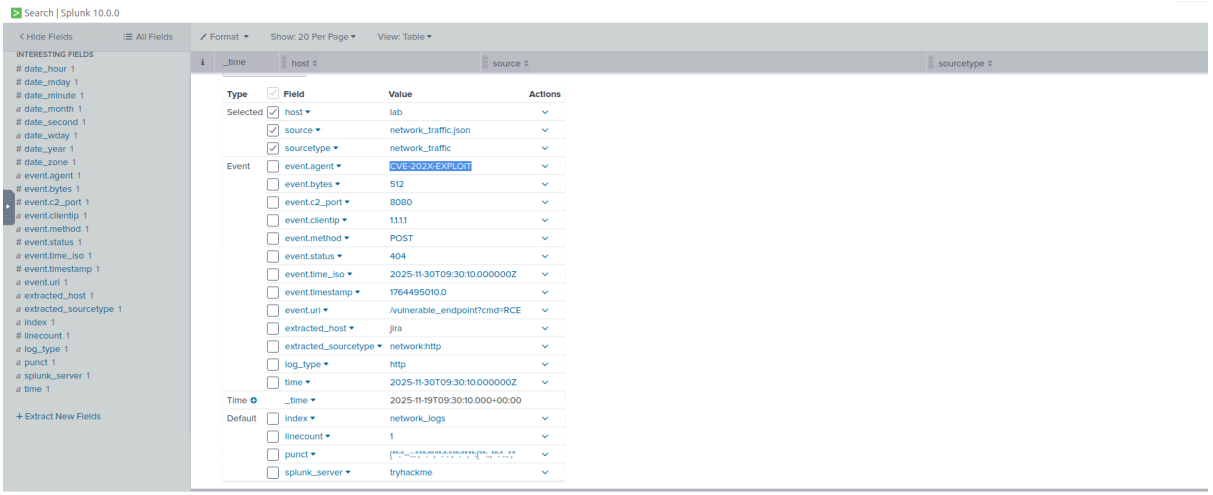


Answer: 00:0c:29:11:22:33

5. What is the non-standard User-Agent hitting the Jira instance?

index=* log_type=http

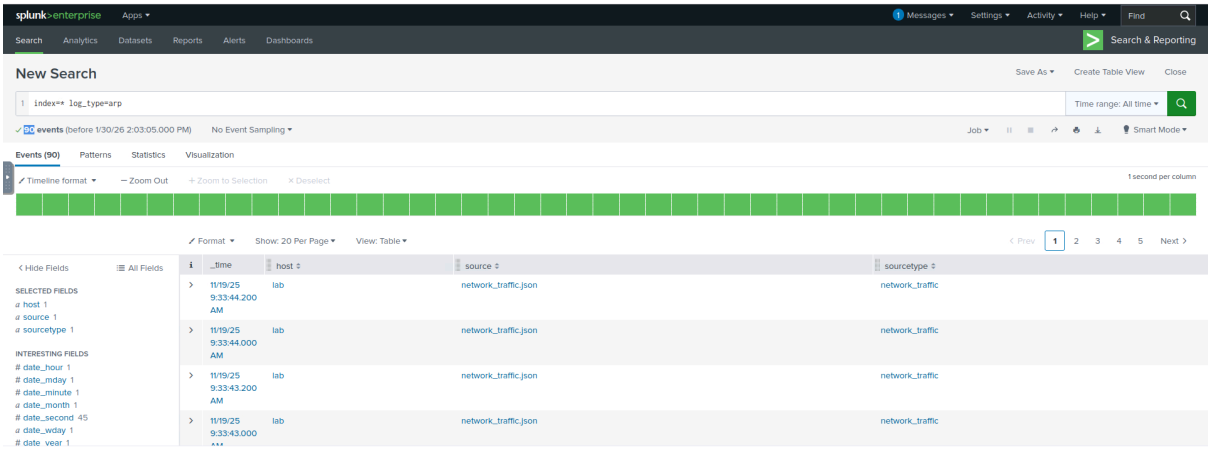




Answer: CVE-202X-EXPLOIT

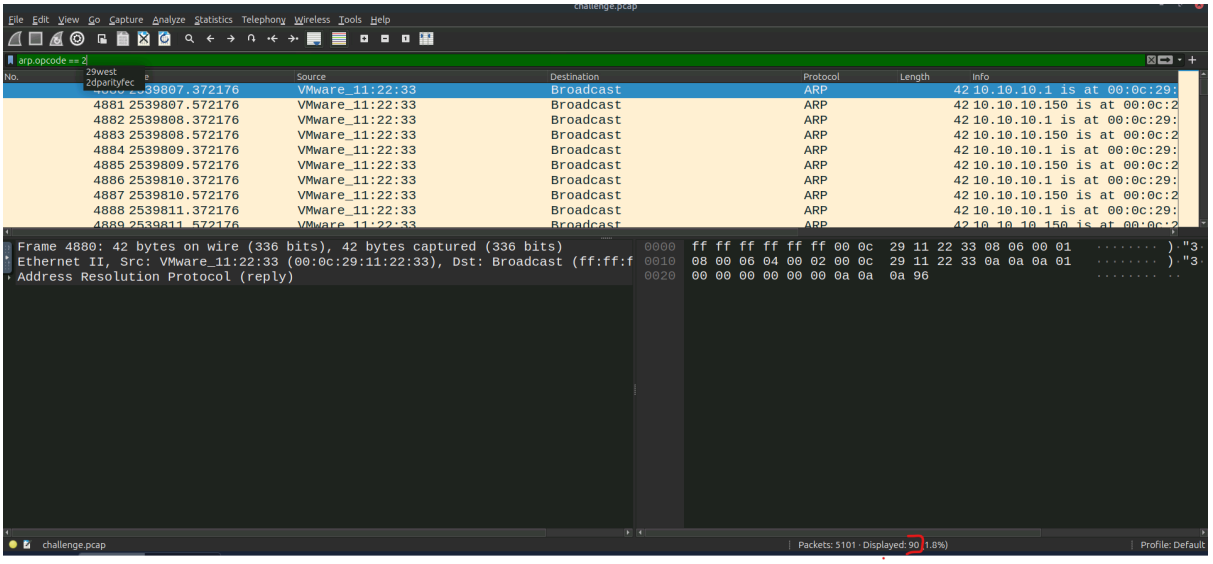
6. How many ARP spoofing attacks were observed in the PCAP?

