Cyber

02/20/24

API- set of rules and tools that defines how different programs communicate with each other

FTP- used for transferring files from client to server unencrypted port 21 encrypted port 990

SMB Server message block- protocol for file sharing, printer sharing and network communication between windows devices.

Telnet- used for remote command line access to device port 23 unencrypted replaced by ssh

SSH- encrypted remote command line access port 22

Rysync- efficient tool used for synchronizing files between systems often over ssh backing up files

RDP- remote desktop protocol- used for graphical remote access on windows.

NMAP- command line used for port scanning, running services and versions, determines operating system, and vulnerabilities in a network.

MongoDB- open source no SQL database designed to handle large amounts of unstructured data. storing data in json like documents bson format.

NMAP Scans- basic scans

Nmap -sP <target> - ping scan checks which hosts are online without scanning

Nmap -sL <target> - Lists targets without scanning

Port scans-

Nmap -sS <target> SYN Stealth scan sends syn packages and listens for responses, stealthier

Nmap -sT <target> TCP connect uses full tcp handshake less stealthy but works without root/admin

nmap -sU <target> - scans for open UDP ports

nmap -p- <target> Full port scan scans all 65,535 ports instead of default 1000.

Service and version detection-

nmap -sV <target> identifies service versions running on open ports

nmap -A <target> agressive scan enables os detection, version detection script scanning and traceroute.

OS and firewall detection-

nmap -O <target> attempts to determine the operating system

nmap -f sends fragmented packets to bypass firewalls.

nmap -D RND:10 <target> spoofs additional IP addresses to hide real source of scan.

cat command is used to read, display and combine file contents

Django- full featured web framework