Sean Tucker Resume

EMAIL: tucker090@protonmail.com
Linkedin: https://www.linkedin.com/in/sean-tucker-0809a0169/

OBJECTIVE:

Desire to be a Offensive Security Professional

School:

Completed my 2-year ATA degree and currently working on my bachelor's degree in Network Operations and Security at Western governor's university https://www.wgu.edu/online-it-degrees/network-administration-information-technology-security-bachelors-program.html

ABOUT ME:

I'm very passionate about information technology, I enjoy learning deep technical knowledge. I have a eagerness to learn, detailed oriented. Strong oral, written and documentation skills. Work great in small, medium or large teams. I have no problem learning new software on the fly. When not working or doing homework, I'm self-teaching myself Python/Bash programming, Cisco networking, Windows/Linux administration and penetration testing in my home lab.

SKILLS:

- Linux CLI, Cisco CLI
- Python, Bash
- Pfsense, Ubiquiti
- CentOS 7, Red Hat 7, Kali
- Windows XP, 7, 8, 10, server 2012/2016
- VMware, Virtual Box, Proxmox, Xenserver, Xcp-ng, Xen Orchestra
- Nextcloud, FreeNAS, Plex
- Microsft Office O365, Microsoft Word, Microsoft Excel, Microsoft Exchange Email
- Connect Wise, Team viewer, RDP, SSH, Telnet, VNC, openvpn, anyconnect, palo alto vpn
- SMB, NFS, UNC, FTP, TCP/IP, DNS, DHCP, LACP Nic bonding, openssl, HTTP, HTTPS
- Troubleshooting hardware, printers, Fast paced, Multi-tasker, Quick learner, lift over 90 lbs!

EXPERIENCE:

Company: VMC Keywords Studios

IT Help Desk Dec. 2018 to Nov. 2019 1 year

- Troubleshooting local and remote client requests through ticketing system and emails
- Re-imaging desktop and laptops
- Setting up Bit locker encryption
- Managing IT inventory assets and loading dock receiver
- Troubleshooting, installing or removing software
- Managing Microsoft AD accounts and Microsoft Exchange email accounts

Company: Northwest Business Technology Solutions (E3 gaming convention)

IT Network Support June 2018 1 week job

- Physically setting up Ubiquiti switches, routers, access points.
- Physically setting up tcp/ip printers. Running and crimping cat5 cables.
- Troubleshooting network connectivity problems.
- Managed Ubiquiti networking hardware, such as creating trunks, vlans, changing AP channels, bandwidth throttling.

Company: F1 Consultancy LLC (Microsoft and Google Convention)

IT Network Support July 2017 8 weeks

- Physically setting up Xirrus wireless access point arrays, Physically setting up switches, Physically setting up desktops / laptop computers, and tcp/ip printers. Running and crimping cat5 cables.
- Troubleshooting network connectivity problems.

Personal Home Project: (In Progress, Not Completed)

Xenserver Hosting the following:

Linux Administration July 2018 to Present

- Spacewalk, DHCP, DNS, Master/Master LDAP servers.
- Master/Master replication of Postgresql Pgpool-II.
- Spacewalk database import to Pgpool II.
- Puppet Master plugged into Spacewalk server.
- Iscitgt and nfs-kernel-server.
- Exported LUN and NFS share.
- Bakula installed using postgresql cluster to store its database.
- Two VM's with Tomcat, which has Jboss cache to replicate the session between the two tomcats
- Iptables-based NAT / round-robin load balancing between the two tomcat servers.
- Postfix installed to be able to send and receive email via a gmail account.
- Nagios for snmp monitoring the communication between every relevant service involved.
- Syslog daemon to listen to every other server's input along with logstash, or kibana, or greylog to parse logs.
- Puppet manifests authenticating to LDAP servers and registered with spacewalk and backed up bakula.
- Razor profile that hooks into each of these things to allow you to recreate from scratch, each individual server.
- Destroy every secondary machine created to allow the above profile to recreate and rejoin them to the clusters as needed.
- Documenting everything I did in the above, into a step by step process in a spreadsheet.

