Reconnaisance with nmap

Izdihar

cyber673

whoami

Izdihar Sulaiman

Husband, Father, Co-founder (cyber673), Avid CTF Player

Principal Consultant @ Swarmnetics 👨🏽‍💻

Placed (🥇 / 🥈 / 🥉) at CyberBattle CTF (Brune) 8 out of 9 times

CVE-2022-40317 (lonely XSS CVE)

CISSP, GXPN, OSEP, OSWE, OSCP, OSWA, OSWP, CRT, CPSA, BSCP, eMAPT...

=> izdiwho.com <=

nmap

- **Discover**: Map network devices & services.
- **Identify**: OS, versions, vulnerabilities.
- **Gather**: Essential intel for security assessments.

Host Discovery

- **Command**: nmap -sP 192.168.1.0/24

- **Explanation**:
  - -sP: Ping scan to find live hosts.
  - 192.168.1.0/24: Target network range.

Service Enumeration

- **Command**: nmap -sV 192.168.1.100

- **Explanation**:
  - -sV: Version detection to identify services.
  - 192.168.1.100: Target IP address.

OS Fingerprinting

- **Command**: nmap -O 192.168.1.100

- **Explanation**:
  - -O: OS detection to guess the operating system.
  - 192.168.1.100: Target IP address.

Different Scan Types

- TCP Connect Scan (**-sT**): Full TCP handshake, basic.
- TCP SYN Scan (**-sS**): Stealthy, half-open (requires root).
- UDP Scan (**-sU**): Scans UDP ports (slow).
- Ping Scan (**-sP**): Host discovery.
- Comprehensive Scan (**-sC**): Uses default NSE scripts.

Quick Port Scan

- **Command**: nmap -F 192.168.1.100

- **Explanation**:
  - -F: Fast scan to quickly identify common open ports.
  - 192.168.1.100: Target IP address.

Combining Techniques

- **Command:** nmap -A 192.168.1.100

- **Explanation:**
  - -A: Aggressive scan combines OS/version detection, script scanning, and traceroute.
  - Comprehensive intel gathering.

Nmap Scripting Engine (NSE) for Recon

- **Automate banner grabbing**: nmap --script banner <target>
- **Find HTTP titles**: nmap --script http-title <target>
- **Discover SMB info**: nmap --script smb-os-discovery <target>
- **Enumerate SSL/TLS issues**: nmap --script ssl-* <target>

Beyond Recon: Troubleshooting

- **Verify connectivity**: nmap -p 80,443 <target> (Check web ports).
- **Check firewall rules**: Identify filtered ports.
- **Diagnose DNS issues**: Check if DNS server is responding.

Beyond Recon: Inventory Management

Discover all devices on a network.

Track changes in network configuration.

Identify unauthorized devices.

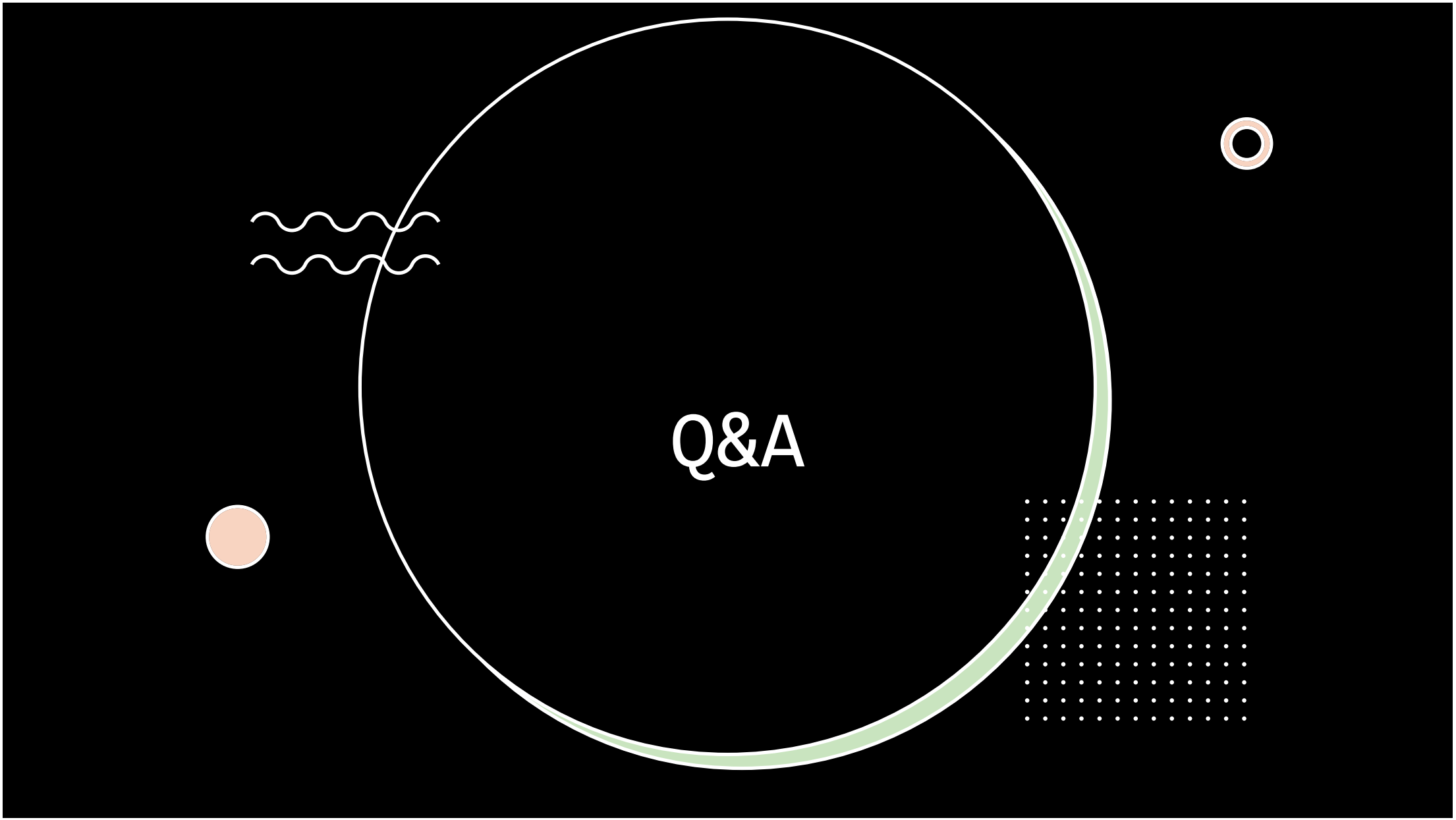
Example:

Analyzing Nmap Output

- Open: Service listening - potential target.
- Closed: No service active on that port.
- Filtered: Firewall blocking - investigate further

Ethical Scanning

- Always get permission!
- Avoid disruption.
- Respect privacy.


Q&A


Thank You!