Project 3

1. **Step 1 – Organizational Boundaries**
    a. Find an organization.
    b. Describe the background of that organization
        i. Purpose
        ii. Organizational structure
        iii. Network system description
        iv. Diagram of the organization (LAN, WAN, intranet, extranet, internet)
    c. Can be real or unreal. Create a network.

2. **Step 2 – Organizational Threats**
    a. Internal Threats
    b. External Threats
    c. Threat Intelligence
        i. OPM Breach
        ii. OPM vs Your Organization
            1. Differences
            2. Similarities

3. **Step 3 – Scanning the Network**
    a. Network Monitoring Tools **(SAR)**
        i. MBSA (Summarize Findings)
        ii. OpenVAS (Summarize Findings)

    b. TCP/IP Model **(SAR & RAR)**
        i. Definition of TCP/IP Model (Suite of Protocols)

4. **Step 4 – Identifying Security Issues**
    a. Password Management
    b. Identity Management
    c. Cain & Abel

5. **Step 5 – Firewalls and Encryption (SAR)**
    a. Role
        i. Confidentiality
        ii. Integrity
        iii. Availability

6. **Step 6 – Threat Identification (SAR)**

a. Cyber Attacks
b. Remediation & Mitigation Techniques
    i. Access Control
    ii. Database Transaction
    iii. Firewall Log Files
    iv. Encryption
        1. Purpose
        2. Function

7. Step 7 – Wireshark Network Analysis (SAR)

a. Results

8. Step 8 – Suspicious Activity (SAR)

a. Results
    i. Real-time Detection
b. Firewall State
c. Recommendations for Remediation

9. Step 9 – Risk and Remediation (RAR)

a. Risk (NIST, 2012)
b. Remediation
c. Security Exploitation
d. Threats/Vulnerabilities
    i. Likelihood of occurring
    ii. Impact to organization

Project 3 Deliverables

Security Assessment Report (SAR)

I. Title Page
II. Abstract
III. Purpose
IV. Organization
V. Scope
VI. Methodology
VII. Data
VIII. Results
IX. Findings
X. Conclusion
XI. References

Risk Assessment Report (RAR)

I. Title Page
II. Abstract
III. Threats
IV. Vulnerabilities
V. Likelihood of Exploitation
VI. Impact from Exploitation
VII. Remediation
    a. Cost/Benefit Analysis
VIII. Plan of Actions & Milestones
    a. Creation
    b. Monitoring
    c. Closing

IX. Conclusion
X. References

References

1. Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy: Recommendations of the National Institute of Standards and Technology*. (Special Publication 800-41). U.S. Department of Commerce, National Institute of Standards and Technology. Retrieved August 5, 2016, from http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

2. U.S. Department of Commerce, National Institute of Standards and Technology (NIST). (2012). *Information security: Guide for conducting risk assessments* (Special Publication 800-30). Retrieved August 5, 2016, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

3. http://2012books.lardbucket.org/books/getting-the-most-out-of-information-systems-v1.3/index.html

4. Introduction to parallel & distributed algorithms by Carl Burch, Hendrix College, August 2009

5. https://lti.umuc.edu/contentadaptor/topics/byid/820a901d-e710-4e8c-9b19-8aaf41baf091

6. Singhal, A., Winograd, T., & Scarfone, K. (2007). *Computer security: Guide to secure web services: Recommendations of the National Institute of Standards and Technology* (Special Publication 800-95). Retrieved from http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

7. https://www.computer.org/cms/CYBSI/docs/Top-10-Flaws.pdf

8. https://umuc.equella.ecollege.com/file/6aa8bfb8-7053-4fed-94f6-2547e454c501/1/web/viewer.html?file=https://umuc.equella.ecollege.com/file/830d820d-c407-49df-ab83-2886fd3a7cbf/1/NISTCloudComputingStandardsRoadmap.pdf

9. Distributing Computing by John DeNero http://composingprograms.com/pages/45-distributed-computing.html

10. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology*. (Special Publication 800-145). U.S. Department of Commerce, National Institute of Standards and Technology. Retrieved August 4, 2016, from nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

11. Trusted Computing Strengths Cloud Authentication by Eghbal Ghazizadeh, Mazdak Zamani, Jamalul-lail Ab Manan, and Mojtaba Alizadeh for the Sceintific World Journal, Volume 2014, Article ID 260187, 17 pages https://www.hindawi.com/journals/tswj/2014/260187/

12. http://www.sciencedirect.com/science/article/pii/S1877042814038592 On this site is access to three more resources

13. Gelles, M. G., & Mitchell, K. (2015). Top 10 considerations for building an insider threat mitigation program. *Journal Of Threat Assessment And Management*, *2*(3-4), 255-257. doi:10.1037/tam0000059

14. Haktip 3: Packet Sniffing 1010: Promiscuous Mode https://lti.umuc.edu/contentadaptor/topics/byid/6c2ac65f-688d-40b2-8856-9f17e7fc0a30

15. CIT 480: Security Computer Systems: TCP/IP Security https://umuc.equella.ecollege.com/file/6aa8bfb8-7053-4fed-94f6-2547e454c501/1/web/viewer.html?file=https://umuc.equella.ecollege.com/file/c14f0796-e3ff-4883-b5bb-6b7bd3bf2eac/1/SecuringComputerSystemsTCPIPSecurity.pdf

16. Bourgeois, D. T. (2014). *Information systems for business and beyond.* The Saylor Academy. Retrieved August 5, 2016, from http://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond.pdf

17. Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices by Steven Thomason Global Journal of Computer Science and Technology Network, Web & Security, Volume 1, 2 Issue 13, Version 1.0, Year 2012

18. Spoofing Attacks on Packets and Methods for Detection and Prevention of Spoofed Packets by K. Phalguna Rao, Ashish B. Sasankar, Vinay Chavan from International Journal of Science Engineering and Advance Technology

19. http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_agents/ComputerNetworkIDS.pdf

20. Defending against denial of service attacks https://securosis.com/assets/library/reports/Securosis_Defending-Against-DoS_FINAL.pdf

21. Mell, P., Kent, K., & Nusbaum, J. (2005).*Guide to malware incident prevention and handling: Recommendations of the National Institute of Standards and Technology*. (Special Publication 800-83). U.S. Department of Commerce, National Institute of Standards and Technology (NIST). Retrieved August 5, 2016, from http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

22. https://globaljournals.org/GJCST_Volume16/1-State-of-the-Art.pdf

23. http://file.scirp.org/pdf/JCC_2014061709494898.pdf

24. Attack Possibilities by OSI Layer https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

25. http://www.sciencedirect.com/science/article/pii/S1877050915007000

26. NIST SP 800-115

27. Mastering Metasploit. (n.d.). Retrieved August 4, 2016, from https://archive.org/details/MasteringMetasploit

28. Singh, G., Goyal, S., & Agarwal, R. (2015). Intrusion Detection Using Network Monitoring Tools. *IUP Journal Of Computer Sciences*, *9*(4), 46-58.

29. Risk Assessment https://umuc.equella.ecollege.com/file/6aa8bfb8-7053-4fed-94f6-2547e454c501/1/web/viewer.html?file=https://umuc.equella.ecollege.com/file/870f372d-3479-4ba0-9083-b8c7c9efaec9/1/RiskAssessment.pdf

30. High level organization of the standard http://www.pentest-standard.org/index.php/Main_Page