Penetration Testing overview and tips for the Developers

peneter.com

Me

- Soheil Hashemi
- MSc in Network Computers
- Network Administrator, Penetration Testing
- Ashiyane Digital Security Team AKA “Xenotix" [2012]
- https://linktr.ee/soheilhashemi

What’s Penetration Testing?

why need Penetration Testing

- Penetration Testing is process which emulate are discovered Attacks(Attack vectors) on Attack surfaces then finally generate the pen Report.
- Threat
- Vulnerability
- Threat Modeling
- Exploit, Payload
- every application should check it before release some testing for performance evaluation and another one relevant to security check such as check input validation, Traffic transfer, etc.
- Web Application, Mobile Application, Network Infrastructure, OT[ICS], IoT

Penetration Testing Terminology

why need Penetration Testing

- Penetration Testing Check List
- Penetration Testing Methodology
- Penetration Testing Standards
- Penetration Testing Tools
- Penetration Testing Frameworks
- Penetration Testing Types[black box, Gray box, White box]
- Ethical Hacker, Penetration Tester
- Red Team, Blue Team, Purple Team
- Certificate [OSCP, CEH, SANS]

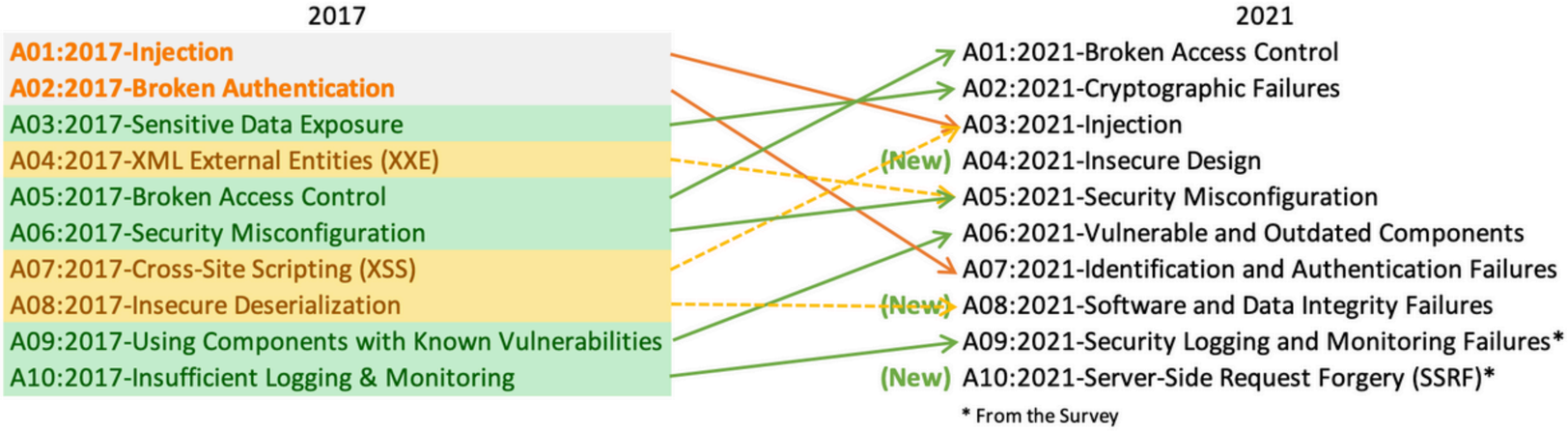
Penetration Testing Check List

- Penetration Check list is security guide line for finding common vulnerability.
- Most Common mistakes in security configuration

Penetration Testing Methodology & Standards

- OSSTMM(open source security testing methodology manual)
- OWASP(open web application security project)
- NIST(the national institute of standards and technology)
- PTES(Penetration Testing Execution standard)
- ISSAF(information system security assessment framework)

