Penetration Testing overview and tips for the Developers

peneter.com

• Soheil Hashemi

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



g notix" [2012]

What's Penetration Testing?

why need Penetration Testing

- surfaces then finally generate the pen Report.
- Threat
- Vulnerability
- Threat Modeling
- Exploit, Payload
- Web Application, Mobile Application, Network Infrastructure, OT[ICS], IoT

• Penetration Testing is process which emulate are discovered Attacks(Attack vectors) on Attack

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.





Penetration Testing Terminology

- 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]

why need Penetration Testing

Penetration Testing Check List

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

e for finding common vulnerability. aration

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)

2017

A01:2017-Injection A02:2017-Broken Authentication A03:2017-Sensitive Data Exposure A04:2017-XML External Entities (XXE) A05:2017-Broken Access Control A06:2017-Security Misconfiguration A07:2017-Cross-Site Scripting (XSS) A08:2017-Insecure Deserialization A09:2017-Using Components with Known Vulnerabilities A10:2017-Insufficient Logging & Monitoring

• Web Application Penetration Testing OWASP

WAP

2021

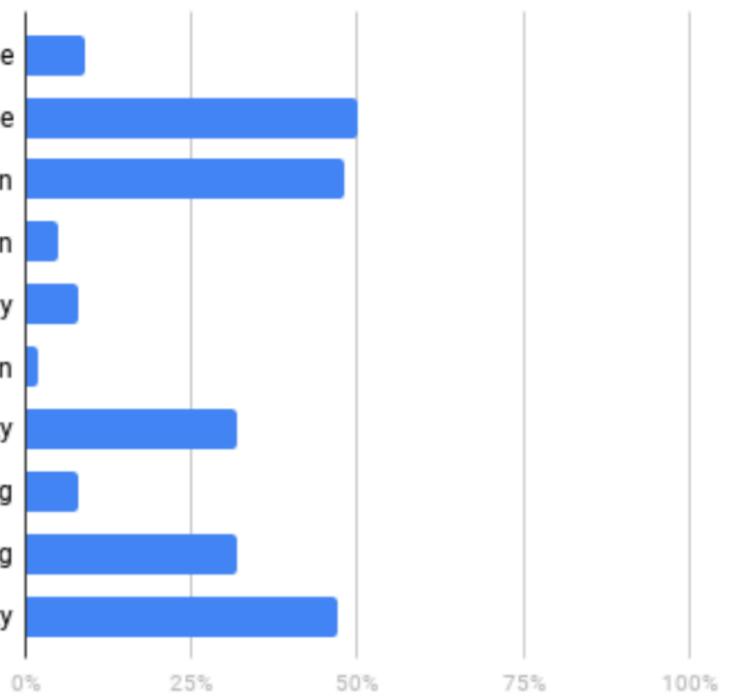
A01:2021-Broken Access Control A02:2021-Cryptographic Failures A03:2021-Injection (New) A04:2021-Insecure Design > A05:2021-Security Misconfiguration A06:2021-Vulnerable and Outdated Components A07:2021-Identification and Authentication Failures (New) A08:2021-Software and Data Integrity Failures A09:2021-Security Logging and Monitoring Failures* (New) A10:2021-Server-Side Request Forgery (SSRF)* * From the Survey

Mobile Pentest

• https://github.com/OWASP/owasp-mstg

OWASP MOBILE TOP 10 VIOLATION RATES

M1 - Improper Platform Usage M2 - Insecure Data Storage M3 - Insecure Communication M4 - Insecure Authentication M5 - Insufficient Cryptography M6 - Insecure Authorization M7 - Client Code Quality M8 - Code Tampering M9 - Reverse Engineering



Cloud Penetration Testing

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

Cloud Penetration Testing

rge Web

ge Kerberos

dentials

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation
Active	Acquire	Drive-by	Command and Scripting	Account	Abuse Elevation Control
Scanning	Infrastructure	Compromise	Interpreter	Manipulation	Mechanism
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts
Gather Victim Org Information	Establish Accounts	Phishing	Scheduled Task/Job	Browser Extensions	Create or Modify System Process
Phishing for	Obtain	Replication Through	Shared	Compromise Client	Domain Policy
Information	Capabilities	Removable Media	Modules	Software Binary	Modification
Search Closed		Supply Chain	Software Deployment	Create	Event Triggered
Sources		Compromise	Tools	Account	Execution
Search Open Technical Databases		Trusted Relationship	System Services	Create or Modily System Process	Exploitation for Privilege Escalation
Search Open	1	Valid	User	Event Triggered	Hijack
Websites/Domains		Accounts	Execution	Execution	Execution Flow
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection
				Hijack	Scheduled
				Execution Flow	Task/Job
				Office Application	Valid
				Startup	Accounts
				Pre-OS	
				Boot	

