Assignment 11

520030910281 肖真然

Question 1:

The stored password hashes are vulnerable to Rainbow Table Attacks. How to Protect Against a Rainbow Table Attack?

A:

1. **Use Salt**: Salt is a random value unique to each password hash. By appending or prepending a salt to the password before hashing, even if two users have the same password, their hashes will be different due to the unique salt. This means an attacker would need to generate a rainbow table for each salt value, greatly increasing the computational effort required.
2. **Use Strong Hashing Algorithms**: Choose strong cryptographic hashing algorithms like SHA-256 or bcrypt. These algorithms are designed to be computationally expensive, making it more difficult for attackers to generate rainbow tables.
3. **Use Key Strengthening**: Techniques like key stretching increase the computational cost of hashing, making it more time-consuming for attackers to generate rainbow tables. bcrypt and PBKDF2 are examples of algorithms that incorporate key stretching.
4. **Use Iterative Hashing**: Instead of hashing the password once, hash it multiple times (iterations). This makes the hashing process slower and more resource-intensive, making rainbow table attacks less feasible.
5. **Implement Account Lockout Mechanisms**: Implement mechanisms that lock out an account after a certain number of failed login attempts. This helps mitigate brute force and rainbow table attacks by limiting the number of attempts an attacker can make.

Question 2:

Why is more than one mixing server useful in the mixnet? That is, why is security better for a mixnet of multiple servers instead of only one?

A:

1. **Increased Anonymity**: With multiple mixing servers, the path that a message takes through the mixnet becomes more complex and less predictable. This enhances anonymity by making it harder for adversaries to trace the origin and destination of messages. If there's only one mixing server, it becomes a single point of failure and potential surveillance.
2. **Resilience to Attacks**: A mixnet with multiple servers is more resilient to attacks such as denial-of-service (DoS) attacks or targeted attacks on individual servers. If one server is compromised or taken offline, the network can still operate effectively through other available servers.
3. **Diverse Jurisdictions**: Multiple mixing servers can be distributed across different jurisdictions or organizations, making it difficult for any single entity to monitor or control the entire network. This decentralization adds another layer of security against censorship or government surveillance.

4. **Reduced Trust**: In a mixnet with multiple servers, users don't need to trust any single server with their data. Even if some servers are compromised or collude, the overall security and privacy of the network can still be maintained as long as a sufficient number of servers remain honest.
5. **Traffic Analysis Resistance**: Multiple mixing servers can introduce variability in the timing and routing of messages, making traffic analysis attacks more challenging. It becomes harder for adversaries to correlate input and output traffic flows, thereby increasing the overall security of the mixnet.

Question 3

Try to hide your real IP address with the help of Tor.

1. You may try some popular Tor-related tools, such as Tor Browser.
2. You need to provide evidence that the IP address is hidden successfully. (hint: you can access http://checkip.amazonaws.com to obtain your IP address.)
3. (Bonus) Now we have achieved anonymous communication. However, using a static IP address with Tor is not safe enough. So, could you provide a way to occasionally change your identity (i.e., IP address) from Tor?

A:

1. Use Tor Browser to hide my IP.

   Part of log:

