Security Testing Essential Training Resources

1. Understanding Security Assessments

- NIST – https://www.nist.gov/
- Verizon Data Breach Investigations Report – https://enterprise.verizon.com/resources/reports/dbir/
- Privacy Rights Clearinghouse – https://www.privacyrights.org/data-breaches
- National Council of ISACs – https://www.nationalisacs.org/
- International Organization for Standardization – https://www.iso.org/
- ISO 27001 Security – http://iso27001security.com/
- ISO 27001 (Official) – https://www.iso.org/isoiec-27001-information-security.html
- NIST Cybersecurity Framework – https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework
- NIST SP 800-53 Rev. 4 – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- Payment Card Industry Data Security Standards Council – https://www.pcisecuritystandards.org/
- HIPAA – https://www.healthit.gov/
- NERC – https://www.nerc.com/
- GLBA – https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
- NIST SP 800-115 – https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

2. Your Testing Environment

- VirtualBox – https://www.virtualbox.org/
- VMware Player – https://www.vmware.com/
- Kali Linux – https://www.kali.org/
- Nmap – https://nmap.org/
  - Nmap Cheat Sheet – https://highon.coffee/blog/nmap-cheat-sheet/
- Nessus Home – https://www.tenable.com/products/nessus-home
- Wireshark – https://www.wireshark.org/
- Lynis – https://cisofy.com/
- Center for Internet Security – https://www.cisecurity.org/
  - CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks/
  - CIS-CAT Lite – https://learn.cisecurity.org/cis-cat-landing-page
- Aircrack-ng – https://aircrack-ng.org/
  - Troubleshooting Wireless Driver Issues in Kali – https://docs.kali.org/installation/trouble-shooting-wireless–driver-issues
  - Aircrack–ng Tutorials

    https://www.aircrack-ng.org/doku.php?id=tutorial

    https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

    https://www.aircrack-ng.org/doku.php?id=cracking_wpa
- Hashcat – https://hashcat.net/
- OWASP – https://www.owasp.org/
  - OWASP Zed Attack Proxy (ZAP) – https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
  - OWASP Juice Shop – https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
  - OWASP Vulnerable Web Applications Directory – https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project

3. Planning Your Assessment

- Risk Assessments
  - NIST SP 800-30 Rev. 1 – https://csrc.nist.gov/
  - Factor Analysis of Information Risk – https://www.fairinstitute.org/
  - SimpleRisk – https://www.simplerisk.com/
- Security Control Assessments
  - NIST SP 800-53 Rev. 4 – https://csrc.nist.gov/
  - OpenFISMA – http://openfisma.org/
  - ISO 27002:2013 – https://www.iso.org/
  - ISO27k Toolkit – http://iso27001security.com/
- Compliance
  - PCI DSS – https://www.pcisecuritystandards.org/
  - HIPAA – https://www.healthit.gov/
  - HIPAA Security Risk Assessment (SRA) – https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
  - Unified Compliance Framework – https://www.unifiedcompliance.com/
- Host Vulnerability Scanners
  - Nessus – https://www.tenable.com/
  - Qualys Cloud Platform – https://www.qualys.com/
  - Nexpose – https://www.rapid7.com/
- Web Application Vulnerability Scanners
  - VERACODE – https://www.veracode.com/
  - AppScan – https://www.ibm.com/security/application-security/appscan
  - Sentinel – https://sentinel.com/
  - Acunetix – https://www.acunetix.com/
  - Checkmarx – https://www.checkmarx.com/
  - Synopsys – https://www.synopsys.com/
  - Burp Suite – https://portswigger.net/burp

  - OWASP ZAP –https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

- Penetration Testing
  - Penetration Testing Execution Standard – http://www.pentest-standard.org/
  - Open Source Security Testing Methodology Manual – http://www.isecom.org/
- Additional Security Testing Resources
  - OWASP Testing Project – https://www.owasp.org/index.php/OWASP_Testing_Project
  - CIS Benchmarks – https://www.cisecurity.org/cis-benchmarks/
  - Phoenix OWASP Chapter – https://www.owasp.org/index.php/Phoenix/Tools
  - SecTools – https://sectools.org/

