# Security Incident Report

## **Section 1:** Identify the network protocol involved in the incident

The transport layer was compromised by the brute force attack (see below)

## **Section 2:** Document the incident

After analyzing the tcpdump, it was observed that the user's communication was intercepted at the transport layer. Here's a timeline of events:

- At 14:18:32.192, the user's computer initiates a regular request to the DNS server, successfully obtaining the corresponding IP address.
- However, at 14:20:32.192, an apparent spoofed request is made by the same machine to the DNS server, which responds with a different IP address.
- The machine establishes a connection with this new IP address and proceeds with downloading malicious software.
- By 14:25:29.57, the machine initiates the download of the malicious software using an HTTP GET request.

Please note that the timeline provided above highlights the sequence of events captured in the tcpdump. *(tcpdump log attached)*

## **Section 3:** Recommend one remediation

One remediation strategy to prevent a brute force attack like the one described would be to implement account lockout policies. Account lockout policies help mitigate brute force attacks by temporarily locking user accounts after a certain number of failed login attempts. This prevents attackers from repeatedly guessing passwords or trying different combinations to gain unauthorized access.

Here's how you can implement this strategy:

1. Define a threshold: Determine the maximum number of allowed failed login attempts before an account gets locked. Consider factors such as the sensitivity of the system and the risk tolerance of your organization.

2. Configure lockout duration: Specify the duration for which an account will remain locked after exceeding the failed login attempt threshold. This duration should be long enough to deter attackers but short enough to minimize inconvenience for legitimate users.

3. Set lockout reset policies: Decide whether the lockout duration should automatically reset after a certain period or require manual intervention from an administrator.

4. Notify users: Clearly communicate the lockout policy to your users, including the threshold, lockout duration, and any instructions they need to follow to regain access to their accounts.

5. Implement secure password practices: Encourage users to create strong, complex passwords and enforce password complexity requirements. This reduces the likelihood of successful brute force attacks by increasing the difficulty of guessing or cracking passwords.

6. Monitor and log failed login attempts: Enable logging of failed login attempts to identify potential brute force attacks or patterns of suspicious activity. Regularly review these logs to detect and investigate any abnormal login behavior.

7. Implement multi-factor authentication (MFA): By implementing MFA, even if an attacker manages to guess or crack a password, they would still need an additional authentication factor (such as a unique code or biometric verification) to access the account. This adds an extra layer of security against brute force attacks.

By implementing account lockout policies, you can significantly reduce the effectiveness of brute force attacks, making it much more difficult for attackers to gain unauthorized access to user accounts.

# LOG FILE

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)


14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr
3302576859], length 73: HTTP: GET / HTTP/1.1
14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
…<a lot of traffic on the port 80>...


14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?
greatrecipesforme.com. (24)
14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A
192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649
ecr 0,nop,wscale 7], length 0
```

```
14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags
[S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS
val 3302989649 ecr 3302989649,nop,wscale 7], length 0
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
…<a lot of traffic on the port 80>...
```