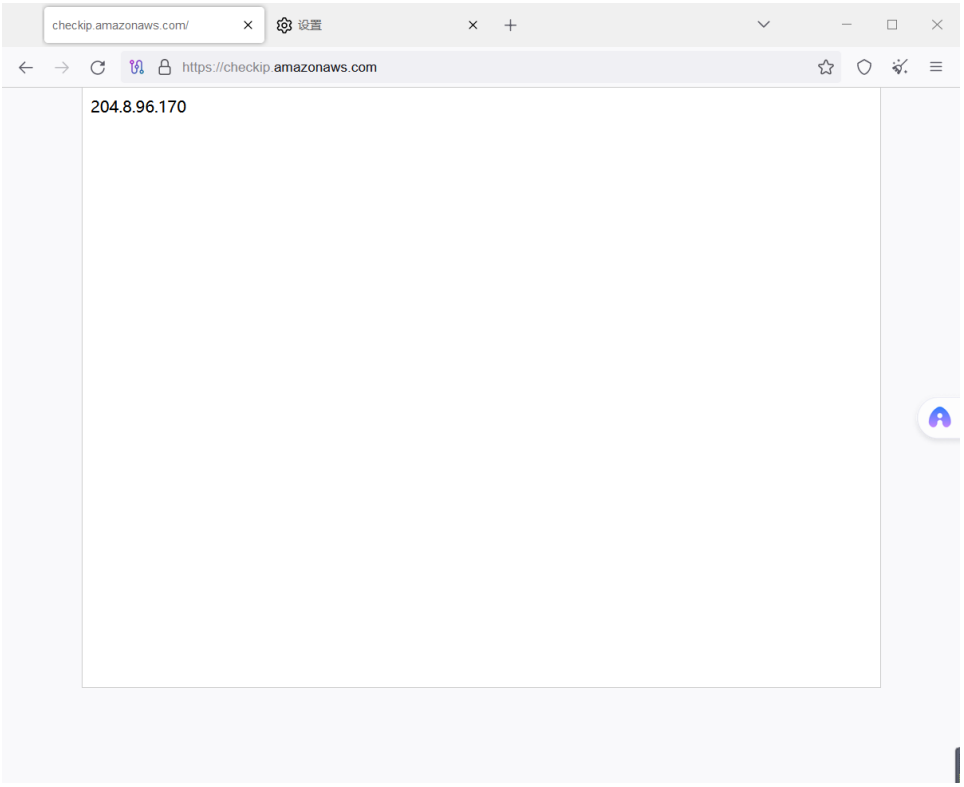
```
2024-05-08 02:32:36.801 [NOTICE] Opening Socks listener on 127.0.0.1:9150
2024-05-08 02:32:36.801 [NOTICE] Opened Socks listener connection (ready) on
127.0.0.1:9150
2024-05-08 02:32:37.831 [NOTICE] Bootstrapped 10% (conn_done): Connected to a relay
2024-05-08 02:32:43.865 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": offer created
2024-05-08 02:32:43.865 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": offer created
2024-05-08 02:32:44.874 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": broker rendezvous peer
received
2024-05-08 02:32:45.208 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": broker rendezvous peer
received
2024-05-08 02:32:46.866 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": connected
2024-05-08 02:32:47.020 [NOTICE] Managed proxy
"TorBrowser\Tor\PluggableTransports\snowflake-client.exe": connected
2024-05-08 02:32:47.020 [NOTICE] Bootstrapped 14% (handshake): Handshaking with a relay
2024-05-08 02:32:47.276 [NOTICE] Bootstrapped 15% (handshake_done): Handshake with a
relay done
2024-05-08 02:32:47.276 [NOTICE] Bootstrapped 20% (onehop_create): Establishing an
encrypted directory connection
2024-05-08 02:32:47.522 [NOTICE] Bootstrapped 25% (requesting_status): Asking for
networkstatus consensus
```

```
2024-05-08 02:32:47.994 [NOTICE] new bridge descriptor 'flakey1' (fresh):
$2B280B23E1107BB62ABFC40DDCC8824814F80A72~flakey1
[1zOHpg+FxqQfi/6jDLtCpHHqBTH8gjYmCKXkus1D5Ko] at 192.0.2.5
2024-05-08 02:32:49.146 [NOTICE] Bootstrapped 30% (loading_status): Loading
networkstatus consensus
2024-05-08 02:32:49.420 [NOTICE] new bridge descriptor 'crusty4' (fresh):
$8838024498816A039FCBBAB14E6F40A0843051FA~crusty4
[tO9nYvNCAdAh9lPoEEv2pZ9BJq+YzmPAMY6pxoFrLuk] at 192.0.2.6
2024-05-08 02:32:51.316 [NOTICE] I learned some more directory information, but not
enough to build a circuit: We have no usable consensus.
2024-05-08 02:32:51.572 [NOTICE] Bootstrapped 40% (loading_keys): Loading authority key
certs
2024-05-08 02:32:52.105 [NOTICE] The current consensus has no exit nodes. Tor can only
build internal paths, such as paths to onion services.
2024-05-08 02:32:52.106 [NOTICE] Bootstrapped 45% (requesting_descriptors): Asking for
relay descriptors
2024-05-08 02:32:52.106 [NOTICE] I learned some more directory information, but not
enough to build a circuit: We need more microdescriptors: we have 1/7264, and can only
build 0% of likely paths. (We have 100% of guards bw, 0% of midpoint bw, and 0% of end
bw (no exits in consensus, using mid) = 0% of path bw.)
2024-05-08 02:32:52.107 [NOTICE] I learned some more directory information, but not
enough to build a circuit: We need more microdescriptors: we have 1/7264, and can only
build 0% of likely paths. (We have 100% of guards bw, 0% of midpoint bw, and 0% of end
bw (no exits in consensus, using mid) = 0% of path bw.)
2024-05-08 02:32:52.654 [NOTICE] Bootstrapped 50% (loading_descriptors): Loading relay
descriptors
2024-05-08 02:32:56.297 [NOTICE] The current consensus contains exit nodes. Tor can
build exit and internal paths.
2024-05-08 02:32:59.551 [NOTICE] Bootstrapped 55% (loading_descriptors): Loading relay
descriptors
2024-05-08 02:32:59.551 [NOTICE] Bootstrapped 60% (loading_descriptors): Loading relay
descriptors
2024-05-08 02:32:59.800 [NOTICE] Bootstrapped 67% (loading_descriptors): Loading relay
descriptors
2024-05-08 02:33:00.315 [NOTICE] Bootstrapped 75% (enough_dirinfo): Loaded enough
directory info to build circuits
2024-05-08 02:33:00.530 [NOTICE] Bootstrapped 90% (ap_handshake_done): Handshake
finished with a relay to build circuits
2024-05-08 02:33:00.530 [NOTICE] Bootstrapped 95% (circuit_create): Establishing a Tor
circuit
2024-05-08 02:33:01.510 [NOTICE] Bootstrapped 100% (done): Done
```

