Practical 1

Monday, 1 August 2022 7:20 PM

Exercises

1. For the host 92.60.36.108, it is running openssh version 7.4p1. There are no vulnerabilities associated with this version.
2. MyCompany
   Issuer: C=US, ST=WA, L=Seattle, O=MyCompany, OU=IT
3. os:"DSM 6.2.2" country:"MY" the top 4 IP addresses are:
   121.121.196.202, 175.144.145.175, 175.143.191.113 and 121.121.196.202
   121.121.196.202 is running the ftp service dsm version
4. Only one.
   os:"windows xp" country:"es" city:"pamplona"
5. Sites found: golomtbank.com and egolomtbank.mn
   who.is(egolomtbank.mn)
   108.59.161.6(1), 108.59.162.6(1), 108.59.163.6(1) and 108.59.164.6(1)
   The number of ports open on each (in brackets)
6. Who.is(http://www.kurgan-city.ru/) IP 85.233.128.162
   it is running a squid/3.5.6 server on port 3128 has the following vulnerabilities:
   CVE-2019-12528 and CVE-2019-12529
7. Using who.is the IP for seek.com.au is 13.55.41.93
   host 202.69.217.11 isn't up
   command nmap --script ssl-enum-ciphers -p 443 13.55.41.93
   TLS v1.0
8. Wacek or axel
9. who.is(golomtbank.com)
   103.51.60.83
   The HTTPS service (port 443) is up
   command nmap --script ssl-enum-ciphers -p 443 103.51.60.83
   TLS v1.2