Step 3: Choosing the Right Tools and Commands

Name: Aum Panchal

Reg No: 22BCE8203

Kali Linux IP: 10.0.2.15

Windows IP: 192.168.0.113

# Tools and Commands

|  |  |
| --- | --- |
| Tool Name | Purpose and Commands |
| Nmap | Network scanning tool to discover hosts and services. Command: `nmap -sS 192.168.0.113` (SYN scan) |
| Maltego | Graphical link analysis tool for information gathering. Command: Run from GUI to visualize entity relationships. |
| nslookup | DNS query tool. Command: `nslookup google.com` |
| Yara | Tool for malware identification using rules. Command: `yara -r myrules.yar /path/to/files/` |
| Hydra | Brute force login cracker. Command: `hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.113 ssh` |
| Zphisher | Phishing tool to generate fake login pages. Command: `./zphisher.sh` (Run and select target site) |
| pfSense | Firewall/router distribution. Use for traffic shaping, firewall rules. Configurable via Web UI. |
| Bettercap | MITM tool for sniffing and manipulation. Command: `bettercap -iface eth0` |

Screenshots and images will be added in subsequent versions where necessary for commands demonstration and traffic analysis.