Omkar Gurav
BE IT
8048

Date: / /
Page No.:

ICS class Assignment 3 (Mapping CO3)

Write brief note on Network Security Scanners 1. Nmap 2. Metasploit.

→

1. Nmap:-

Nmap(network map) is a free & open-source security scanner that is used to discover hosts & services on a computer network, thus building a "map" of the network.

Nmap sends specially crafted packets to the target host & then analyses the responses to build a network map of the infrastructure.

It is written in C, C++, python & Lua.

Features & Capabilities:-

① Host Discovery: Identify machines on a network
② Port Scanning: Identify open ports on machines
③ Service & Version Detection: Identify version number of the running services
④ OS Detection: OS name, Description, Vendor name, Device Type & CPE
⑤ Automation: Nmap Scripting Engine (NSE) helps to automate several networking tasks

Date: / /
Page No.:

Typical Usage:-

① Security auditing of devices & networks
② Identifying various ports & services
③ Build infrastructure inventory
④ Identify vulnerabilities

2. Metasploit:-

Metasploit is a penetration testing platform that enables you to find, exploit & validate vulnerabilities.

Penetrating testing is a domain within information security which involves conducting deep security testing of the deployed infrastructure. Its focus is to identify & fix vulnerabilities before the vulnerabilities could be discovered & exploited by the attackers. Metasploit is one of the most used tools in the security industry & offers several capabilities.

It is written in Ruby.

Features & Capabilities:-

① OS Fingerprinting: Identify OS details
② Identify open ports & running services
③ Conduct vulnerability scan
④ Exploit know vulnerabilities manually or automatically

Scanned with CamScanner

⑤ Password cracking

Typical Usage:-

① Penetration testing
② Conducting security audit
③ Vulnerability reporting & compliance verification