4. Review Techniques

- Log Management Tools
  - Splunk – https://www.splunk.com/
  - QRadar – https://www.ibm.com/
  - LogRhythm – https://logrhythm.com/
  - AlienVault – https://www.alienvault.com/
  - Syslog – native to Linux systems
  - Syslog-ng – https://www.syslog-ng.com/
  - Graylog – https://www.graylog.org/
  - ELK Stack – https://www.elastic.co/
- Critical Log Review Checklist for Security Incidents –
  - https://zeltser.com/cheat-sheets/
- Firewall Ruleset Reviews
  - Nipper – https://titania.com/
- System Security Configuration Scanners
  - Lynis – https://cisofy.com/lynis/
  - CIS-CAT – https://learn.cisecurity.org/cis-cat-landing-page
- File Integrity Monitoring
  - Tripwire – https://www.tripwire.com/
  - OSSEC – https://www.ossec.net/

5. Identifying Your Targets

- Passive Network Scanners
  - Nessus Network Monitor -

    https://www.tenable.com/products/nessus/nessus-network-monitor
  - Passive Network Sensor –

    https://www.qualys.com/passive-network-sensor/
- OSINT Resources
  - Shodan – https://shodan.io/
  - Censys – https://censys.io/
  - BGP Toolkit – https://bgp.he.net/
  - DNS Zone Transfer Lookup – https://www.ultratools.com/tools/zoneFileDump
  - ZoneTransfer.Me – https://digi.ninja/projects/zonetransferme.php
- Vulnerability Severity Scoring
  - CVSS – https://www.first.org/cvss/
  - CWE – https://cwe.mitre.org/
- Wireless Security Testing Tools
  - Aircrack-ng – https://aircrack-ng.org/

6. Vulnerability Validation

- F5 Report
  - Lessons Learned From a Decade of Data Breaches – https://www.f5.com/labs/articles/threat-intelligence/lessons-learned-from-a-decade-of-data-breaches-29035
- Additional OSINT Tools
  - Discover – https://github.com/leebaird/discover
  - Hunter – https://hunter.io/
  - FOCA – https://github.com/ElevenPaths/FOCA
  - Metagoofil – https://github.com/laramies/metagoofil
- Social Engineering
  - Social-Engineer Toolkit – https://www.trustedsec.com/social-engineer-toolkit-set/

7. Additional Considerations

- Vulnerable Test Systems
  - OSBoxes – https://www.osboxes.org/
  - VulnHub – https://www.vulnhub.com/
- Encryption Tools
  - BitLocker – https://docs.microsoft.com/en-us/powershell/module/bitlocker/?view=win10-ps
  - VeraCrypt – https://www.veracrypt.fr/
- Encrypted File Sharing
  - Box – https://www.box.com/
  - ShareFile – https://www.sharefile.com/
- Secure File Deletion
  - CCleaner – https://www.ccleaner.com/
  - BleachBit – https://www.bleachbit.org/

    Linux utilities

    shred

    wipe

    secure-delete

8. Conclusion

- Recommended Reading
  - RTFM: Red Team Field Manual

    https://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504/
  - iBTFM: Blue Team Field Manual

    https://www.amazon.com/Blue-Team-Field-Manual-BTFM/dp/154101636X/
  - Hash Crack: Password Cracking Manual

    https://www.amazon.com/Hash-Crack-Password-Cracking-Manual/dp/1975924584/
  - Penetration Testing: A Hands-On Introduction to Hacking

    https://www.amazon.com/Penetration-Testing-Hands-Introduction-Hacking/dp/1593275641/
- NIST Publications
  - SP 800-30 Rev. 1: Guide for Conducting Risk Assessments

    https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
  - SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations

    https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
  - iSP 800-115: Technical Guide to Information Security Testing and Assessment

    https://csrc.nist.gov/publications/detail/sp/800-115/final
- Professional Organizations
  - ISSA – https://www.issa.org/
  - ISACA – https://www.isaca.org/
  - (ISC)2 – https://www.isc2.org/
  - InfraGard – https://www.infragard.org/
  - OWASP – https://www.owasp.org/
- Information Security Conferences
  - InfoSec Conferences – https://infosec-conferences.com/
  - BSides – http://www.securitybsides.com/

- Conference Videos
    - Adrian Crenshaw (@irongeek_adc)

      http://www.irongeek.com/
- Me (Jerod)
    - https://www.linkedin.com/in/slandail
    - https://www.slideshare.net/JerodBrennenCISSP
- IT Security Career –https://itsecuritycareer.com/