◉SCANNING TOOLS◉

- **Prepared By :-**

  MAHESH SARJERAO GIRHE

  ◈[MSG]◈

Follow me ✔

1. NETWORK SCANNING TOOLS

Nmap (Network Mapper)

- **Purpose**: Network discovery and security auditing.
- **Key Features**:
  - Host discovery to identify live systems.
  - Port scanning to detect open/closed/filtered ports.
  - OS and service detection.
  - Scriptable interaction via NSE (Nmap Scripting Engine).
- **Best For**: Penetration testers, network administrators.
- **Platforms**: Windows, macOS, Linux.
- **Example Command**:

```
nmap -A -T4 target_ip
```

(Performs aggressive scan with OS and service detection).

Masscan

- **Purpose**: High-speed port scanning.
- **Key Features**:
  - Capable of scanning the entire Internet in minutes.
  - Customizable scan rates for large-scale assessments.
- **Best For**: Large-scale network research and scanning.
- **Platforms**: Windows, Linux, macOS.
- **Example Command**:

```
masscan -p80 192.168.1.0/24 --rate=1000
```

(Scans port 80 across the specified subnet).

Advanced IP Scanner

- **Purpose**: Detect and manage network devices.

- **Key Features**:
  - Identifies active devices and open ports.
  - Supports remote desktop and SSH capabilities.
- **Best For**: Small to medium-sized networks.
- **Platforms**: Windows.

2. VULNERABILITY SCANNING TOOLS

Nessus

- **Purpose**: Comprehensive vulnerability assessment.
- **Key Features**:
  - Detects misconfigurations, outdated software, and CVEs.
  - Compliance checks for standards like PCI-DSS, HIPAA.
  - Custom scan templates.
- **Best For**: Enterprises for vulnerability management.
- **Platforms**: Windows, macOS, Linux.
- **Example Use Case**: Scanning internal networks for missing patches.

OpenVAS (Greenbone Vulnerability Management)

- **Purpose**: Free, open-source vulnerability scanning.
- **Key Features**:
  - Regular updates with vulnerability feeds.
  - Advanced scheduling and reporting.
- **Best For**: Those needing a free alternative to Nessus.
- **Platforms**: Linux, Docker.

Qualys

- **Purpose**: Cloud-based vulnerability management.
- **Key Features**:

  - Continuous monitoring of vulnerabilities.
  - Built-in compliance reporting.
  - Easy scalability with cloud-based deployment.
- **Best For**: Organizations needing large-scale vulnerability scans.
- **Platforms**: Cloud.

3. WEB APPLICATION SCANNING TOOLS

Burp Suite

- **Purpose**: Web application penetration testing.
- **Key Features**:
  - Intercepts HTTP/S requests via proxy.
  - Automated and manual testing for vulnerabilities.
  - Comprehensive scan for OWASP Top 10 issues.
- **Best For**: Security professionals testing web apps.
- **Platforms**: Windows, macOS, Linux.

OWASP ZAP (Zed Attack Proxy)

- **Purpose**: Open-source web application security scanner.
- **Key Features**:
  - Interception proxy for live traffic analysis.
  - Automated and manual vulnerability detection.
  - Integration with CI/CD pipelines.
- **Best For**: Web developers and testers.
- **Platforms**: Windows, macOS, Linux.

Acunetix

- **Purpose**: Commercial web vulnerability scanner.
- **Key Features**:

  - Detects SQL Injection, XSS, and other OWASP Top 10 vulnerabilities.
  - Advanced crawling for dynamic content.
- **Best For**: Enterprises with multiple web assets.
- **Platforms**: Windows, macOS, Linux.

4. WIRELESS SCANNING TOOLS

Aircrack-ng

- **Purpose**: Wireless network penetration testing.
- **Key Features**:
  - Captures and decrypts WPA/WPA2 traffic.
  - Supports packet injection for testing purposes.
- **Best For**: Testing the security of wireless networks.
- **Platforms**: Linux, Windows, macOS.

Kismet

- **Purpose**: Wireless network detection.
- **Key Features**:
  - Passive scanning of networks and devices.
  - Works with Wi-Fi, Bluetooth, and other radio protocols.
- **Best For**: Wireless network mapping and monitoring.
- **Platforms**: Linux, macOS.

Wireshark

- **Purpose**: Network protocol analysis.
- **Key Features**:
  - Captures and analyzes packets in real time.
  - Decodes hundreds of network protocols.
- **Best For**: Debugging and monitoring network traffic.
- **Platforms**: Windows, macOS, Linux.

5. MALWARE AND EXPLOIT SCANNING TOOLS

ClamAV

- **Purpose**: Open-source malware scanning.
- **Key Features**:
  - Real-time scanning for malicious files.
  - Cross-platform antivirus solution.
- **Best For**: Scanning servers and endpoints for malware.
- **Platforms**: Windows, macOS, Linux.

Metasploit Framework

- **Purpose**: Exploit development and vulnerability validation.
- **Key Features**:
  - Integrated vulnerability scanner.
  - Exploitation and payload delivery.
- **Best For**: Penetration testers validating vulnerabilities.
- **Platforms**: Windows, macOS, Linux.

6. COMPLIANCE AND CLOUD SCANNING TOOLS

Tenable.io

- **Purpose**: Cloud vulnerability and compliance management.
- **Key Features**:
  - Scans cloud assets for misconfigurations.
  - Built-in compliance checks (e.g., CIS benchmarks).
- **Best For**: Hybrid environments.
- **Platforms**: Cloud.

Prowler (AWS)

- **Purpose**: Security scanning for AWS environments.
- **Key Features**:

  - Compliance checks for AWS security standards.
  - Detects misconfigurations in IAM, S3, and EC2.
- **Best For**: AWS users needing periodic security checks.
- **Platforms**: Cloud (AWS).

7. SPECIALIZED SCANNING TOOLS

Nikto

- **Purpose**: Web server vulnerability scanning.
- **Key Features**:
  - Detects outdated software and misconfigurations.
- **Best For**: Quick scans of web servers.
- **Platforms**: Linux, macOS, Windows.

Retina Network Security Scanner

- **Purpose**: Enterprise-grade vulnerability scanning.
- **Key Features**:
  - Network and application-level vulnerability checks.
  - Automated reporting with patching recommendations.
- **Best For**: Large enterprise environments.
- **Platforms**: Windows, Linux.

Benefits of Using Scanning Tools

- Proactively identifies vulnerabilities before attackers exploit them.
- Automates repetitive tasks like port scanning and vulnerability assessments.
- Ensures compliance with regulatory standards.
- Saves time and improves accuracy in large IT environments.

Connect with Me

📧 **Email**: girhemahesh777@gmail.com

🔗 **LinkedIn**:
https://www.linkedin.com/in/maheshgirhe7875

🌟 **Follow Me for More Resources**:

💡 Stay updated with the latest **cybersecurity insights, tips, and tools**!
👉 Feel free to reach out for collaboration or queries.