### **Acoustic Lab — CyberDefenders**

**Scenario:** This lab takes you into the world of voice communications on the internet. VoIP is becoming the de-facto standard for voice communication. As this technology becomes more common, malicious parties have more opportunities and stronger motives to control these systems to conduct nefarious activities. This challenge was designed to examine and explore some of the attributes of the SIP and RTP protocols.

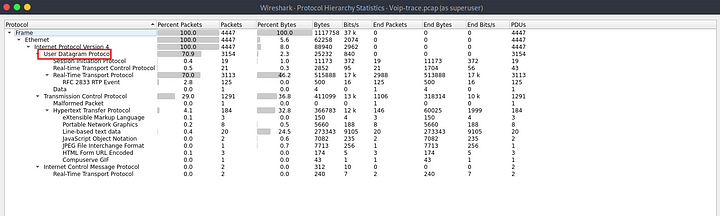
Lab Files:

* *“log.txt*” was generated from an unadvertised, passive honeypot located on the internet such that any traffic destined to it must be nefarious. Unknown parties scanned the honeypot with a range of tools, and this activity is represented in the log file.
* The IP address of the honeypot has been changed to “honey.pot.IP.removed”. In terms of geolocation, pick your favorite city.
* The MD5 hash in the authorization digest is replaced with “MD5\_hash\_removedXXXXXXXXXXXXXXXX”
* Some octets of external IP addresses have been replaced with an “X”
* Several trailing digits of phone numbers have been replaced with an “X”
* Assume the timestamps in the log files are UTC.
* *“Voip-trace.pcap*” was created by honeynet members for this forensic challenge to allow participants to employ network analysis skills in the VOIP context.

As a soc analyst, analyze the artifacts and answer the questions.

1. **What is the transport protocol being used?**

Go to Statistics -> Protocol Hierarchy.

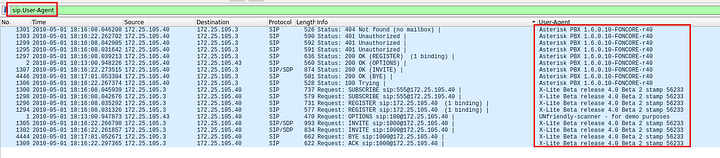


**Answer:** UDP

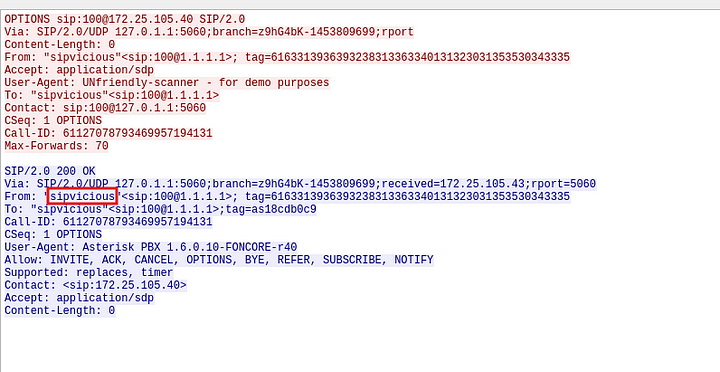
**2. The attacker used a bunch of scanning tools that belong to the same suite. Provide the name of the suite.**

As we see above, the use of Session Initiation Protocol(SIP). We can have a look at these packets as they will have a User-Agent field which can contain details about the tools used.

sip.User-Agent



Now, we can see different tools in the User-Agent field. While looking at the packets closely, we can find the suite of the tools.



Answer: Sipvicious

**3. What is the User-Agent of the victim system?**

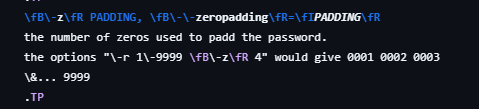
On the same packet above, we can see the User-Agent of the victim.



**Answer:** Asterisk PBX 1.6.0.10-FONCORE-r40

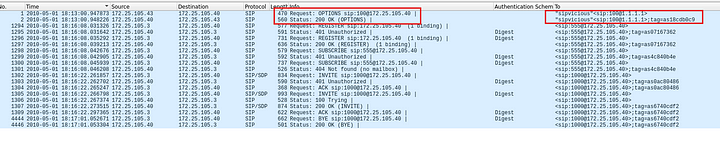
**4. Which tool was only used against the following extensions: 100,101,102,103, and 111?**

Reading through the code of the tools in the sipvicious suite, we can see that only one of these tools is capable of being used on specific extensions.