Defense Evasion	Creden Acces
Abuse Elevation	Brute
Control Mechanism	Force
Access Token	Credentials
Manipulation	from Password Stores
BITS Jobs	Exploitation for Credential Access
Deobfuscate/Decode	Forced
Files or Information	Authentication
Direct	Forge Web
Volume Access	Credentials
Domain Policy	Input
Modification	Capture
Execution	
Guardrails	Man-in-the-Middle
Exploitation	Modify
for Defense Evasion	Authentication Process
File and Directory	Network
Permissions Modification	Sniffing
Hide	OS Credentia
Artifacts	Dumping
Hijack	Steal
Execution Flow	Application Access Token
Impair	Steal or
Defenses	Forge Kerberos Tickets
Indicator	Steal Web
Removal on Host	Session Cooki
Indirect	Two-Factor
Command Execution	Authentication
Execution	Interception Unsecured
Masquerading	Credentials
Modify	oreactiliais
Authentication	
Process Modify	
Registry	
Modify System Image	
System Image Network	
Boundary	
Bridging Obfuscated	
Files	
or Information	
Pre-OS Boot	
Process	
Injection	
Rogue Domain Controller	
Rootkit	
Signed	
Binary Proxy Execution	
Signed	
Script Proxy Execution	
Subvert Trust	

Scheduled

Task/Job

Software Component

Signaling

Traffic

Valid Accounts

Server

Credential Discovery Access Account Discovery Application Window Discovery Browser Bookmark Discovery Cloud Service Dashboard Cloud Service Discovery Domain Trust Discovery n-the-Middle and Directory Discovery Network Service Scanning Network Share Discovery redential Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups ession Cookie Discovery Process Discovery Query Registry Remote System Discovery Software Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery System Service

Discovery System Time Discovery Virtualization/Sandbox

Lateral Movement of Remote Services Internal Spearphishing Lateral Tool Fransfer emote Service jacking Remote Services Replication Through Removable Media Software eployment Taint Shared Content Use Alternate Authentication Material

Collection Archive Collected Data Audio Capture

Automated Collection Clipboard Data Data from Configuration Repository Data from nformation Repositories Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Email Collection Input Capture Man in the Browser /an-in-the-Middle Screen Capture Video Capture

and Contro
Application
Layer Protocol
Communication Through Removable Media
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Remote Access Software
Traffic Signaling
Web

Service

Exfiltration

Command

Automated Exfiltration Data Transfer Size Limits xfiltration Over Alternative rotocol Exfiltration C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Physical Medium xfiltration Web Service Scheduled Transfer

Impact

Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Defacement Disk Wipe indpoint Denial of Service Firmware Corruption Inhibit System Recovery Network Denial of Service Resource Hijacking Service Stop System Shutdown/Reboot

Figure 1 The output of the Center's mapping project is a guide showing which Azure controls best protect against each ATT&CK TTP.