index=* log_type=arp



Also

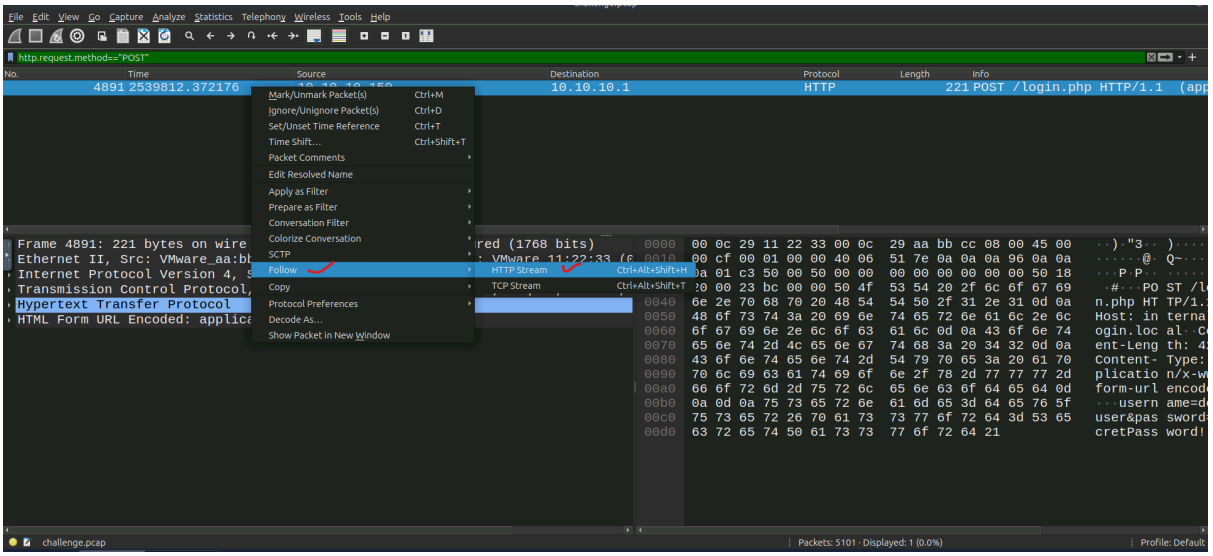
arp.opcode == 2

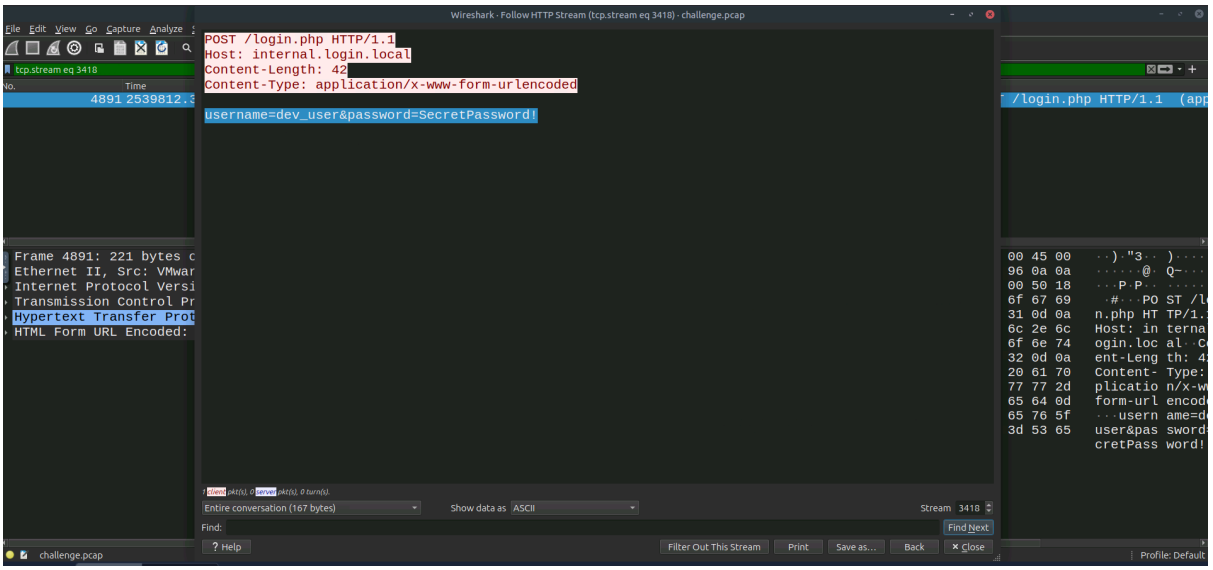


Answer: 90

7. What's the payload containing the plaintext creds found in the POST request?

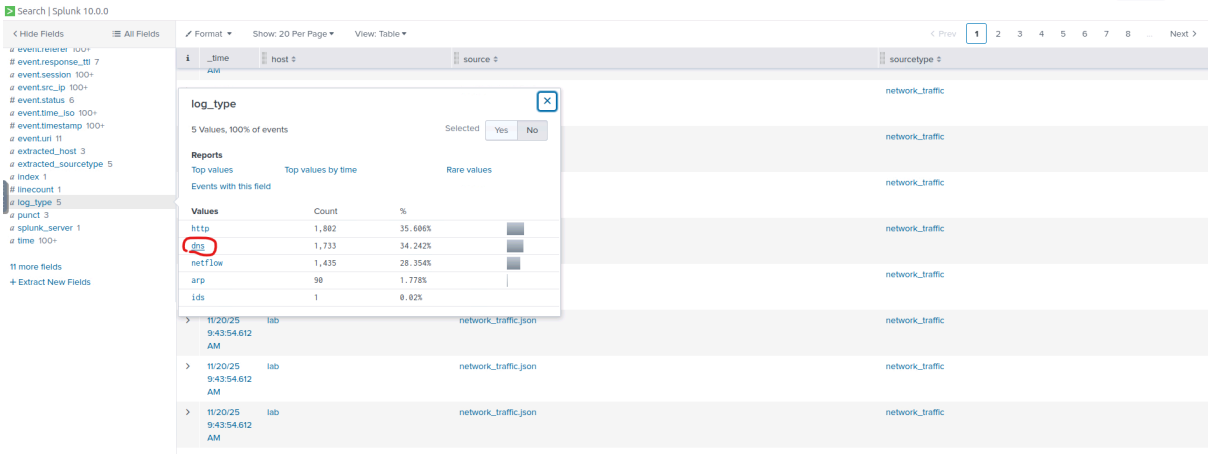
http.request.method=="POST"

