Darnell Miller

Web & Mobile App Penetration Tester

Boca Raton, FL | **Phone:** 540-699-4954 | **Email:** darnellemiller@outlook.com | LinkedIn

Professional Experience

20 years experience in the professional field of technology. Strong background in Offensive Security, Networks, Servers, Cloud, Systems, Programming languages and strong ambition in offensive cyber security as penetration tester. Deliver high levels of customer service while providing clear communication. Long track record of completing projects and SLAs

Penetration Tester **Remote**
Bug Bounty Hunter Oct. 2023 – Present

- Penetration testing and vulnerability analysis for diverse client web applications, with a focus on identifying and
- exploiting vulnerabilities across a wide range of web applications, mobile apps and source code
- Created Python script that will check for valid emails in the target web app
- utilize github for additional security testing tools and python scripts for detailed testing
- Utilized Android Studio Meerkat | 2024.3.1 to test for vulnerabilities in Android applications using, setup virtual AVD
- and export Burp certificate
- Enumerate exploit user authentication with burp suite
- Configure burp suite attacks capture token and cookie, generated brute force list using crunch, send to intruder review
- results
- Reconnaissance tools such as the harvester utilizing multiple sources on targets
- automated Reconnaissance utilizing python scripts
- utilize Scapy with python (p.show) (traffic analysis with python) reading and viewing packets using Scapy
- developed python applications for network scanning
- python scripts for detailed port scanning vs nmap scanning entire range of ports causing alarms; searching for well
- known protocols
- Created and optimized Python scripts to automate data extraction, exploit vulnerabilities, and conduct efficient web
- scraping for reconnaissance and data analysis. This automation streamlined the penetration testing process, enabling
- faster identification of risks and deeper system insights.
- Specialized in comprehensive web application security testing with a focus on the OWASP Top 10 vulnerabilities,
- including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Security Misconfigurations,
- and Sensitive Data Exposure.
- Leveraged Burp Suite (version 2024.7.6) for in-depth analysis of HTTP traffic, automated scanning, and manual
- testing, enabling meticulous inspection of application requests, responses, and hidden parameters.
- Conducted thorough source code reviews and dynamic application walkthroughs to identify insecure coding practices,
- logic flaws, and improper input validation across complex applications.
- Utilized a range of industry-standard tools, including:
- Nmap: For port scanning, service identification, and network enumeration, pinpointing open services and
- misconfigurations that could be exploited.
- Shodan: Employed Shodan to search for and identify exposed systems and open services, providing a quick overview
- of potential attack surfaces and entry points.
- Gobuster: Used for directory and file brute-forcing to locate hidden and potentially vulnerable resources, including
- administrative directories and sensitive endpoints.
- Sublist3r and Amass: Performed DNS reconnaissance to discover subdomains and map attack surfaces, aiding in
- domain reconnaissance and expanding the scope of potential vulnerabilities.
- SQLmap: Automated the testing of SQL injection vulnerabilities, enabling fast and accurate validation of injection
- points.
- Nikto and Wfuzz: Conducted additional application testing to uncover parameter tampering, fuzzing, and exploit
- detection, enhancing application resilience against common attack vectors.
- Executed black-box and gray-box testing to simulate real-world attack scenarios, uncovering vulnerabilities in
- applications without prior knowledge of the underlying architecture. Applied advanced techniques for host header
- injection, Cross-Site Scripting (XSS), and parameter tampering, validating server-side input validation mechanisms
- and uncovering potential security weaknesses.
- Utilized advanced network enumeration and analysis tools such as Reconing and the Harvester to gather valuable
- data on targets, supporting initial reconnaissance and enabling a deep understanding of client infrastructure. Cross-
- referenced identified vulnerabilities with the Exploit Database and continuously monitored public vulnerability
- disclosures to stay current with evolving security threats and exploit techniques.
- Documented findings with extensive detail, delivering clear, actionable reports to client organizations. Each report
- included a thorough description of vulnerabilities, technical impact assessments, and step-by-step remediation
- recommendations. Maintained strict confidentiality and professionalism in all client communications, ensuring clients
- received the necessary guidance to address and mitigate discovered vulnerabilities effectively.
- Engaged in continuous professional development through Capture the Flag (CTF) competitions, security conferences,
- and hands-on labs to stay abreast of the latest advancements in penetration testing techniques and web application
- security.
- Active utilized github repositories for custom and automated penetration testing during detail vigorous penetration test,
- install github repositories for pentesting

Darnell Miller

Web & Mobile App Penetration Tester

Boca Raton, FL | Phone: 540-699-4954 **| Email:** **darnellemiller@outlook.com | LinkedIn**

- Edit, nano /etc/hosts config directing to target with DNS and IP address
- Utilize MITRE ATT&CK framework, CVE and Exploit database
- Experience using Hydra and Burp Suite brute force on vulnerable Web Applications.