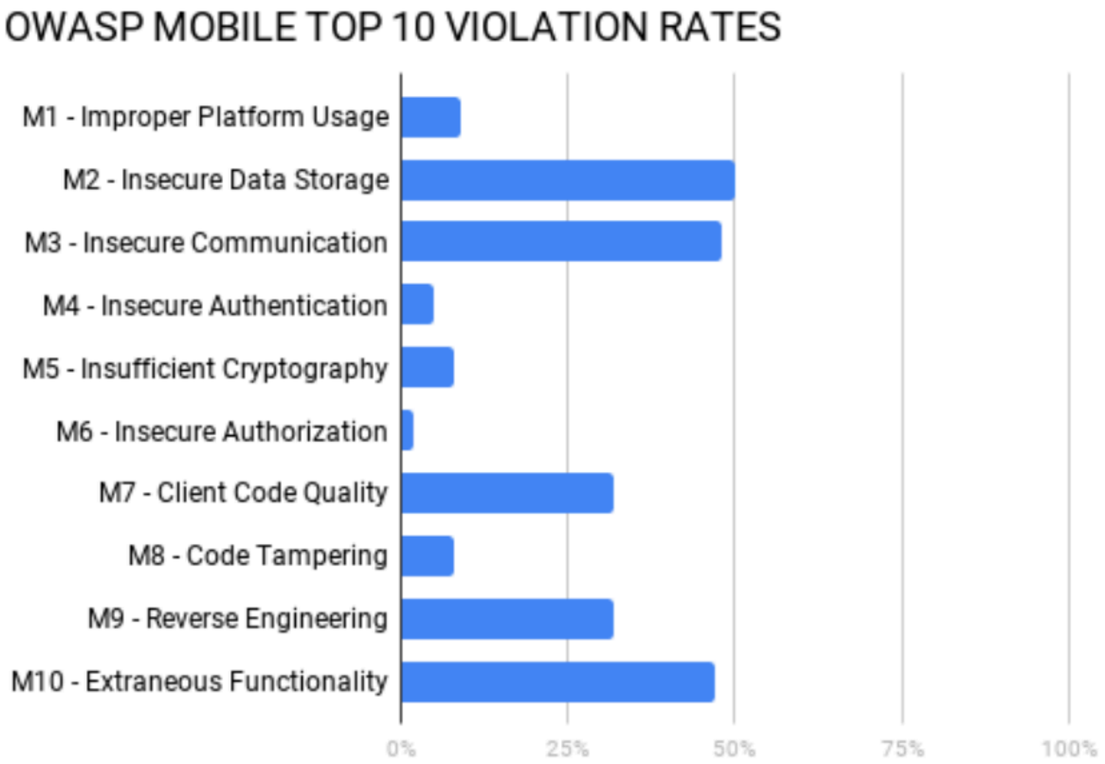
WAP



- Web Application Penetration Testing OWASP

Mobile Pentest

- https://github.com/OWASP/owasp-mstg



Cloud Penetration Testing

- https://aws.amazon.com/security/penetration-testing/
- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement?rtc=1
- https://support.google.com/cloud/answer/6262505?hl=en
- https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

