Systematic Embedded Device Analysis

(Case by Case)

2015 .10.25

Pwners Lab.

Jaeki Kim

jack2@korea.ac.kr

Contents

PWNERS LAB

- Intro
- Pwners Lab
- Case Study
- Methodology
- Conclusion

Intro

- **Topic**
  - ✓ **Case Study**
    - ✓ Vulnerability of Embedded Devices

Intro

PWNERS LAB

- **Topic**
  - ✓ **Case Study**
    - ✓ Vulnerability of Embedded Devices
  - ✓ **Analysis Methodology**
    - ✓ Reduce wasting time
    - ✓ Checklist for analysis

Pwners Lab

PWNERS LAB

- **Purpose**
  - ✓ **Practical follow-up Group**
    - ✓ Development
    - ✓ Penetration
    - ✓ Vulnerability Analysis

Pwners Lab

PWNERS LAB

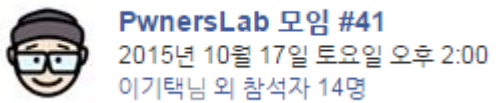
▪ History

No.	일시	분류	내용	비고
0	2014.03	-	BOB 실전 모의해킹 모임	
1	2014.03 ~ 05	스터디	웹 해킹 관련 학습 및 연구	SQL 인젝션 도구 분석 테스트 사이트 구축 후 모의해킹 진행 모의해킹에 대한 보고서 작성 및 피드백
2	2014.03	프로젝트	KISA 융합보안 시범사업 자문	교통, 물류, 의료, 금융, 지불 분야
3	2014.05	프로젝트	모의해킹 프로젝트	한국 ebay
4	2014.05 ~ 09	스터디	리버스 엔지니어링 학습 및 세미나	Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation
5	2014.07	운영	글로벌 해킹보안 컨퍼런스 시큐인사이드 2014 운영	해킹그룹 연합 HARU
6	2014.09 ~ 10	프로젝트	모의해킹 프로젝트	SKT 서비스 관련
7	2014.10	발표	무선 공유기 취약점 연구 발표 및 시연	삼성전자, 스마트 보안AP 솔루션 데이
8	2014.11	운영	산업자원부 보안 경진대회 문제출제 및 운영	한전 KDN
9	2015.03	-	그룹명 변경 : JosunHackers	
10	2015.03 ~	스터디	하드웨어 해킹 관련 학습 및 연구	공유기, CCTV, STB 등
11	2015.03 ~	스터디	오픈소스 웹 취약점 연구	워드프레스, 제로보드 등
12	2015.06	스터디	Lord of SQLi (LOS) 문제 풀이 및 강의	Rubiya
13	2015.07	프로젝트	웹 취약점 관련 번역 프로젝트	CN SECURITY
13	2015.07	프로젝트	APT 공격시나리오 작성 프로젝트	KISA
14	2015.07	-	그룹명 변경 : Pwners Lab	
15	2015.07	-	팀블로그 개설	http://pwnerslab.com/
16	2015.07	운영	글로벌 해킹보안 컨퍼런스 시큐인사이드 2015 운영	해킹그룹 연합 HARU
17	2015.07	발표	SECUINSUDE 2015 - CTB	4개 부분 참여
18	2015.07	발표	SECUINSUDE 2015 - Conference 발표	Welcome to mobile connetected World
19	2015.08	스터디	취약점 관련 학습 및 정리	The Shellcoder's Handbook: Discovering and Exploiting Security Holes

