ISEC3002 Penetration Testing and Defence Workshop 1

What is Shodan?

Shodan is a search engine for finding various type of devices, server, services, and operating system connecting to Internet. Shodan can search for things like webcam, linksys, cisco, netgear, and SCADA by scanning the entire Internet and parsing the banners that are returned by online devices.

Some of the Shodan Filters

city: find devices in a particular city
country: find devices in a particular country
geo: you can pass it coordinates
hostname: find values that match the hostname
net: search based on an IP or /x CIDR
os: search based on operating system
port: find particular ports that are open
before/after: find results within a timeframe

Perform the following search examples and analyse the result:

- apache city:“San Francisco”
- nginx country:“ES”
- Server: gws hostname:“google”
- server: "apache 2.2.3"
- Server: SQ-WEBCAM
- "Siemens, SIMATIC" port:161
- html:"def_wirelesspassword" // Wifi Passwords:
- Android Webcam Server
- os:"windows xp"
- org:"Google"
- geo:"48.1667,-100.1667"
- nginx before:13/04/2020 after:13/04/2018
- has_screenshot:true city:"George Town" // has_screenshot:
- NETSurveillance uc-httpd // Surveillance Cams:
- title:"citrix gateway"
- "\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00" // Windows RDP Password
- net:34.98.0.0/16
- "MongoDB Server Information" port:27017 -authentication // Mongo DB servers
- "220" "230 Login successful." port:21 // FTP servers allowing anonymous access
- x-jenkins 200 // Jenkins
- NCR Port:"161" // Open ATM
- "Android Debug Bridge" "Device" port:5555 // Android Root Bridge
- port:23 console gateway // Telnet Access
- "ETH - Total speed" // Etherium Miners
- "Android Debug Bridge" "Device" port:5555 // Android Root Bridge

Shodan Command-Line Interface Cheat Sheet

- pip install shodan
- shodan init PRIVATE_API_KEY
- shodan
- shodan myip
- shodan host shodan host 63.X.X.X
- shodan count Apache Tomcat/8.5.13
- shodan search --fields ip_str,port,org Apache Tomcat/8.5.13
- shodan download Apache Tomcat/8.5.13
- shodan parse --fields ip_str,port,org --separator " - " Apache.json.gz

Exercise 1. What is the OpenSSH version running on the current servers connecting to Internet (e.g. 92.60.36.108)? If there are any vulnerabilities associated with that version of the service, specify the impact in term of confidentiality, integrity and availability.

Exercise 2. What is the of the Certificate Authority used by the site hosted on 146.67.160.215?

Question 3. What are the IP addresses of the organisations that are running the Synology DiskStation Manager (DSM) 6.2.2-24922 OS that are located in Malaysia? Which pf these organisations is running the DiskStation version of the ftp service?

Question 4. How many systems are running some version of Windows XP in Pamplona Spain?

Question 5. What are the IP addresses of the first four name servers for the Golomt Bank (that have P06 in the name) and how many ports are open on each name server? (Hint: who.is , shodan.io)

Question 6. Specify two Squid related vulnerabilities for the following site: www.kurgan-city.ru

Question 7. What is the lowest version of TLs supported by seek.com.au (IP address 202.69.217.11)?

Question 8. Specify a username for an account on the server at 185.51.118.38. (Hint: shodan.io, Remote Desktop Protocol)

Question 9. What is the highest level of TLS support provided by the Golomt Bank site?

Reference:

https://thedarksource.com/shodan-cheat-sheet/#country
https://www.shodan.io/dashboard
https://github.com/jakejarvis/awesome-shodan-queries
https://www.exploit-db.com/docs/english/33859-searching-shodan-for-fun-and-profit.pdf
https://who.is/
https://who.is/whois/egolomt.mn