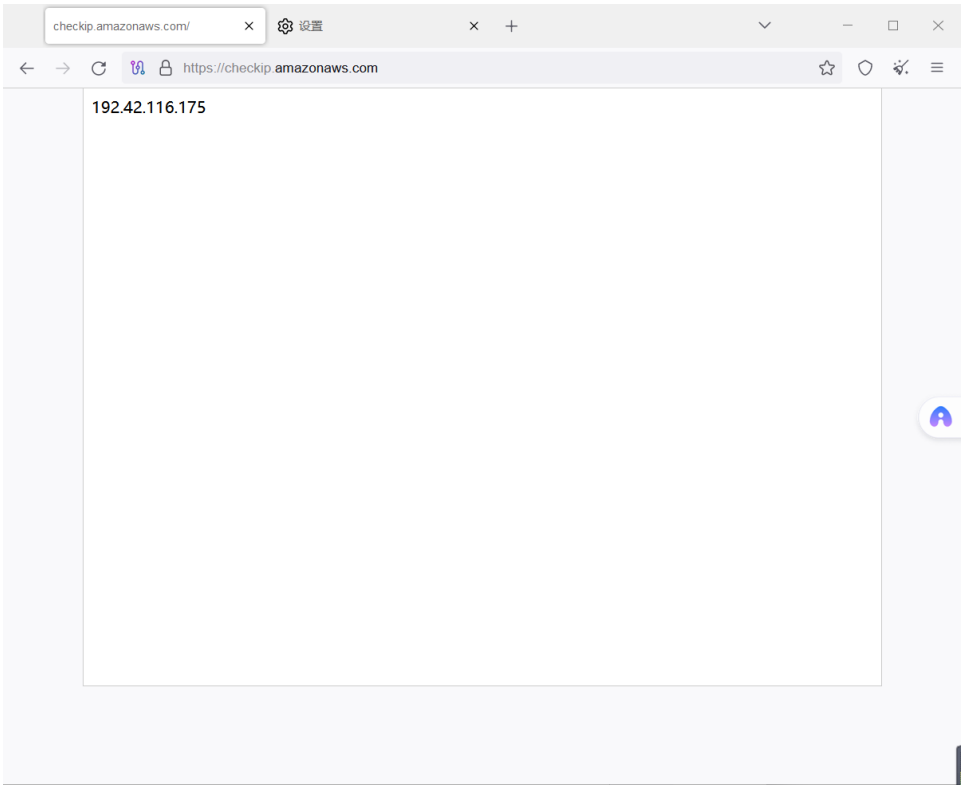
2.

My true IP:

