Network and Information Security

Lab Information Gathering

Ethical hacker

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities hat a malicious hacker could potentially exploit.

Passive information gathering

A lot of important information can be passively gathered and subsequently used in a direct attack or to reinforce other attacks targeted at an organization. Some Web Hosting service providers provide Website analysis that may pose a risk to security of an organization.

Active information gathering

Unlike passive information gathering, active information gathering collects the most updated and current data. The information collected in this manner can be influenced by various factors that include your current location, ISP, network constraints, etc. This information can be used to investigate the current state of the target.

Zenmap

Zenmap or Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. It is useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Read more at www.nmap.org

NetCraft

Netcraft is an internet services company providing internet security services, including anti-fraud and anti-phishing services, application testing, code reviews, and automated penetration testing. It also provides research data and analysis on many aspects of the internet. Netcraft has explored the internet since 1995 and is a respected authority on the market share of web servers, operating systems, hosting providers, ISPs, encrypted transactions, electronic commerce, scripting languages and content technologies on the internet. Visit www.netcraft.com

Task: Information Gathering

Using Zenmap and NetCraft to scan www.nwpu.edu.cn. Gather and compare the information collected.

1. What is its Ip address?
2. Type the IP address in the browser to access the webpage, explain your observations.
3. Who is the IP owner?
4. What is the server’s operating system?
5. What type of web server is being used?

6. What is its server-side scripting technology?
7. Can you find the email for the domain admin of this website for a possible phishing attack?
8. What is the ‘Reverse DNS’ for the website?
9. Who is the domain registrar?
10. What is nameserver organization?
11. What company is hosting the website?
12. Where is the hosting company geologically located?

Information gathering can be achieved using various open source intelligence tools. A list of such possible tools can be found at: https://securitytrails.com/blog/osint-tools As always, use the tools within a controlled safe environment.