Systems Administrator Systems Administrator Systems Administrator - CyberStrata Leesburg, VA Work Experience Systems Administrator CyberStrata - Sterling, VA January 2016 to Present Conduct security audits of network systems (internal and external), including penetration testing of all public attack vectors and points of failure. Engage with active threat mitigation, bleeding edge methodologies. virtual infrastructure (layer 7 firewalls, VMware, Virtual Box), and network architecture. Work with and configure basic cloud services like AWS (Amazon Web Services) Provided support for a wide range of vendor gear, such as Juniper, Cisco, Huawei, TP-Link, Pal Alto, etc. Configured Cisco and Juniper hardware to meet client demands and needs. Education vocational Monroe Tech Academy 2017 to 2019 several dual-enrollment and advanced placement Heritage Highschool 2016 to 2019 Marymount University - Arlington, VA 2017 George Mason University, Potomac Arts Academy - Sterling, VA 2015 Skills CISCO (2 years), JUNIPER (2 years), MITIGATION (2 years), SECURITY (2 years), TESTING (2 years) Links https://www.linkedin.com/in/dominicwclark Certifications/Licenses Security+ 2018 to 2021 XPJH8S8V5ZLLVLW5 Network+ 2018 to 2021 YHK37CLXYR9PF9KM CTECH Certified Copper Specialist Present CTECH Certified Fiber Specialist Present Additional Information AREAS OF EXPERTISE Routing, Switching, & Firewall Management Mobile Sec, Malware, & Policy Penetration Testing Network Security, Implementation, & Operations Juniper & Cisco * Wireless, Ethernet, Optical Android, Unix/Linux, Windows OS IDS / IPS and Honeypot specialist (deployment / configuration). Have effectively configured and deployed solutions such as Honey Drive, Stratagem, ADHD, and other anti-exploitation strategy solutions. Extensive knowledge on opensource softwares for mitigation of passive, active, and external attacks. Experience with a wide variety of Operating Systems and their functions, including many flavors and variants of Android ROM's, Windows (server and client), and Unix based systems. Currently use Debian, CentOS, and Ubuntu systems daily. In possession of many custom and specialized distributions, including BlackHat Security, TopHat Security, and HackerSchool release distros. Comfortable and experienced with many integrated exploitation toolsets, including Metasploit console and its graphical counterparts: Armitage and Cobalt Strike. Familiar with OSINT (open source intelligence)

tools and methodologies: Maltego (and Sploitego) and Recon-NG. Innate knowledge of mobile (Android) based exploitation and monitoring tools, such as Csploit, zANTI, Intercepter-NG, and Wifite. Knowledge of network footprint and scanning tools such as Nessus, UnicornScan, AngryIP, and various front-ends for Nmap. Direct knowledge and experience with packet capture / forensics with an array to tools including Wireshark, Bettercap, Ettercap, Nessus, and OpenVAS. Strong skills with virtualization, working directly and maintaining VMWare workstations, servers, and network-boot clients (PXE boot). Experience with VMWare, VirtualBox, Hyper-V, QEMU, and other VM containers. Familiar with scripting in Python, Ruby, and Powershell; experience with object-oriented languages like C++, C#, Java Network Deployment and Configuration consultant, regularly working with Juniper, Cisco, Huawei, Pal Alto, and TP-Link hardware (switches / routers) to effectively run and maintain large scale network operations. Strong skills with post-assessment mitigation of vulnerabilities. Familiar with Endpoint Security products such as McAfee, Sophos, and Carbon Black. Experienced with installing and configuring malware, rootkit, anti-exploit, virtualization, and virus removal tools to minimize impact of a successful network penetration. Strong belief in Security In-Depth, CIA (confidentiality, integrity, availability), and principle of least privilege as it applies to internal network security. D. W. CLARK |

Name: Teresa Brown

Email: cliffordhanna@example.org

Phone: 370-505-5651x1506