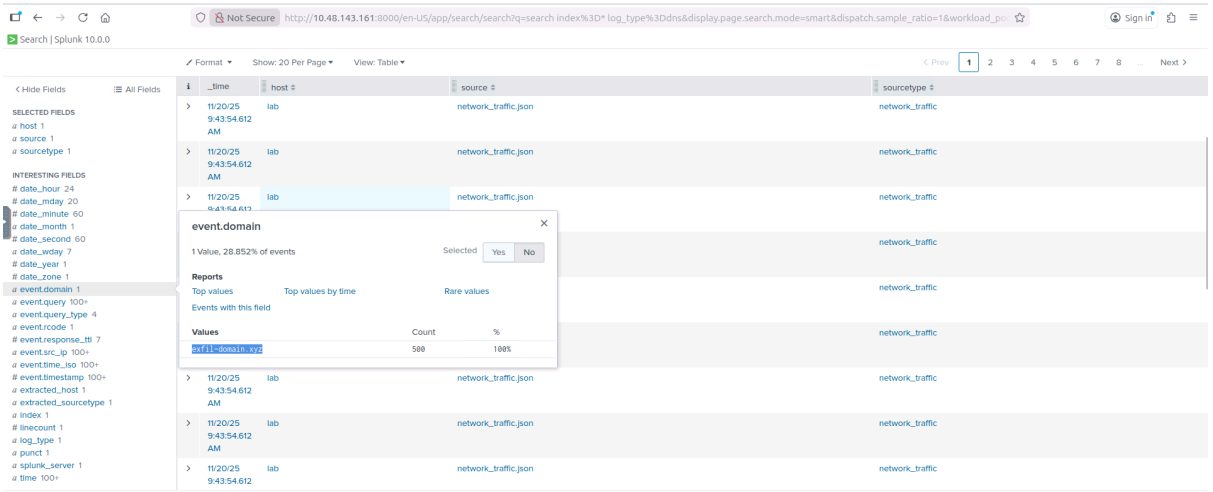




Answer: username=dev_user&password=SecretPassword!

8. What domain, owned by the attacker, was used for data exfiltration?





Answer: exfil-domain.xyz

9. After examining the logs, which protocol was used for data exfiltration?

Answer: DNS