SharePoint Developer | Junior Penetration Tester **Remote**

TransCore Nov 2017 – Oct. 2023

- Jira Ticketing system Graveyard Shift 12:00 AM - 9:00 AM EST
- exploiting vulnerabilities across a wide range of web applications, mobile apps and source code
- Created Python script that will check for valid emails in the target web app
- utilize github for additional security testing tools and python scripts for detailed testing
- Utilized Android Studio Meerkat | 2024.3.1 to test for vulnerabilities in Android applications using, setup virtual AVD
- Penetrate and report finding on corporate wireless networks for annual testing using Air-Crack ng
- Create new SharePoint Intranet pages for 7 different domains for sunpass, FDOT and TransCore.
- Conduct penetration testing across multiple web applications and networks conducting internal annual testing
- Assist Nightly hand over with engineers to maintain toll lanes to save company time and money for toll lane
- transactions
- Managed VMware vSphere 6.0 environments, including taking snapshots, creating LUNs, and performing VMotion
- migrations.
- Administered HPE Fibre Channel Switches SN6000B, 48-port and Dell SAN, carved out LUNs, and performed
- troubleshooting with vendor-specific tools for RAID controllers.
- Restored failed VMs using Veeam Backup & Recovery and performed routine Disaster Recovery tests and failover
- Led upgrades and decommissioning of legacy systems (Windows Server 2003/2008), ensuring smooth transitions
- Diagnosed issues with Cisco ASA 5510, Nexus 9332 C switches, and performed configuration backups using SFTP
- Verified LDAP replication and supported Active Directory operations across 7 different domains.
- Apply Zero Day patches System Center Configuration Manager
- Administrator HPE fibre channel switch 48 port 16 GB Sn6000b with putty, ssh, SNMP, remote monitoring HPE
- Upgrade and decommission legacy server 2003, and 2008 creating snapshots using Vsphere
- Troubleshoot cisco firewall ASA 5510, Nexus 9332C Switch and backup configurations using SFTP
- Assist with infrastructure support with 7 different Domains on Hyper-V
- Carved out new LUN in Dell SAN for new MDC toll lanes
- Identify faulty tools using vendor specific tools and crystal disk on storage Raid Controllers
- Restored failed VMs using Veeam BackUp and Recovery on Hyper-V
- Verify LDAP replication, FSMO roles
- Responds to Veeam Alerts configured via email group
- Deploy Chef images to custom built linux and windows nodes for highway toll lane transactions for FDOT & Sunpass

NASA HQ **Washington, DC**

Network Security Engineer July 2016 – Nov 2017

- Reported to Darlene Brown NASA HQ director and Melissa Forrest DMI subcontractor HITSS contract Arlington and
- DC office
- Managed Temp role in HITSS contractor office network with T1 line to NASA HQ, administer OSPF, GRE Tunnel, and
- IPsec
- Service Now ticketing system
- conduct network assessment and identify vulnerabilities in current network
- Lock all usb ports symantec AV
- Performed Active Directory vulnerability analysis, focusing on user authentication, Kerberos ticketing issues, and
- permissions misconfigurations.
- Conducted thorough network vulnerability assessments and implemented security protocols to mitigate risks across
- access points and communication channels.
- Collaborated closely with Cisco to replace legacy and vulnerable network components, including switches and
- routers, providing a seamless T1 line connection to NASA HQ and enhancing overall system resilience.
- Diagnosed and resolved complex Active Directory replication issues within the contractor office, ensuring consistent
- user authentication, resource access, and directory synchronization across multiple sites.
- Led troubleshooting efforts for IPsec VPN and OSCP network configurations, successfully establishing and
- maintaining a secure VRE (Virtual Routing and Forwarding) tunnel for encrypted data transmission between remote
- locations.
- Monitored network performance and security through real-time analysis tools, proactively identifying and mitigating
- potential bottlenecks, packet loss, and unauthorized access attempts.

Darnell Miller

Web & Mobile App Penetration Tester

Boca Raton, FL | Phone: 540-699-4954 **| Email: darnellemiller@outlook.com | LinkedIn**

- Configured and enforced strict firewall rules and access control lists (ACLs) to protect critical infrastructure and ensure
- compliance with NASA's stringent security policies.
- Oversaw system patching, hardware upgrades, and network documentation, maintaining comprehensive records for
- disaster recovery planning and ongoing audits.
- Effectively communicated with cross-functional teams, vendors, and NASA's IT leadership to align network strategies
- with organizational goals, addressing evolving project requirements and adhering to rigorous standards for operational
- continuity and cybersecurity compliance.

