# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| 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) |
|

**The first DNS & HTTP Traffic log file shows the source computer your.machine.52444 sending a request to the destination URL dns.google.domain. then the second section shows the destination replying back to the source computer using the IP address 203.0.113.22**

|  |
| --- |
| **Section 2: Document the incident** |
| 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 |

**The .36086 means that the source computer of your.machine.36086 is using port 36086 directly to the destination url of yummyrecipesforme.com/http. HTTP is commonly associated with port 80 the destination acknowledged the request and sent back Flag (S) which means that a connection has been started. The time of connection is 14:40 the communication between Source and Destination lasts about 2 mins between the 14:40 and 14:20 according to the timestamps and the next DNS Request.**

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| **I recommend implementing both stricter password policies to force stronger passwords within the company, and I also recommend implementing MFA or Multi-Factor authentication so that the company has greater control and safety from anyone who is trying to get access to the company’s information when they do not have clearance or need to do so.** |