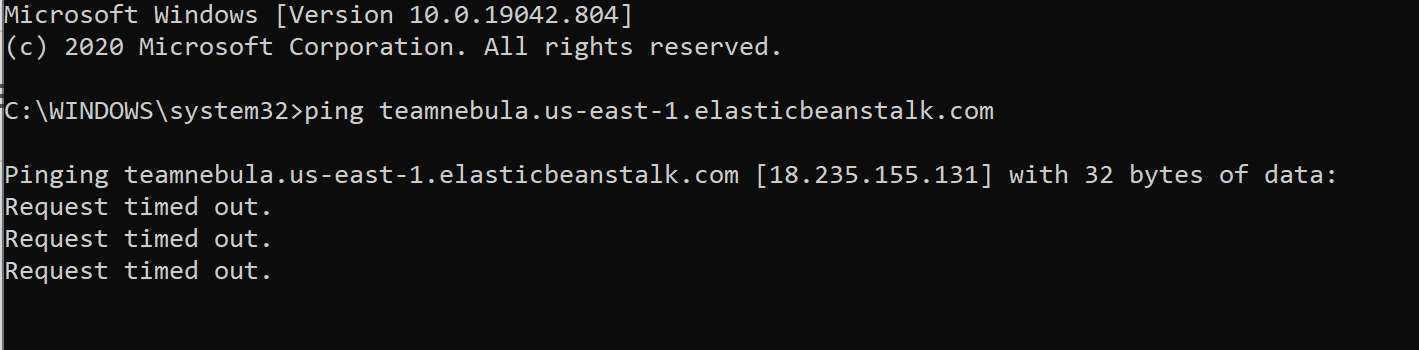
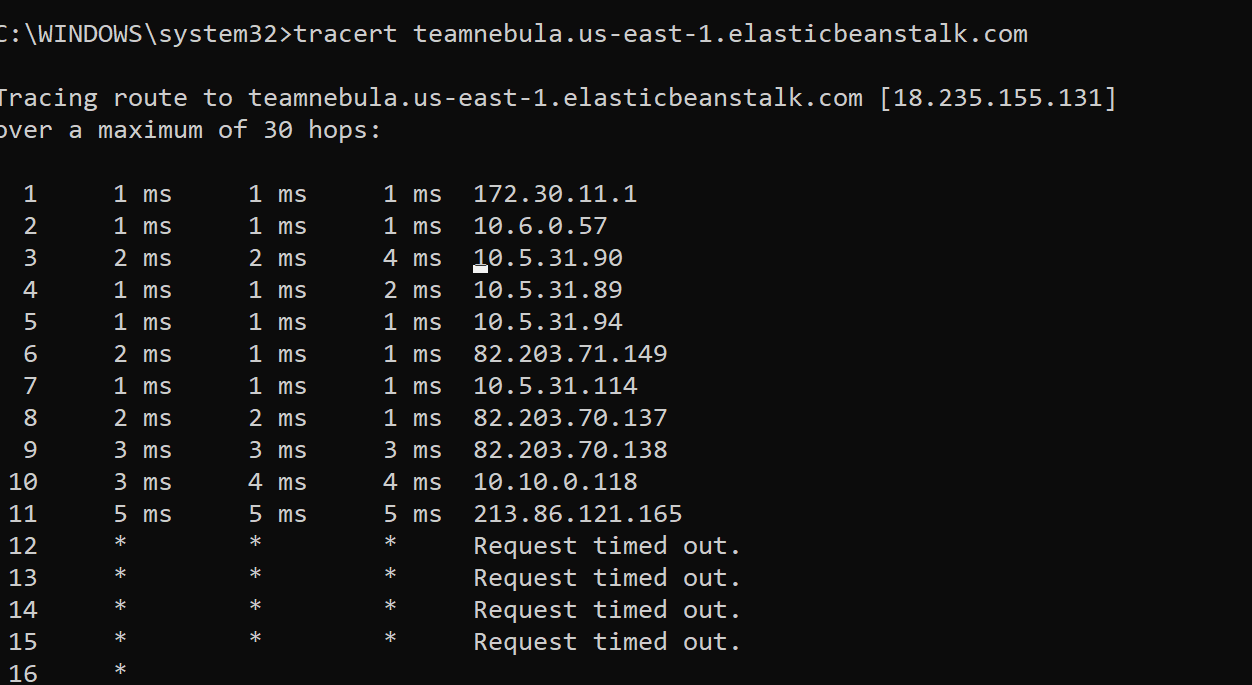
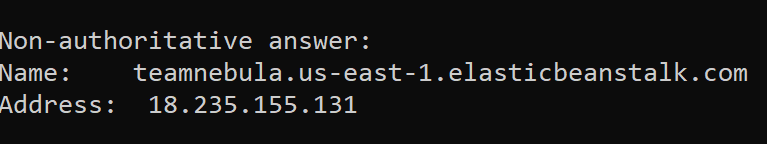
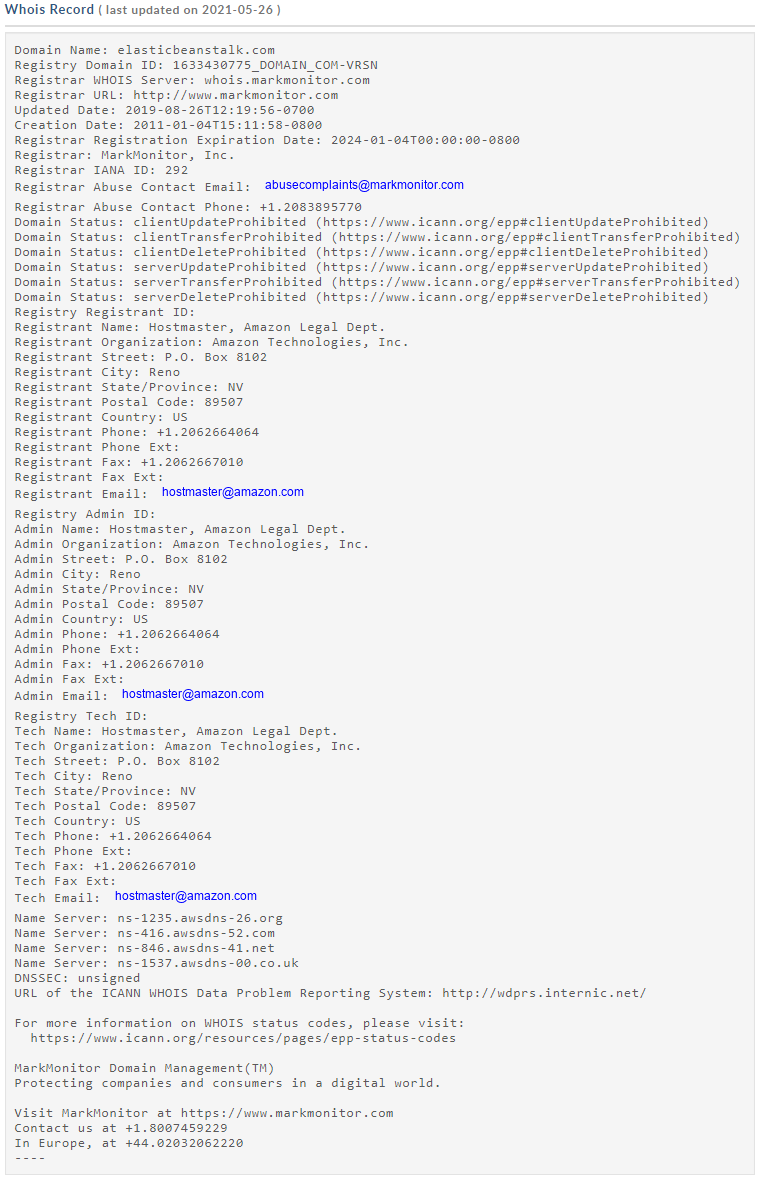
basic tools/ scans we have used:  
  
Windows CMD:

1. Ping

Information: The web site cannot be pinged



1. Tracert  
   Information: Each member has different result. Usually 13-30 hops, with 1-30ms TTL: 
2. Nslookup: The ip of the website is easy to find via nslookup, which is 18.235.155.131:  
   
3. Other Whois records:  
   All this information can be discovered by accessing domaintools.com



How this will shape the type of pen tests you will undertake after your initial report:

External Pen test: With the web site information, we can simulate the malicious activities to identify security holes in the web site. This helps us understand:  
- vulnerabilities are in the web site  
- how they could be exploited  
- impacts would be if an attacker were successful.

Web application penetration testing: After having obtained the web site information, we can introduce a web app penetration test including:  
 - database injections (if have)  
 - cross-site scripting (XSS)  
 - broken authentication