Cloud Penetration Testing

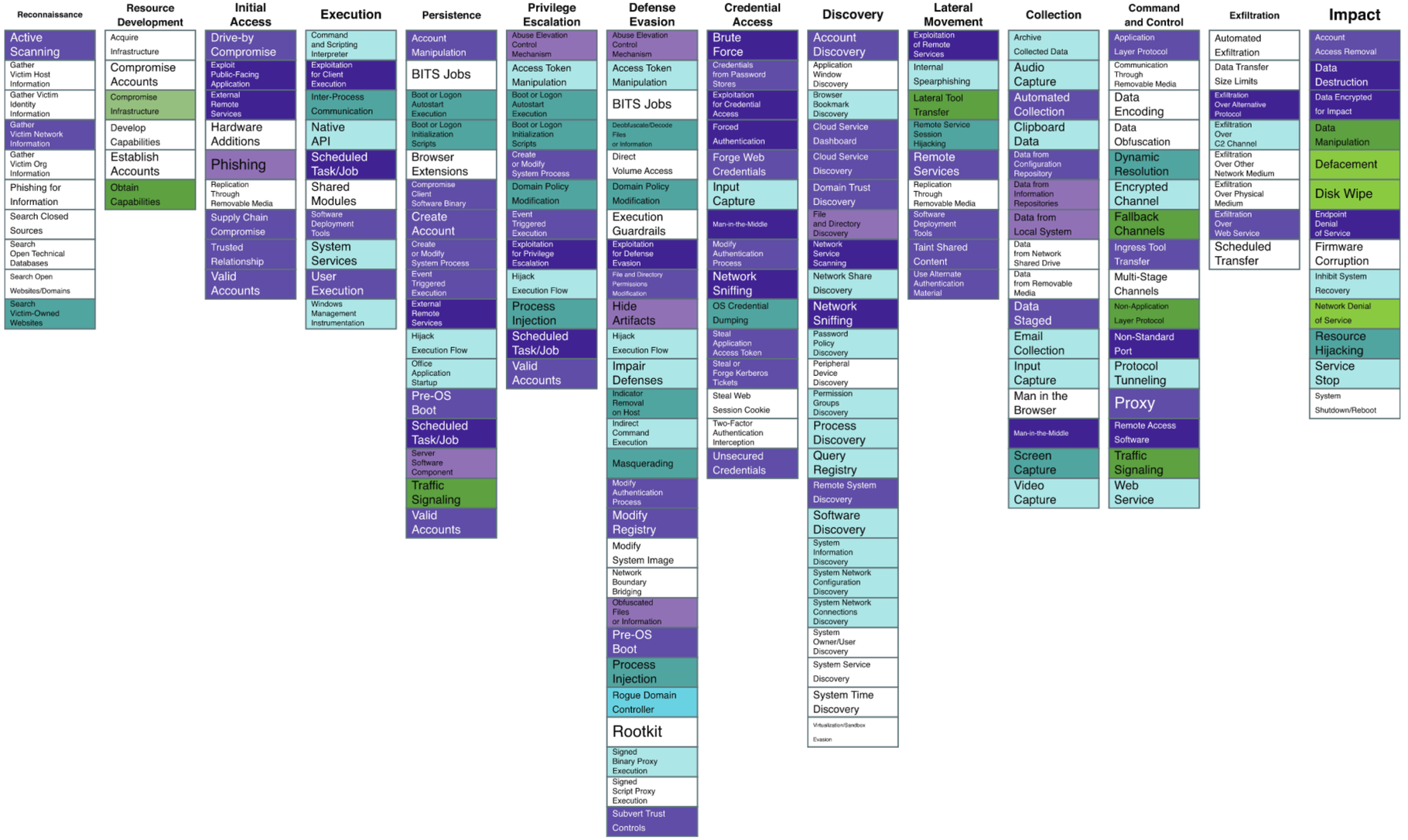


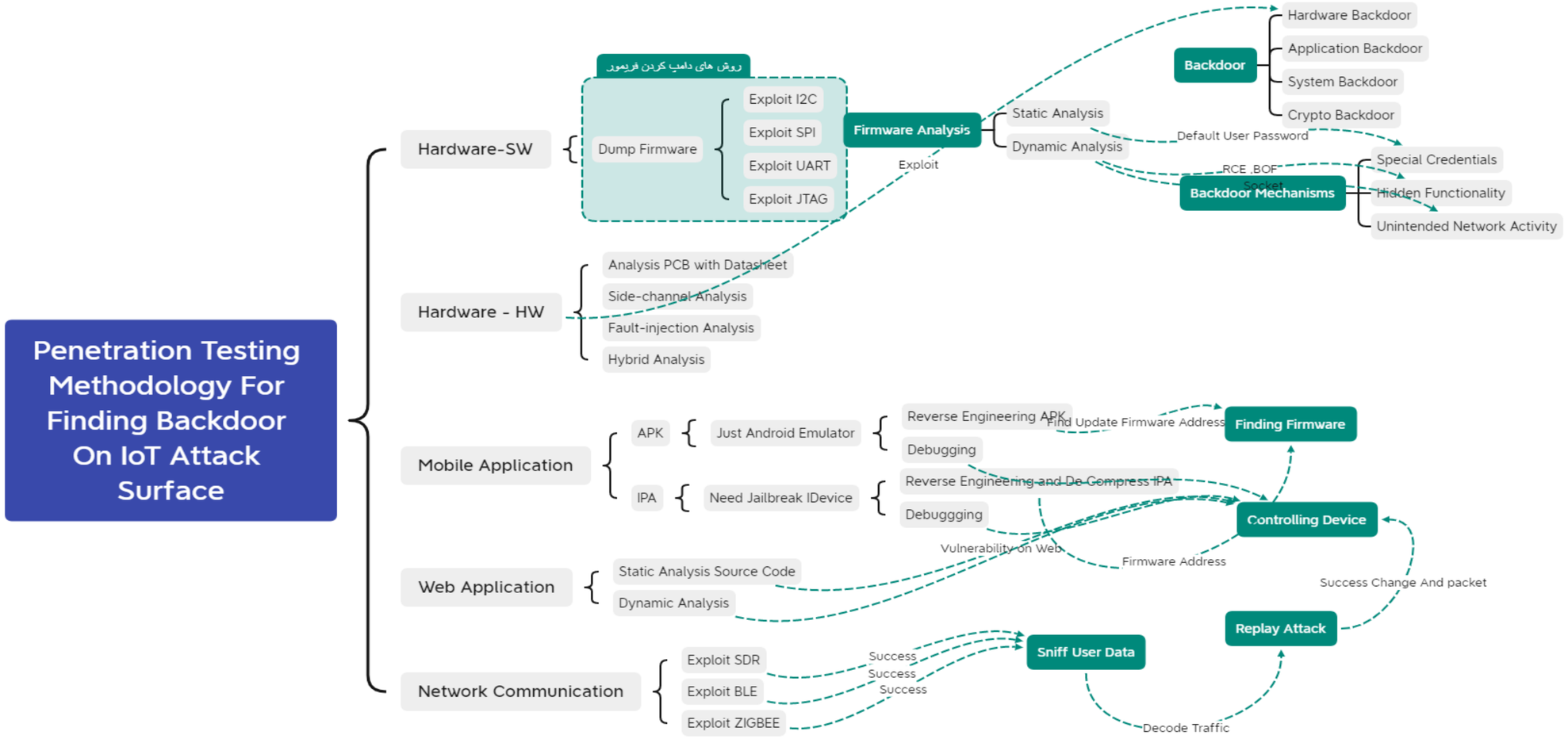
Figure 1

The output of the Center's mapping project is a guide showing which Azure controls best protect against each ATT&CK TTP.

IoT Penetration Testing

- Attack surface (Embedded Device[SW,HW], Cloud, Mobile Application, Network Communication Protocols)
- Embedded device Penetration Testing
- Firmware Penetration Testing

IoT Penetration Testing



Penetration Testing Tools

- Penetration Testing Tools is automated penetration testing methodology for finding and exploiting vulnerabilities most of tools are available open source and free in Kali Linux
- https://tools.kali.org/

Penetration Testing Frameworks

- If the frameworks design and contain of multiple tools and modules called Penetration testing Frameworks such as Metasploit, MoBSF(Mobile Security Framework), PENIoT

Penetration Testing Types

- Penetration Testing Types are black, Gray, White it depends on the information which told to penetration tester team about the network infrastructure info such as firewall, IDS if the info not tell to team the test will be black because is blind if some limit info gave to team the type will be gray and the penetration testing from inside the network or gave the source code of Application {APK, IPA, WA } the test will be white.

Ethical Hacker & Penetration Tester

- Ethical hacker and penetration tester have same define if the person start the cyber security start course with CEH can certified as Ethical hacker because knowing about the Methodologies and learn the rules for privacy of customer and confidentiality about the report and also NDA(non-disclosure agreement)

