Network Security & Tools Quick Reference Guide

For Ethical Hackers

Equipment Hardening

Routers

- Change default credentials (admin/admin)
- Disable unused ports and WPS
- Enable WPA3 encryption
- Update firmware regularly

Switches

- Configure VLANs properly
- Disable unused ports
- Enable port security and Dynamic ARP Inspection
- Monitor for VLAN hopping

Firewalls

- Default deny policy
- Block unused ports: 21, 23, 135, 139, 445
- Enable logging and regular audits

Access Points

- Strong WPA3 passwords
- Disable WPS
- Monitor for rogue APs

Common Attacks & Detection

ARP Spoofing: Duplicate MAC addresses, sudden slowdown **MITM Attacks:** SSL warnings, unexpected

proxy settings

Unauthorized Access: Unknown devices, failed logins **DoS Attacks:** Service unavailability, high traffic

---

Essential Commands

Network Discovery:

```bash
nmap -sn 192.168.1.0/24
nmap -sS -p 1-1000 <target>
```

Wireshark Filters:

```
tcp.flags.syn == 1
arp.duplicate-address
http.request.method == GET
```

Traffic Monitoring:

```bash
sudo tcpdump -i eth0 arp
sudo arpwatch -i eth0
arp -a
```

Tool Selection Guide

Task	Tool
Network Discovery	nmap
Traffic Analysis	Wireshark
Wireless Monitoring	Kismet
ARP Monitoring	ARPwatch
Port Scanning	nmap

Critical Ports

Port	Service	Action
21	FTP	Block if unused
22	SSH	Restrict access
23	Telnet	Block (use SSH)
135/139/445	RPC/SMB	Block external
3389	RDP	VPN only