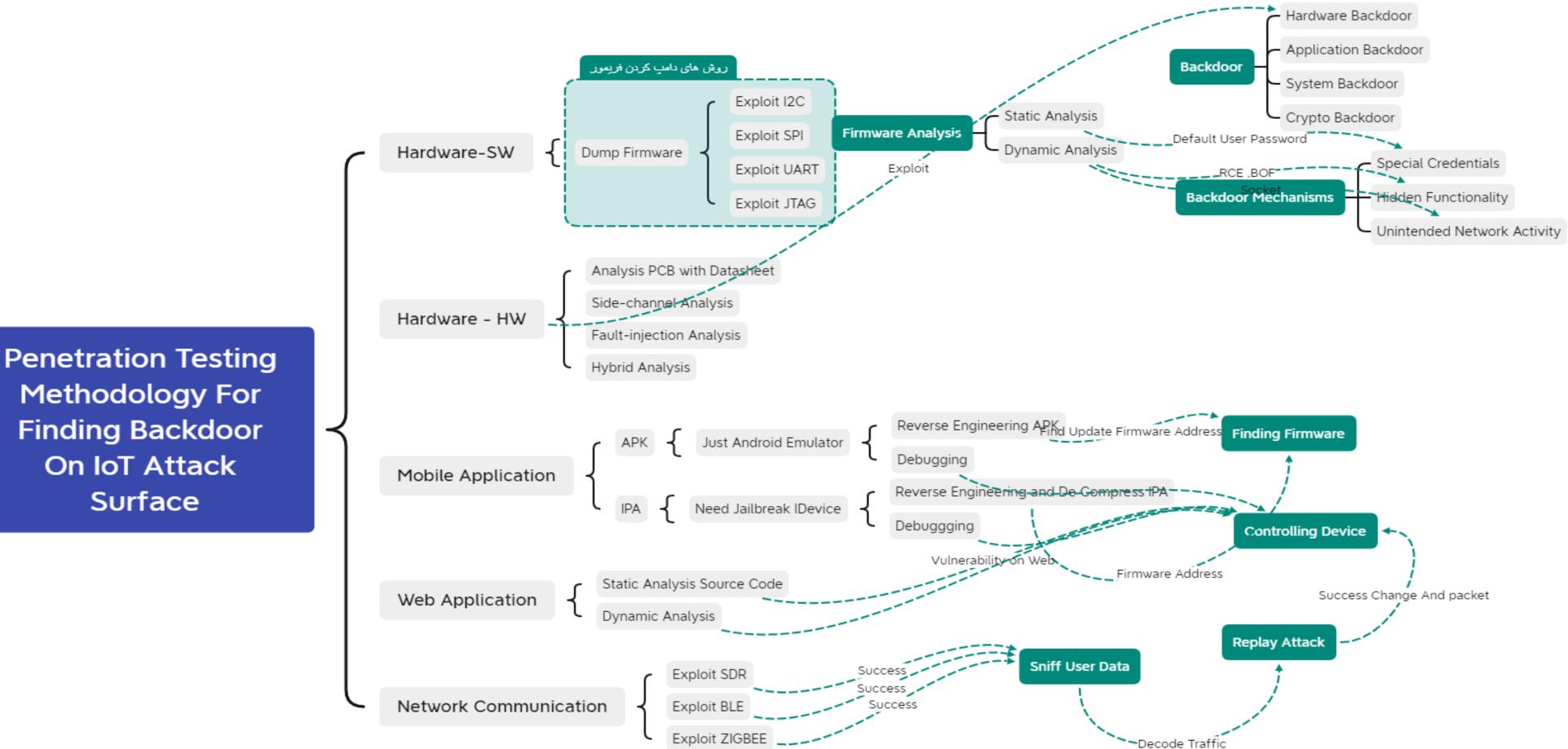
IoT Penetration Testing

- Communication Protocols)
- Embedded device Penetration Testing
- Firmware Penetration Testing

• Attack surface (Embedded Device[SW,HW], Cloud, Mobile Application, Network



IoT Penetration Testing



Penetration Testing Tools

- https://tools.kali.org/

• 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



Penetration Testing Frameworks

Frameworks such as Metasploit, MoBSF(Mobile Security Framework), PENIoT

• If the frameworks design and contain of multiple tools and modules called Penetration testing



Penetration Testing Types

Application {APK, IPA, WA } the test will be white.

• 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



Ethical Hacker & Penetration Tester

and also NDA(non-disclosure agreement)

• 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



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 Phases of the Intrusion Kill Chain



Research, identification, and selection of targets

- Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
- Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
- Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
- The weapon installs a backdoor on a target's system allowing persistent access
- Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
- The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target



APT Attack

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/
- <u>https://cwe.mitre.org/index.html</u>
- <u>https://cve.mitre.org/</u>

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

- Configuration Files and etc.
- and other attack vectors.

Some Services such as SMB, SNMP can enumerate and collect data such as Usernames,

Scanners are work base on threat modeling [CVE,CVSS] and checking the input validation



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

Exploiting

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

shown the lateral movement or proof take over Website, Network and etc.

• 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

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 [<u>https://owasp.org/www-community/</u> <u>Free_for_Open_Source_Application_Security_Tools</u>] sonarqube, codeql
- Vulnerability Assessment Scanners [Acunetix, openvas, netsparker, IBM app scan, HCL web inspect]
- Mobile application [Mobfs]
- BoF[Fuzzing]

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

More resource