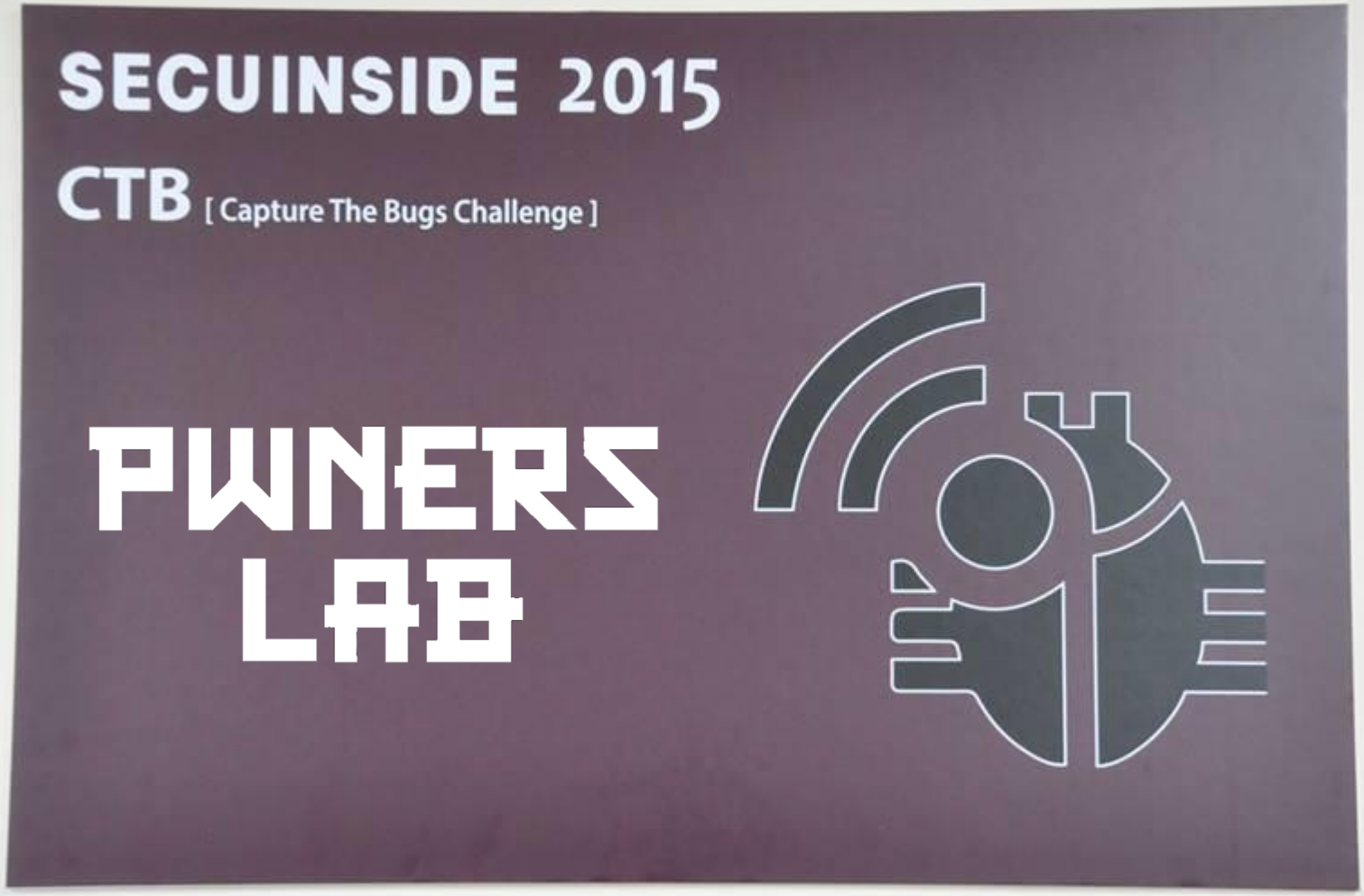
Pwners Lab

PWNERS LAB

- **Activity**



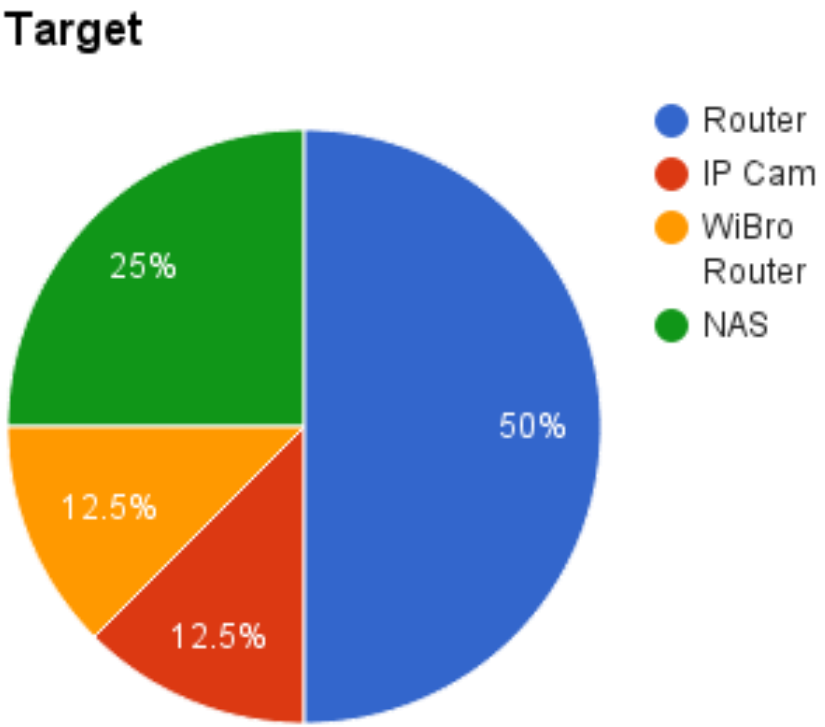
Case Study



Case Study

PWNERS LAB

