HOMELAB SECURITY CHECKLIST

- ✓ **DMZ**: Every public server should be on a network separate from your LAN.
- ✓ **IDS/IPS**: Setup an Intrusion Detection / Prevention System. Some Firewalls (such as UniFi's Security Gateway) have this built in.
- ✓ **VPN**: If you need access into your LAN remotely setup a VPN. OpenVPN is very popular, ZeroTier requires no ports to be open on your firewall.
- ✓ **Security/Vulnerability Scanner**: Regularly scan your LAN and public IP with Cloudflare's Flan Scan to find open ports and known vulnerabilities.
- ✓ **Separate Guest Wi-Fi**: Don't let guests onto your LAN when not needed.
- ✓ Setup **VLANS** on Managed Switches to separate traffic: DMZ, LAN, and Guest is good for a homelab.
- ✓ Use **Named User Accounts** where practical instead of having the entire family share a login
- ✓ **Battery Backup**: APC or CyberPower offer protection against brief power failures
- ✓ **Backups**: You must have offsite versioned backups of everything you don't want to lose.
- ✓ **Reset All Default Passwords**: Don't forget out of band management interfaces like IPMI.
- ✓ **Automatic Security Updates**: Make sure every device on your network is configured to install security updates automatically. Otherwise check at least once a month.
- ✓ **Continuity**: Give your family instructions on who to call and what to do should you perish so they don't lose any data. Make sure an acquaintance is familiar enough with your homelab.

- ✓ **Web Application Firewall**: If you have a public webserver at your house, put it behind Cloudflare for a little protection. Plus, it acts as a CDN giving you a performance boost.
- ✓ **SSH Key Authentication**: Disable password authentication.
- ✓ Install **Fail2Ban** on all Linux Servers
- ✓ Setup an **SMTP** server (or use SES, Mailgun or Sendgrid) for servers to send out alerts
- ✓ Setup **Network Monitoring** (Nagios, Zabbix, Icinga)
- ✓ Setup **Log Monitoring** (Splunk, Grafana, Kibana)
- ✓ Use a **Password Manager** such as KeePass or LastPass. Use strong unique passwords for every system.
- ✓ Register a real **domain** for your Homelab, NameCheap or Cloudflare are reputable registrars. That way you can access all your servers using a proper FQDN. Setup DNSSEC and DMARC.
- ✓ Use Let's Encrypt to **automatic SSL certs** (requires a domain name).
- ✓ **Secure DNS**. Use CleanBrowsing, OpenDNS, or 1.1.1.3 to prevent bad sites from loading.
- ✓ **Encrypt** all sensitive data at rest. Some systems like FreeNAS can encrypt the disks.
- ✓ Don't forgot **Physical Security**. Get a dog.
- ✓ Use **2FA** where possible

Have fun!

Thank you for considering the items on this security checklist! You may not be able to implement all of them right away, and some may be overkill for your environment and that's fine. Start with what is most interesting or most important. Enjoy learning! – Ben