**Answer:** svcrack.py

**5. Which extension on the honeypot does NOT require authentication?**

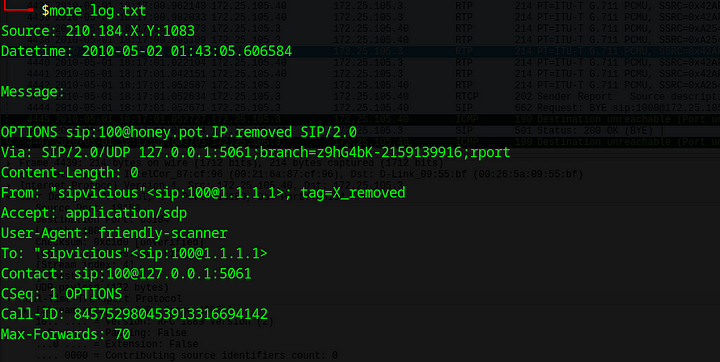
****

As we can see above, the request to the extension 100 did not require any authentication.

Answer: 100

**6. How many extensions were scanned in total?**

We were also given a log file along with the packet capture, let us look at the contents of the log file.



It seems like an sip log. We can extract the number of extensions scanned from this file.

cat log.txt |grep -A 1 "friendly-scanner" | grep "To" | cut -d "\"" -f 3 | cut -d "@" -f 1 | cut -d ":" -f 2 | sort | uniq | wc -l

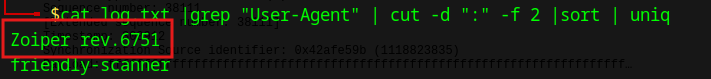
This will cut out all the unique extensions that were scanned and then gives out the count.



**Answer:** 2652

**7. There is a trace for a real SIP client. What is the corresponding user-agent? (two words, once space in between)**

cat log.txt |grep "User-Agent" | cut -d ":" -f 2 |sort | uniq

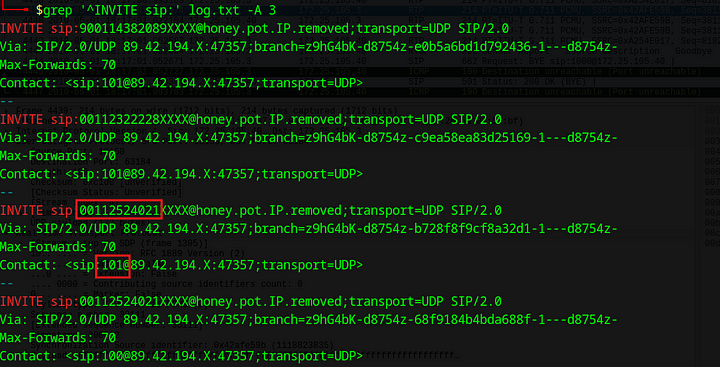


**Answer:** Zoiper rev.6751

**8. Multiple real-world phone numbers were dialed. What was the most recent 11-digit number dialed from extension 101?**

We can carve out the log file to show the invite field.

