Anthony Tillman II

Fort Washington, MD
tillmana@gmail.com
Cell: 240-838-6556

Summary:
Over seven years of experience exclusively in the Information Security industry. Focusing primarily on Vulnerability Management and Penetration Testing, worked to improve the security posture of high-profile organizations in the federal space and the private sector. Used knowledge of Red Team and Blue Team methodologies to serve the Department of Defense, State Department, and several Fortune 500 companies. Contributed to the development of consulting practices, by rewriting and updating service offerings and descriptions that are more actionable to the sales force. Excels in team environments, as well as working independently.

Education:
University of Maryland University College, Adelphi, MD B.S., Computer and Network Security December 2019 (Est.)

Clearance:
Current Secret

Technical Skills:
Metasploit Framework, SQLmap, Nessus, Qualys, Retina, Social Engineers Toolkit, DNSrecon, Nmap, BurpSuite, Masscan, Vega Web Proxy, ZED Attack Proxy, SQLMap, Linux, Kali Linux, MySQL, Python, Macromedia Dreamweaver, HTML, Adobe Photoshop, Fireworks

Work Experience:
Senior Penetration Tester (Project Basis)
Lunarline Inc. 6/2016-Present

- *Hands-on penetration testing, security test planning, vulnerability analysis, and exploitation of application and systems level designs*
- *Ethical hacking mindset with proven professional experience in assessing diverse network and system architectures in a comprehensive manner.*

Security Consultant/Penetration Tester
DXC Technology 6/2013-Present

- *Provide consulting services to Fortune 500 clients across industry verticals*
- *Lead large scale penetration testing engagements, developing project schedule, creating attack plans, and assigning roles to team members*
- *Conduct remote and onsite assessments of client web applications and networks using Nmap, Metasploit, Burpsuite, SQLMap, Maltego and other tools on Kali Linux*
- *Conduct group Red Team operations using Colbalt Strike, allowing the team to share sessions, credentials and other pertinent information*
- *Use open source intelligence to profile companies and their employees to determine viable attack vectors on engagements*
- *Perform social engineering assessments via phone, email, and onsite*
- *Create custom websites and malicious emails to elicit target action in social engineering campaigns*
- *Create scenario scripts for social engineering engagements to determine potential outcomes and exit strategies for phone and onsite tests*
- *Perform vulnerability assessments using automated tools (Nessus, Qualys) and manual verification of findings*
- *Conduct policy gap Analysis to help clients bridge deficiencies in industry standards/best practices*
- *Perform threat modeling to aid customers in identifying potential attacks and vectors*
- *Convey vulnerability findings in written reports, providing actionable recommendations*
- *Improve internal documentation by updating current offerings and service definitions*

Security Engineer/Penetration Tester

EWA Information and Infrastructure Technologies, Inc., Arlington, VA 4/2011-6/2013

- *Provide direct support to Federal client*
- *Perform security audits and penetration testing of networks and web applications*
- *Techniques utilized include SQL Injection, Directory Traversal, Password Recovery, Fuzzing, Pass-the-Hash, Etc.*
- *Utilization of Metasploit Framework, Social Engineers Toolkit and other security auditing tools to identify and execute attack vectors.*
- *Analyze output of automated tools and perform manual verification of all findings. ● Compile data into readable, fluent reports for client consumption.*
- *Recommend remediation and countermeasure techniques to better protect clients ● Brief stakeholders regarding major vulnerabilities and industry best practices to remediate those threats*

IT Specialist

Department of the Navy, Arlington, VA 6/2009-4/2011

- *Manage Accounts, network rights, and access to systems and equipment*
- *Troubleshooting*
- *Conduct vulnerability scans using Retina and DISA's Gold Disk ● Install software patches and updates.*
- *Compile reports of vulnerabilities and actions taken to mitigate the risk posed by those vulnerabilities ● Review audit logs*
- *Executed antivirus scans and eradicate viruses and malicious code.*
- *Respond to customer service requests*
- *Conduct vulnerability scans, access machines and provide security patches and updates*
- *Implemented the command's first RIM Blackberry Pilot Plan which deployed handsets to management personnel OCONUS and CONUS*
- *Engineered and implemented an asset management framework to account for Blackberry Devices*

Relevant Training:

Interconnecting Cisco Network Devices Pt. 1
Interconnecting Cisco Network Devices Pt. 2
Certified Ethical Hacker
Contracting Officers Technical Representative
InfoSec Institute Ethical Hacking
NSA Blue Team Bootcamp
Offensive Security Penetration Testing with Kali
Red Teaming with Hak5

Certifications:

(ISC)2 Certified Information Systems Security Professional (CISSP)
CompTia A+
CompTia Network+
CompTia Security+
EC-Council Certified Ethical Hacker (C|EH)
IACRB Certified Penetration Tester (CPT)

Accomplishments:

Defcon 23 Social Engineering CTF Top 10 Finisher