Nicholas Clement Nicl7004

1. Mac Addresses: 52:54:00:12:35:03, 52:54:00:12:35:02. IP Addresses: 10.0.2.15, 10.0.2.3. Gathered the mac address from statistics -> conversations, gathered IP from ‘info’ tab after filtering for ARP protocol.
2. !!!!!!!!!!!!
   1. Destination: RealtekU\_12:35:02 (52:54:00:12:35:02)
   2. Many of the commands sent to the telnet sever are in plaintext, and can be seen by an adversary.
   3. Show ip bgp
   4. SSH (secure shell). Allows you to still execute commands on a remote machine but encrypts the transmission.
   5. Dst: login.live.com.nsatc.net (131.253.61.100)
   6. There is a method called domain masking. One way to achieve this is to use virtual hosting where the server serves several websites based on the content of the http header.
   7. Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b) – SHA256, Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f) – SHA 256, Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a) – SHA, Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xc009), Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013), Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014), Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0xc012), Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA (0xc007), Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA (0xc011), Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x0033), Cipher Suite: TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA (0x0032), Cipher Suite: TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0045), Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0039), Cipher Suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA (0x0038), Cipher Suite: TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0088), Cipher Suite: TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x0016), Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f), Cipher Suite: TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (0x0041), Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035), Cipher Suite: TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x0084), Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a), Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005) –All use variations of SHA, Cipher Suite: TLS\_RSA\_WITH\_RC4\_128\_MD5 (0x0004) – MD5
   8. MD5 is worrisome, it is susceptible to length extension attacks. MD5 can be quickly preformed with a strong GPU (billions of attempts per second) as well.
   9. The sever decides to use Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014).
   10. 10.0.2.15 uses the bing domain at time 62.6
   11. The protocol used between the client and the search engine was http, it allows us to see the cookies passed to the search engine.
   12. “is my search engine secure”
   13. Users can protect themselves from passive listeners by using https connections, encrypting all traffic.
3. Five years.