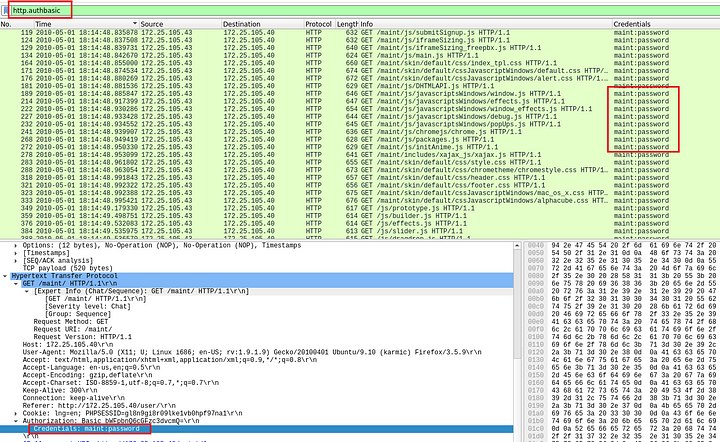
grep '^INVITE sip:' log.txt -A 3



**Answer:** 00112524021

**9. What are the default credentials used in the attempted basic authentication? (format is username:password)**

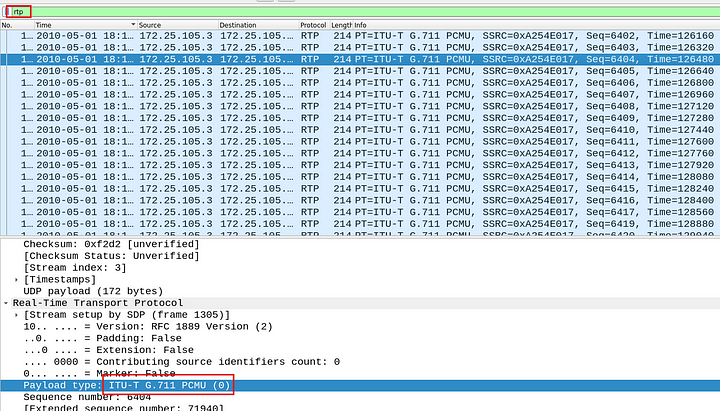
http.authbasic



**Answer:** maint:password

**10. Which codec does the RTP stream use? (3 words, 2 spaces in between)**

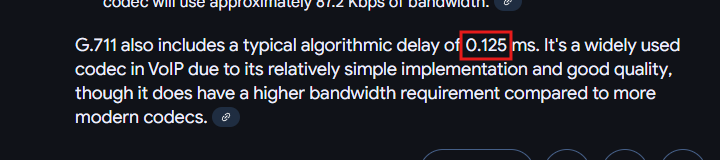
rtp



**Answer:** ITU-T G.711 PCMU

**11. How long is the sampling time (in milliseconds)?**

Quick google search with G.711 reveals the answer.

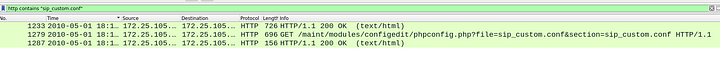


Answer: 0.125

**12. What was the password for the account with username 555?**

VoIP soft‐switches and PBXs often store user credentials in plain‐text config files. So as per the hint we will search for http packets containing sip\_custom.conf file.

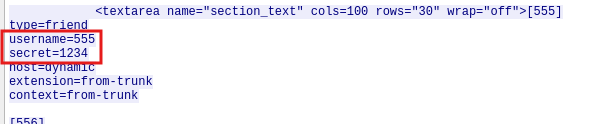
http contains "sip\_custom.conf"



One of these packets contains the file.



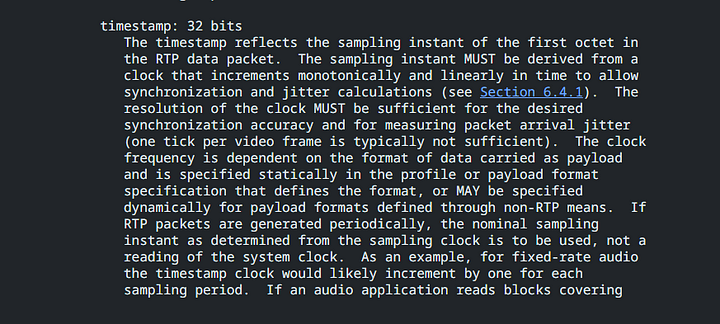
Let us examin this packet by following the TCP stream.



**Answer:** 1234

**13. Which RTP packet header field can be used to reorder out of sync RTP packets in the correct sequence?**

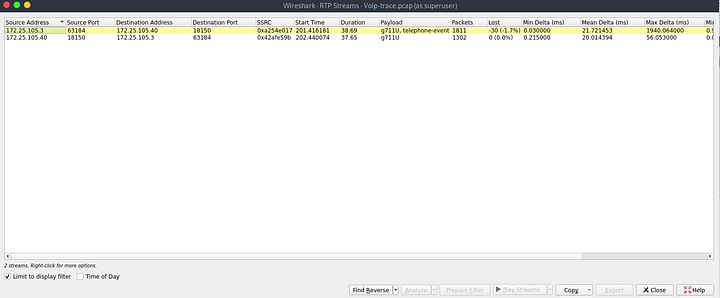
We can read the RTP documentation for this.



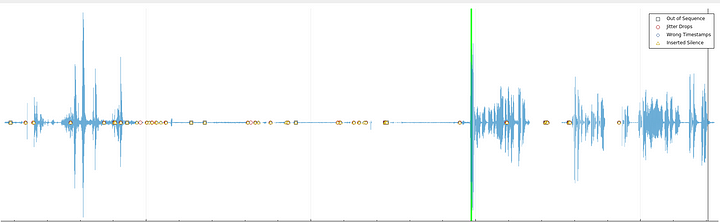
Answer: Timestamp

**14. The trace includes a secret hidden message. Can you hear it?**

We can Click on Telephony -> RTP -> RTP Streams



Select stream and click play streams.



**Answer:** Mexico

This is the end of this walkthrough.