Red team, Blue team, Purple team

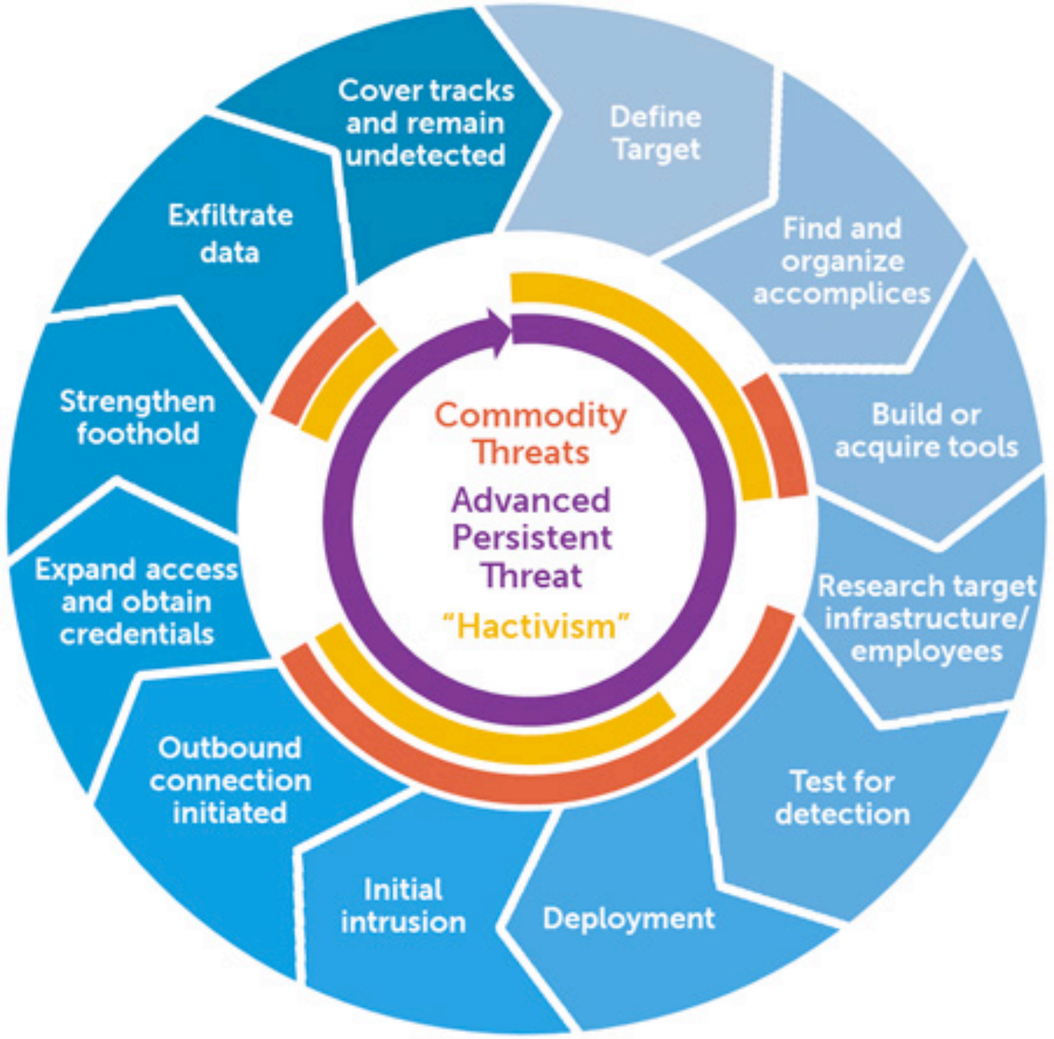
- Red Team guy equal to hacker they are same because testing all the exploit and attack surface such as social engineering techniques and want breach the network with any way.
- Blue Team guy is same T3 of SOC they should knowing about Forensic, Threat hunting and also good knowledge about network configuration because when figure out any threat available should change configuration network with permission of CEO for mitigation plan.
- Purple Team guy is management level they manage the Red and blue team also the most important duty of team is APT hunting they should know about all ransomware gangs and knowing APT teams for finding threats.

Certificate, License

- Certificate [OSCP, CEH, SANS]
- Offensive security OSCP
- Ec-Council CEH
- SANS depend on branch mobile web iot ics ,…
- ICS crisp

Cyber kill chain

APT Attack


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

MITRE framework TTP

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Mitre Project

- Https://attack.mitre.org/
- https://d3fend.mitre.org/
- https://car.mitre.org/
- https://cwe.mitre.org/index.html
- https://cve.mitre.org/

Penetration Testing Steps

- Information Gathering
- Enumeration & Scanning
- Exploiting
- privilege Escalation and Maintain Access
- Post Exploit
- Report

Information Gathering

- Collection information about Company or Target (Assets)
- OSINT about company employee, Service, Technology, C-level[Email, Social Media, Document]

Enumeration and Scanning

- Some Services such as SMB, SNMP can enumerate and collect data such as Usernames, Configuration Files and etc.
- Scanners are work base on threat modeling [CVE,CVSS] and checking the input validation and other attack vectors.

Exploiting

- Exploiting Vulnerability and grant Access depend on payload cli or GUI

Privilege Escalation & maintain Access

- Privilege Escalation [vertical, Horizontal]
- Maintain Access[Backdoor] Application, System, Crypto, Hardware
- Backdoor can be part of system features.

Post Exploiting

- Stealing and dumping Credential
- Stealing Documents, DB

Reporting

- Report drafts are base on some methodology and standards such as OWASP, OSSTM, ISSAF, Pets and cover the which methodology is used and the Vulnerability list and POC which are shown the lateral movement or proof take over Website, Network and etc.

Developers

- Owasp secure code best practice [secure by design]
- Mitigation [WAF]
- Monitoring [LOG]
- Server Hardening [Permission check on Web server, Ftp, tmp folders]
- Check your code [https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools] sonarqube, codeql
- Vulnerability Assessment Scanners [Acunetix, openvas, netsparker, IBM app scan, HCL web inspect]
- Mobile application [Mobfs]
- BoF[Fuzzing]

More resource

- https://github.com/Peneter/Cybersecurity-Roadmap
- https://application.security/
- https://portswigger.net/research/top-10-web-hacking-techniques-of-2020
- t.me/learnpentest
- t.me/peneter_news
- t.me/peneter_tools
- t.me/peneter_media

Q/A