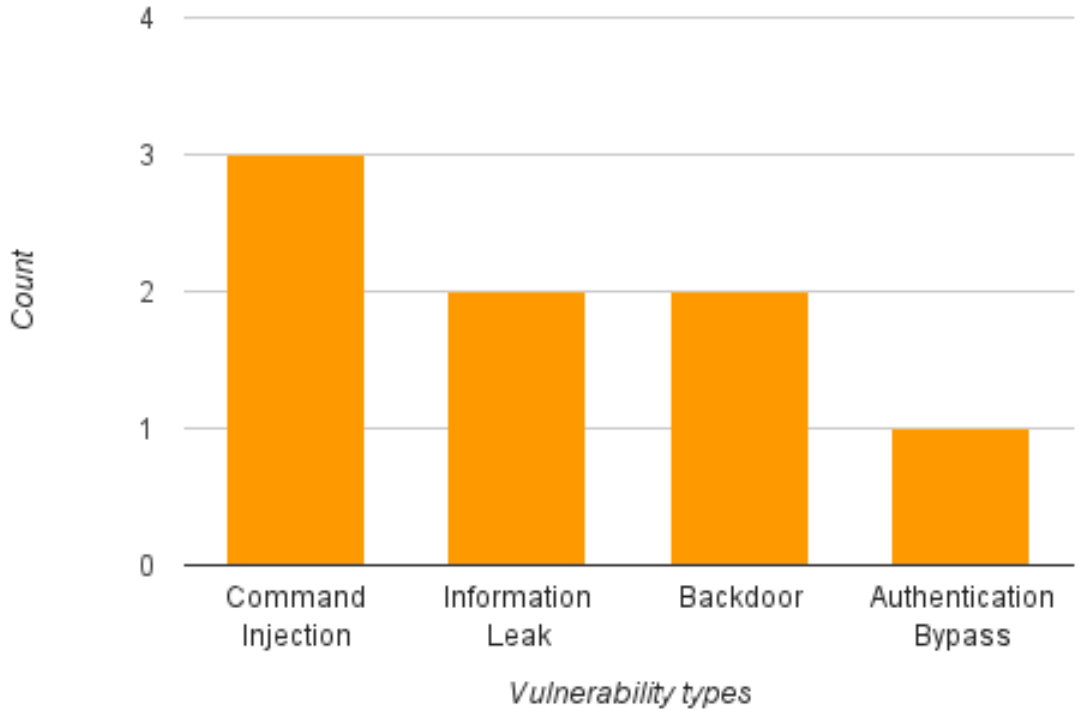
- **Classification (1)**
  - ✓ **Target (Total : 8)**
    - ✓ Router – 4
    - ✓ NAS – 2
    - ✓ WiBro Router - 1
    - ✓ IP Cam - 1