Innovative Inc **Washington, DC**

Network Systems Engineer Oct 2015 – July 2016

- Utilize autotask and Labetch
- Assisted clients in achieving PCI compliance through extensive network vulnerability assessments utilizing trustwave.
- Administer Linux Centos servers resolving issues bash scripts with DHCP
- Disable guest session Ubuntu lsb_release -a
- Configure basic firewall, router and switches meraki, hp, cisco 3800,
- Played a key role in assisting clients to achieve and maintain PCI compliance, utilizing extensive knowledge of
- network security and compliance standards.
- Conducted thorough network vulnerability assessments and applied hands-on expertise to secure infrastructures,
- reduce risks, and protect client assets.
- Proactively guided clients through the PCI compliance process, performing rigorous network scans using Trustwave
- and other compliance tools to identify vulnerabilities.
- Analyzed scan results and collaborated with clients to close exposed ports, reinforce firewall security, and configure
- access controls in line with PCI standards.
- Provided detailed documentation to ensure clients understood compliance requirements and could sustain ongoing
- adherence to industry regulations.
- Active Directory Management and Permission Structuring
- Managed and optimized Active Directory (AD) security permissions, working directly with clients to review and adjust
- user roles, group policies, and access controls.
- Led consultations with stakeholders to ensure permissions aligned with organizational security protocols, reducing
- unnecessary access and enhancing system integrity.
- Regularly conducted AD audits to identify potential security gaps and applied best practices for AD security
- management, growing my expertise in enterprise-level user and resource management.
- Developed robust network infrastructures using Cisco Meraki routers and Fortigate firewalls, configuring and
- maintaining secure, resilient environments for clients across multiple sites.
- Utilized Cisco Meraki's dashboard to monitor network performance, troubleshoot connectivity issues, and apply
- security updates, ensuring high availability and protection against potential intrusions.
- Configured Fortigate firewalls with custom rules and security settings tailored to client-specific needs, implementing
- advanced threat management and secure access.
- Established and maintained secure site-to-site VPN connections, enabling seamless communication and data sharing
- across distributed client locations. Configured VPNs to support remote workers and interoffice communication,
- ensuring data privacy and integrity through encrypted tunnels. Monitored VPN connections to ensure reliable uptime,
- promptly addressing any connectivity or security concerns.
- Worked closely with client leadership and IT teams to align security strategies with business goals, address
- compliance needs, and continuously improve network security. Regularly provided updates, recommendations, and
- technical support to ensure client satisfaction and project success.
- Communicated effectively with clients, translating complex security and network concepts into clear, actionable steps.
- Assist engineers with network Installation and configuration providing on call support when short staffed
- Administered VMware ESXi hosts and Hyper-V , utilizing vMotion for VM migrations, and ensured integrity of backups
- (full, incremental, and differential)
- Worked with HP Smart Array RAID controllers and managed storage solutions from Pure Storage and Cohesity.
- Utilized Datto and Veeam for backup and disaster recovery, ensuring zero data loss during VM migrations.
- Created Power BI reports connected to SCCM SQL database, and automated patch deployments across servers and
- workstations
- Supported Cisco Hyperflex and Fortinet Networking infrastructures, ensuring smooth operation of storage and
- network resources.
- Played a key role in Disaster Recovery drills and systems maintenance, ensuring minimal downtime.
- Complete migrations of VMs using Vmotion and vSphere 6.0
- Complete and verify integrity of backups full, incremental and differential
- Troubleshoot Raid Controllers identify faulting drives in raid array HP Smart Array
- Verify LDAP replication
- Power BI Desktop with SCCM reporting
- Patch VMware ESXI host using putty
- Verify and troubleshooting any Backup errors
- Provide Tier 3 escalated help desk support to Junior staff, Provide clear communication to users
- Configure new Fortigate and Cisco Meraki routers, firewalls and switches onsite deployments

Darnell Miller

Web & Mobile App Penetration Tester

Boca Raton, FL | **Phone:** 540-699-4954 | **Email:** darnellemiller@outlook.com | LinkedIn

Educational Accomplishments

Junior Penetration Tester *Jan 2024*
Try Hack Me

Web Application Penetration Tester *Feb 2024*
Try Hack Me

Full Stack Developer *Dec* 2023
London App Brewery

Security+ *June* 2017
Udemy

Pentest+ *June* 2020
udemy

Google Cyber Security *May* 2023
Coursera