Dwight Walker

Penetration Tester - PENTESTDC, LLC
Washington, DC 20024
dwight.walker445@gmail.com
202-498-4299

Security + Certified, 3 years in network security/ penetration testing, over 10 years of network experience. Will have the EC-Council's Certified Ethical Hacking (CEH) and Amazon Web Services Architect Associate certifications before the end of this year.
Willing to relocate: Anywhere

Work Experience

Penetration Tester

PENTESTDC, LLC
January 2013 to Present

• Used HP Fortify to find and mitigate errors using Java.
• Found and offered suggestions for fixing vulnerable coding errors.
• Remediate a wide range of security vulnerabilities, including the OWASP top10
• Provided guidance in helping the DC government's Department of Human Services pass the US government's Social Security Administration, and the IRS's compliance audits.
• Consulted with the client to help with setting up policies and procedures to comply with the HIPAA security rule.
• Administered the Oracle Identity Management logon system to provision user access in 2000 + user environment.
• Helped secure the new District of Columbia Access System software for revision 2 updated web application and portal.
• Configured SLUNK security information and event management to log invalid logon issues.
• Created SPLUNK dash boards to view valid and invalid logons.
• Foot printing and scanning networks suing public information about a target of evaluation.
• Scanned networks for web vulnerabilities using Nessus.
• Logged onto Nessus Server using port 8834.
• Ran credentialed scans and allowed others to run scans with provisioned access.
• Created credentialed scans to find vulnerabilities in their network and web applications.
• Edited policies and enabled plugins to run scans.
• Ran scans for all 65,535 ports, or and IP hosts ranges.
• Provided Asset Discovery scans for selected or all hosts on the network.
• Enumerated target hosts for more information about the particular host.
• Created policies for HIPAA compliance using Nessus.
• Helped clients develop business continuity planning and backup plans as part of compliance.
• Downloaded and interpreted reports.
• Provided consulting on findings.
• Scanned ports using NMAP to find services being used and open ports to send payloads to the network.
• Provide risk assessments and security plans to healthcare concerns to comply with HIPAA.

• Used Netcat to transfer files and communicate with remote hosts.
• Executing payloads using Metasploit.
• Helped create policies, procedures, guidelines, and baselines for companies.
• Used Burpe Suite to scan web applications and attack vulnerabilities.
• Mapped Web Applications using Burpe Suite by following links, sending forms, and stepping through the phases process of request/response urls.
• Completed recon and analysis of Web app to scan for vulnerabilities to exploit the web app.
• Attacked content discovery using Burpe Intruder to brute force third party apps, and redirecting url's,

• Authentication, session handling using cookies, authentication, and access control on wep app using automated and manual testing..

Network Administrator

Democracy Data & Communications
January 2008 to January 2013

• Used Active Directory to administer the network.
• Assisted in MS Exchange migration.
• Installed workstations, servers, network printers, and routers.
• Provided day to day technical support to the network devices.
• Resovled connectivity issues with the cables, patch panels, host configurations.
• Created and installed new Domains using Active Directory.

Help Desk Analyst 4/2005 to1/2008
National Claims Administrative Services
• Provided help desk support to include logon/off issues.
• Helped with network printing issues, slow network responses, email issues.
• Provided desktop support to resolve host pc issues and problems.

Education

Certification

University of Maryland University College - Largo, MD

Skills

Java., Metasploit., Nessus., NMAP, SPLUNK, Penetration Testing, Ethical, CEH

Additional Information

COMPUTER SKILLS
Software
• Javscript, Python, SQL, Java, CC++
• Proficient in: Kali Linux, Metasploit, Meterpreter, Backtrac 5 R3, Nessus, Wireshark, NMAP, Prorat, Burpe Suite, IBM App Scan, Acunetix, Superscan, Angry IP, IDA Pro, Nitko2, Witko
• Familiar with: OWASP, Samurai WTF, Pen testing Execution Standard (PTES), Snort, and SPLUNK
• Database: Microsoft SQL Server and Microsoft Access

- Platforms: Windows 7-10, some Linux
- Expert Computer User