Case Study

PWNERS LAB

- **Classification (2)**
  - ✓ **Vulnerability**



Case Study

PWNERS LAB

- **Methodology (1)**

  1) Beforehand

  - ✓ **Check Manual (Spec)**
  - ✓ **Test Function**
  - ✓ **Port Scanning**
  - ✓ **Find Attack Vector**

Case Study

- **Methodology (2) Firmware**

2) Firmware Acquisition

- ✓ **Support Official website**
- ✓ **Sniff Update packet**
- ✓ **Use download vuln**
- ✓ **Extract Firmware**
  - ✓ **JTAG/UART**

Case Study

PWNERS LAB

- **Methodology (2) Firmware**

3) Firmware Analysis

- ✓ Identify Firmware structure
- ✓ Extract filesystem
  - ✓ Overall process
    - ✓ Ex) Init.d, Open source, web daemon
  - ✓ Try to get $hell
    - ✓ Check low vulns - Command Injection
  - ✓ Check Hidden functions
    - ✓ Ex) backdoor

Case Study

- **Methodology (3)**

4) Web page for Administration

- ✓ **Pentest Web vulns**
  - ✓ **Ex) File upload, XSS, SQL Injection**

5) Binary Analysis

- ✓ **Dynamic**
  - ✓ **Virtual environment Configuration - QEMU**
  - ✓ **Actual Device (using file upload vuln)**

Case Study

PWNERS LAB

- **Methodology (3)**

5) Binary Analysis

- ✓ **Static**
  - ✓ **Check Vulnerable functions**
  - ✓ **Available to control via user input**

6) Try to Exploit

- ✓ **Using discovered vulns**
- ✓ **Check associated with different attack vector**

- **Topic**
  - ✓ **Case Study**
    - ✓ Vulnerability of Embedded Devices

Methodology

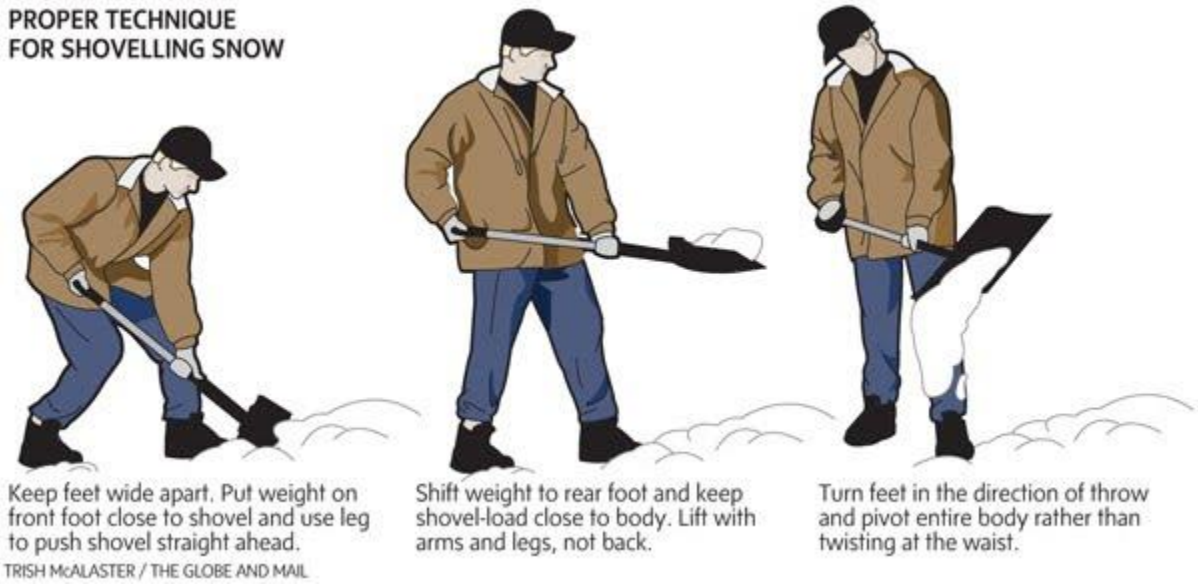
- **Previous**

이건 좀 아닌듯

Methodology

PWNERS LAB

- **How**
  - ✓ **Analysis Methodology**
    - ✓ Checklist for analysis
    - ✓ Reduce wasting time