Personal Home Project: (Completed)
Xenserver Hosting the following:
Windows Administration July 2018

- Connected 2 Domain controllers as Active / Passive replication
- Setup OU's, forest, and computers connected to the domain controller
- Users Accounts for 3 different departments

Personal Home Project: (Completed)
Pfsense Router, Ubiquiti Switch and Ubiquiti Access points:
VPN / Vlan / Stronger Wifi Signal Aug. 2018 – Dec. 2018

- Openvpn
  - Access to my VM home lab setup on my Xenserver
- Vlans
  - Allow for good security posture for my wifi IOT and wifi cameras
- Access points
  - Creates multiple vlan ssids and long range wifi roaming

Personal Home Project: (Completed)
Cisco equipment:
Networking Jan 2019 to Present

- I practice Cisco CLI on 2 routers and 3 switches

Personal Home Project: (Completed)
FreeNAS Server: Aug. 2018 – Dec. 2018
Storage

- RAID 6 backup
  - Nextcloud file sharing service data are stored on the FreeNAS server
  - Xenserver VM's are stored and automatically backed up every week using delta backup
  - Plex video streaming data is stored on the FreeNAS server

Personal Home Project: (Completed)
Pentesting Lab *Dec. 2015 to Present*

- Raspberry pi Rouge AP
  - Reaver pin cracking, SSL stripping, Deauthing beacons, Website cloning, Pcap and wpa, handshake cracking, Ubertooth one Bluetooth hacking, Wifite, FruityWiFi framework, Aircrack, Fluxion
- Arduino Pro micro Bad USB / Rubber Ducky
  - Automated Reverse admin powershell payload
- Raspberry pi's connected to Cisco routers and switches
  - Simulate vlan hopping using yersinia on physical cisco equipment
- Vulnerable VM lab
  - LAMP stack hosting Mutillidae II and DVWA , metasploitable 2, My Linux VM project, My Windows VM project (I monitor my attacks with security onion).
- Tools I used
  - Metasploit framework, Veil Evasion, Wifite, Cobalt Strike / Armitage, FruityWiFi Framework, Burp Suite, Aircrack-ng, SEToolkit, Msfvenom, Netcat, Nmap / Zenmap, Sslstrip, URLsnark, Arpspoof, Wireshark, Crunch, Hydra, John the ripper / John, Hping3, Slowhttptest, Dnschef, Ettercap / Bettercap, Tcpdump, Sqlmap, The Harvester, Bluelog, Bluesnarfer, WPScan, Nikto, Macchanger, Proxychains, Hash-identifier, Fluxion, DHCPig, Other third party Git repo's tools.

Ext:

Read Violet python
Read Black hat python
Read Python crash course
Read Basic Security Testing with Kali Linux and Intermediate Security Testing with Kali Linux 2
I refer to the Red team field manual book
HackTheBox.eu
I regularly attend security conferences to learn more

EDUCATION:

- **Everett Community College** 2016-2018
- Associate degree
    - Intro to Information Technology
    - Device and Mobility fundamentals
    - Networking Fundamentals
    - Computing Hardware/Tech
    - Computing & Troubleshooting
    - Information Security Fundamentals
    - Linux Systems Administration
    - Server Administration Fundamentals
    - Network Application Support
    - Ethical hacking and counter measures
    - CCNA R&S: Introduction to Networks
    - CCNA R&S: Routing and Switching Essentials
    - CCNA R&S: Scaling Networks
    - CCNA R&S: Connecting Networks
- **Western Governors University** 2018-Present
- Bachelor's degree
    - Networks – C480
    - Network and Security – Applications – C178
    - Cloud Foundations – C849
    - IN PROCESS OF FINISHING

Certificates:

- **220-901 & 220-902 CompTIA A+**
  http://verify.CompTIA.org code: BYDC536PBHEE16CJ
- **N10-007 CompTIA Network+**
  http://verify.CompTIA.org code: 0D6CBREEYDEE1V3J
- **SY0-501 CompTIA Security+**
  http://verify.CompTIA.org code: 45CQ0WE3YDVE1FGE
- **CL0-001 CompTIA Cloud Essentials**
  http://verify.CompTIA.org code: 23EHZ0NEZGR11935
- **010-150 LPI Linux essentials**
  https://cs.lpi.org/caf/Xamman/certification/verify/LPI000382014/qxxlkaywgj
- **98-365 MTA Windows Server Administration Fundamentals**
  http://verify.certiport.com code: wdvGP-HaM4
- **98-366 MTA Networking Fundamentals**
  http://verify.certiport.com code: w6KVr-4SCx
- **98-367 MTA Security Fundamentals**
  http://verify.certiport.com code: wEKeh-4SCC
- **98-368 MTA Mobility and Device Fundamentals**
  http://verify.certiport.com code: wuLce-48aP