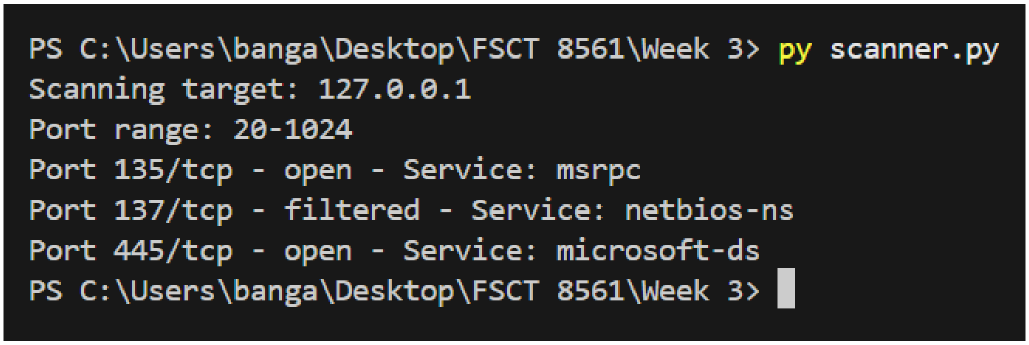
FSCT 8561 – Lab2: Network Scanning & Enumeration – Python Nmap Port Scanner

By: Jose Bangate, A01271709

Part 5 – Reflection Questions

1. Port scanning reveals which network services are exposed on a target system.
2. Because it enables an attacker to find out which services are accessible on a target system, port scanning is frequently the initial stage of an assault.
3. By keeping an eye on network traffic and limiting service exposure, defenders can identify or stop port scanning.
4. Basic port scanning has a number of drawbacks. It doesn't indicate whether the services behind the ports are genuinely vulnerable. It just displays which ports react. Ports may be blocked or hidden by firewalls and IDS/IPS systems, which could result in scans missing services or reporting them as filtered.

Part 6 – Security Analysis



```
PS C:\Users\banga\Desktop\FSCT 8561\Week 3> py scanner.py
Scanning target: 127.0.0.1
Port range: 20-1024
Port 135/tcp - open - Service: msrpc
Port 137/tcp - filtered - Service: netbios-ns
Port 445/tcp - open - Service: microsoft-ds
PS C:\Users\banga\Desktop\FSCT 8561\Week 3>
```

The target system's port scan (127.0.0.1) identified a number of network services with significant security implications. Specifically, TCP port 135 (msrpc) and 445 (microsoft-ds) were found to be open by the scan, however TCP port 137 (netbios-ns) was noted as filtered. These services can greatly expand a system's attack surface and are frequently connected to Windows networking and file-sharing features.

Microsoft Remote Procedure Call Services, which facilitate inter-process communication across a network, use port 135 (msrpc). This service may be targeted for enumeration for exploitation if it is exposed needlessly, especially if the system is not properly patched. In the past, system compromise and remote code execution have been made possible via flaws in RPC services. Server Message Block (SMB) connectivity, which facilitates file sharing, printer sharing, and remote administration, uses port 445 (Microsoft-ds). Because they have been used in significant assaults like ransomware outbreaks that took advantage of known SMB vulnerabilities, open SMB services are particularly dangerous.

A Firewall or filtering rules may be in place if port 137 (netbios name service) is present in a filtered state. Even if filtering lessens direct vulnerability, the service's detectability still gives attackers useful reconnaissance data. By assuming that the system is probably a Windows host, an attacker could adjust their attack plan.

By concentrating on service-specific assaults, attackers can misuse this information. Attackers can try credential brute-force assaults, take advantage of unpatched vulnerabilities, or utilize network enumeration to find shared resources and user accounts when they are aware that SMB and RPC are present. This information aids attackers in prioritizing targets and lowering noise in subsequent attack stages, even in the event that direct exploitation is unsuccessful.

Defenders should take a number of precautions to lessen exposure. Particularly on systems that aren't meant for file sharing, unnecessary services like SMB should be removed or restricted if they aren't needed. Only trusted IP ranges should be able to access these ports thanks to host-based firewalls. To mitigate known vulnerabilities, it is essential to have the operating system and services completely patched. Furthermore, intrusion detection systems and network monitoring can aid in the early discovery of questionable scanning or exploitation attempts. When taken as a whole, these steps greatly lower the risk related to network services that are exposed.