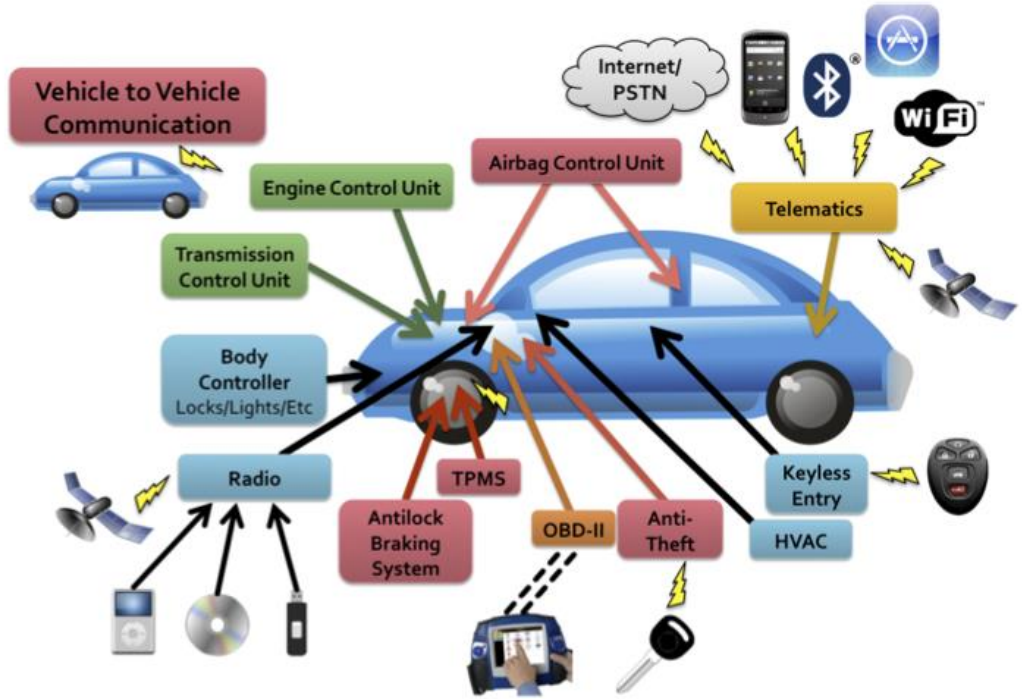
Methodology

PWNERS LAB

- **How**

1) Identify assets

- ✓ **Enumerate functions**
- ✓ **Draw Data Flow Diagram**



Methodology

PWNERS LAB

- **How**

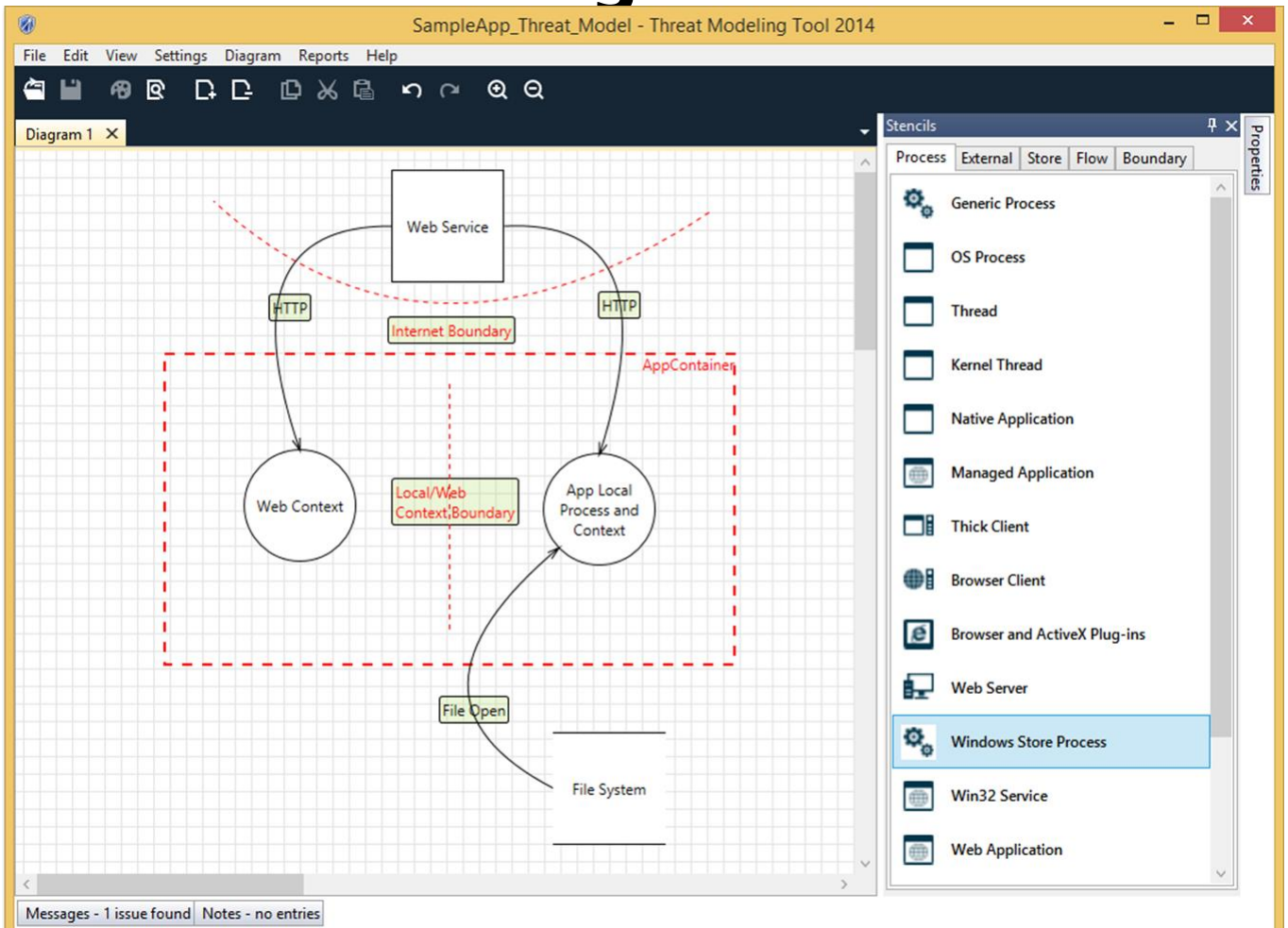
2) Threat Analysis

NO	Type	Perspective	Coverage	Apply	Remark
1	**Misuse Case**	Defender	Threat	O	Threat identification
2	**Attack Tree**	Attacker	Threat	O	
3	**Vulnerability Cause Graph (VCG)**	Defender	Vulnerability	X	Well-known Vulns Ex) CVE
4	**Vulnerability Detection Condition**	Defender	Vulnerability	X	
5	**Security Goal Indicator Tree (SGIT)**	Defender	Security Function	O	Only Security function
6	**Security Indicator Specialisation Tree**	Defender	Requirement, Design docs, Source code	X	Design stage
7	**Guided Security Inspection Checklist (GSIC)**	Defender	Requirement, Design docs, Source code	X	
8	**Vulnerability Inspection Diagram (VID)**	Attacker	Products, Source code	O	
9	**Security Inspection Scenario (SIS)**	Attacker	Products, Source code	O	

