QUADRANT

**Donn Gordon**
**(240)-498-7266**
**donn.cyber@gmail.com**
**Gaithersburg, MD,**
**Web Penetration Tester**

**Professional Summary:**

- Licensed web penetration tester in which I identify, protect, detect, respond.
- Structed External, Internal, Firewall, IDS, Web, SQL, Database, Mobile, Cloud Penetration testing and expert in a professional reporting.
- Give the client a better understand what, where and how to change the security control by following the regulation for the NIST etc.
- Monitor the security of critical systems (e.g., e-mail servers, database servers, web servers, etc.) and make changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted irregularities.
- Conduct network vulnerability assessments using tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures.
- Conduct routine social engineering tests, such as Phishing exercise.
- Plan and coordinate the testing of recovery support and business resumption procedures while ensuring the recovery and restoration of key IT resources and data and the resumption of critical systems within the desired timeframe.

**Education:**
Associates Degree: Westwood College - Applied in Network Security
Bachelors Degree: University of Phoenix - Software Development

**Certificates:** CEH, ECSA, LPT and OSCP

**Professional Experience:**
**RCMT, Deerwood, MD** **Jan 2018-Present**
**Web Penetration Tester**
Objectives during the CSPT activities are to conduct the following:

- Conduct vulnerability scanning, validation and exploitation. The focus of which is to identify potentiallynew vulnerabilities and to validate previously identified vulnerabilities
- Conduct phishing/client-side attack and training within the organization and recommend users for remedial training
- Conduct Web Application Scanning and Penetration Testing. Scan run against TA web application and web services to identify any known vulnerabilities accessible on the public facing TA infrastructure
- Engage in Security Assessment Report that contain vulnerability and penetration test results. The report will include, at a minimum:
  - Executive summary, which provide a summary of the types of test performed and assessment methods used. I also identify the vulnerabilities, characterized by severity.
  - Build a risk matrix that details vulnerability identified and ranks by severity.
  - Detail description with the applicable artifact (screenshots, logs, etc.) of vulnerabilities identified and exploited.
- Tested Sensitive information and Reporting
  - Vulnerabilities discovered during CSPT activities that present an immediate risk or which may allow immediate access to the Client system will be reported promptly to the IT manager and Incidence Response Lead.
  - In discovery of information that relates to serious crimes such as sabotage or threats or plans to commit offenses that threaten a life or could cause significant damage to or loss of the client property.
  - Discovery of personally identifiable information will be promptly reported to the IT manager
- Follow the ROE, that will engage in the following activities:
  - Passive Reconnaissance

- Active Reconnaissance

- Penetration Testing
- Attacks against the confidentiality, integrity and availability of information system assets, include hardware, software, firmware and information being processed
- Exploitation errors and misconfigured, spoofing (simulation of trust
- Password cracking and buffer overflows

**768 Alternative Solution, Fairfax Virginia** **Feb. 2007 to Jan. 2018**
**Web Penetration Tester**
**Responsibilities:**

- Formulating hard-hitting measures with a view to secure the domains that can portray threat to the significant information owned by the organization
- Identifying efficient measures of sustaining network security at a constant rate
- Becoming familiar with the business functions and infrastructure of the organization
- Performing sophisticated penetration examinations for the purpose of ascertaining the technical weaknesses existing the computer systems
- Finding out effective ways of manipulating the vulnerable domains of the systems Maintaining high level of security of the information that is crucial for the business growth of the organization
- Conducts research with external information on events, incidents, outages, threats, and technical vulnerabilities.
- Coordinates individual organizational actions to reduce overall shared risk.
- Possesses elementary information about various platforms such as Linux, Windows, Unix, etc
- Well acquainted with the regular Web Server Security concerns and advanced concepts associated with system networking
- Proficient with the processes associated with shell scripting, PHP, Perl, Java, and SQL
- Expert with the workings of software technologies that include SSH & Anti-virus, Visual Studio 6, and Apache Web Server
- Eagerness to inculcate new skills and learn about the latest technological aspects related to ethical hacking
- Scanning Ports and seeking vulnerabilities for mitigation purpose
- Examining patch installations
- Engaging in social engineering concept such as ‘Dumpster diving’.
- Sniff the network
- Analyze incoming and outgoing packets
- Pre-penetration Testing Steps
- Extract a company information
- List Employees of the Company
- Use the Nessus and OpenVas Tools Scan the Network
- Bypass firewalls by using various tools such as HTTport, and HPING3
- Check live system and open ports
- Understanding when and how web application connects to a database server in order to access data
- Extracting basic SQL injection flaws and vulnerabilities
- Testing the Web application for Blind SQL injection vulnerabilities
- Scanning web server and analyzing the reports
- Information on securing web application and web servers
- Extract database and user credentials, using the tool Havij
- Secure your cloud network from Heartbleed vulnerability
- Perform banner grabbing and so fingerprinting
- Identify network vulnerabilities
- Draw network diagram of vulnerable host
- Use the Browser Exploitation Framework (BeEF)
- Attain Credential of a user account in plain text
- User name and User Groups
- List of Computers, their operating systems, and ports
- Machine Name, Network resources, and Services

- List of Shares on Individual host on the network
- Policies and Passwords
- Making training available as part of a company’s security awareness and training program
- Keeping security procedures and policies updated
- Co-working with developers to provide advice on security requirements and needs
- Providing feedback for an organization fixing security issues
- Making new penetration tests and tools.
- Documentation for penetration testing report

**Expert Testing Tools**: Nessus, Nmap, Nikto, Comonview Voip Analyzer, foundstone, qualysguard, paros proxy, webscrab, Sql map, Microsoft baseline security analyzer, GFI languard, kismet, Cain & Abel, brutus, netsparker, burp suite, skipfish, acunetix, hp web-inspect, firebug, w3af, asteroid and Burpsuite, ACAS (Assured Compliance Assessment Solution), NetApp, Akamai, Splunk, Wireshark

**PROTOCOLS:** Ethernet, TCP/IP, SSH
**SOFTWARE/OS:** MS Office Suite- (Visio/Project), McAfee, Remedy, Windows, UNIX, Linux
**DATABASES:** Oracle, SQL Server
**PROGRAMMING:** Programing and scripting in HTML, .NET, C#, Perl, Python and JAVA.
**Operating System:** Windows, Linux, and Centos