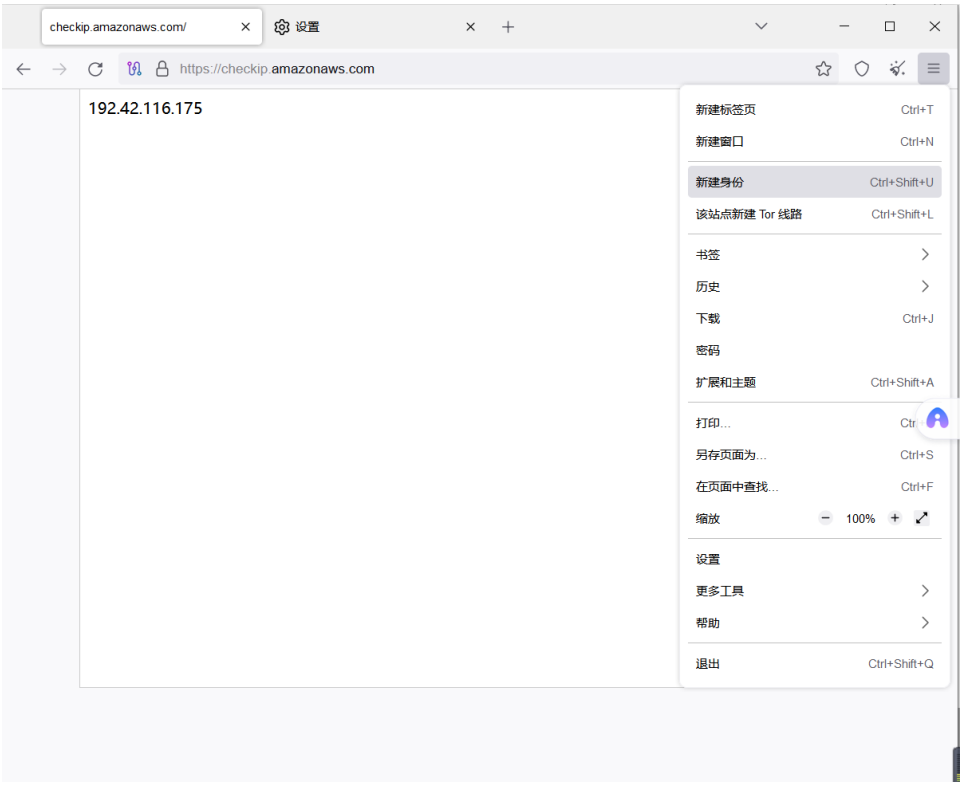
Fake IP:

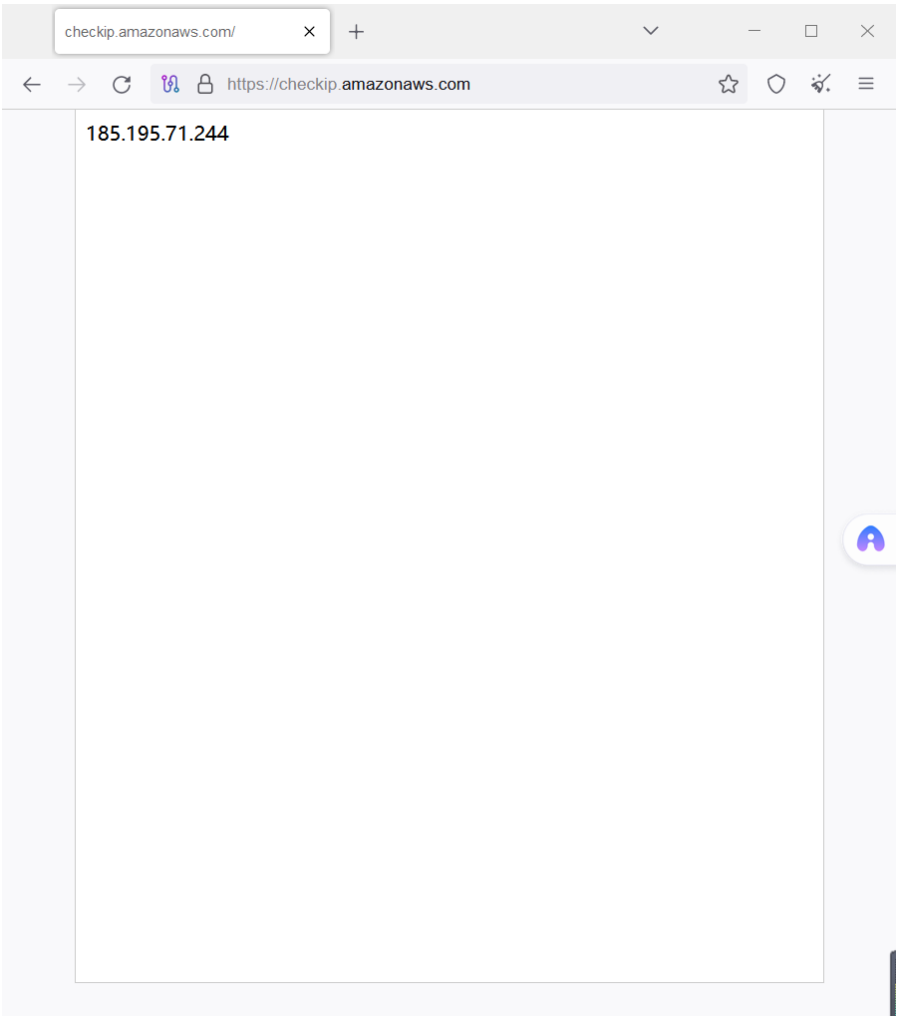


And it can change every once in a while.



3.
- Use VPN.
- Ask Tor for a new identity.




checkip.amazonaws.com/
https://checkip.amazonaws.com
185.195.71.244