Methodology

- **How**

3) Threat Modeling



Methodology

PWNERS LAB

- **How**

4) Checklist for analysis

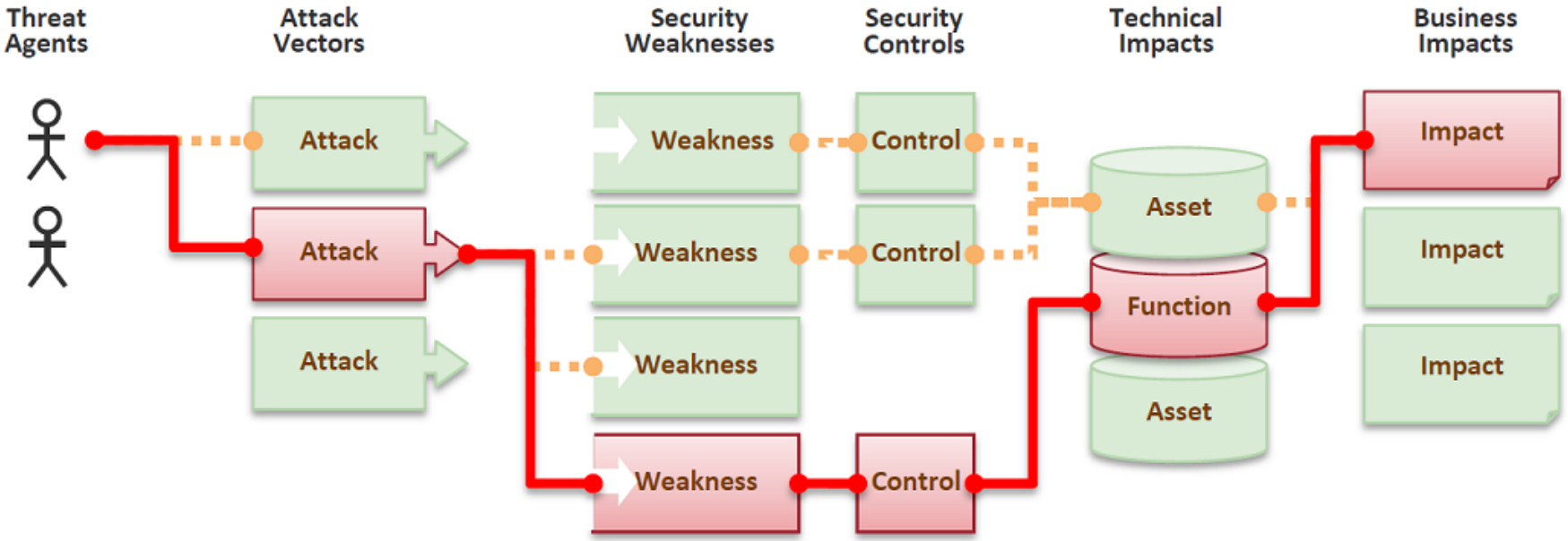
Test Name	Ref. Number	Status	Risk
Spiders, Robots and Crawlers	*IG-001*	Not Done	
Search Engine Discovery/Reconnaissance	*IG-002*	Done	L
Identify application entry points	*IG-003*	Done	H
Testing for Web Application Fingerprint	*IG-004*	Done	M
Application Discovery	*IG-005*	Done	H
Analysis of Error Codes	*IG-006*	Not Done	
SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) - SSL Weakness	*CM-001*	Done	H
DB Listener Testing - DB Listener weak	*CM-002*	Not Done	
Infrastructure Configuration Management Testing - Infrastructure Configuration management weakness	*CM-003*	Done	H
Application Configuration Management Testing - Application Configuration management weakness	*CM-004*	Not Done	
Testing for File Extensions Handling - File extensions handling	*CM-005*	Not Done	
Old, backup and unreferenced files - Old, backup and unreferenced files	*CM-006*	Done	M
Infrastructure and Application Admin Interfaces - Access to Admin interfaces	*CM-007*	Not Done	
Testing for HTTP Methods and XST - HTTP Methods enabled, XST permitted, HTTP Verb	*CM-008*	Done	
Credentials transport over an encrypted channel - Credentials transport over an encrypted	*AT-001*	Not Done	
Testing for user enumeration - User enumeration	*AT-002*	Not Done	

Overall Status	
Done	19 / 66
Total Vulns	17
Completion Status	29%

Conclusion

PWNERS LAB

- **Systemic Analysis**



Conclusion

PWNERS LAB

- **Step back and see the big picture**