Final Report

Intelligence-led Penetration Test

Wong Chun Ho
3035093850

Supervisor: Dr. K. P. Chow

Date of Submission: 15th April 2018

Contents

1. Acknowledgment 2
2. Disclaimer 2
3. Abstract 2
4. Project Background 3
5. Project Objective 3
6. Deliverable 4
7. Project Methodology 4
8. What is iCAST? 5
9. iCAST Tester 6
   a. iCAST Tester certifications comparison in high level 7
   b. CREST – Certified Tester Analysis 9
   c. EC Council - Certified Ethical Hacker 11
10. CREST Threat Intelligence Analyst 14
11. CREST Simulated Attack Manager and Specialist 18
12. Intelligence Led Penetration test case study 21
13. Limitations 27
14. Project Schedule and Plan 28
15. Conclusion 28
16. List of Figures 29
1. Acknowledgment

I would like to express my special thanks to my supervisor Dr. K. P. Chow for guiding me throughout the project with patient and useful advice. Without his sincere help, this project would not be complete.

2. Disclaimer

The information provided on this paper is to be used for educational purposes only. Any actions and or activities related to the material contained within this paper is solely your responsibility. The misuse of the information in this paper can result in criminal charges brought against the persons in question. The author is in no way responsible for any misuse of the information provided.

3. Abstract

Many technical companies put a lot of effort in developing software. Nevertheless, they usually underestimate the importance of cyber securities. For example, an E-commerce websites and company brand may take years to build up, but a single system loophole can destroy the trust of this company in a second when tons of client’s data is stolen. As such, an intelligence led penetration test like iCAST is invariably necessary to every company. However, many small companies and technical staff are still unfamiliar to the implementation and details of the test. Therefore, this paper aims to understand more about intelligence-led penetration test.
4. Project Background

Computer Security becomes more and more important nowadays because of the increasing use of online financial system. As the value of the online system grows, it will be more lucrative to hackers. To standardize the defending level, in 2016 December, HKMA (Hong Kong Monetary Authority) has launched the Cyber Security Resiliency Framework (CRF). It promotes intelligence-led Cyber Attack Simulation Testing (iCAST), in which tester will simulate the actions of cyber attacker and exploit vulnerabilities to gain unauthorized access to the online systems of various organizations. iCAST is built up on top of traditional penetration testing (pen test) [1]. Only a few certifications are considered qualified to perform iCAST, for example, CREST Certified Simulated Attack Specialist. [2] Meanwhile, there are some certifications that are not on the list, for instance, Certified Ethical Hacker (CEH). [3]

As new software vulnerabilities are discovered every day, a pen tester faces profuse challenges. Life-long studying is required to be equipped and qualified as a pen tester. Since there are many types of certifications with different exam contents, it is not easy to find out one common criterion to be qualified as a iCAST tester. As such, this project aims to understand the implementation of iCAST and look for new elements that are missing in the traditional pen test standard.

This paper will first explain the objective and deliverable of the project. Secondly, it will describe the methodologies. Thirdly, it will also explain what is iCAST with details. Finally, it will list out the project limitation and project schedule.

5. Objective

The project objective is to study Intelligence Led Penetration test through studying iCAST in 3 areas, namely, iCAST Manager, iCAST Specialist, iCAST Tester, whereas study of C-RAF Assessor is not in the scope of this project. [4] At the same time, it would like to find out some important elements that are missing from unaccepted certificates or even missing element in iCAST.
6. Deliverable

There are two deliverable products in this project. Firstly, it is the study paper on Intelligence Led Penetration Test through reviewing iCAST. Secondly, it is a brief practical guide for executing Intelligence Led Penetration Test based on iCAST. This guide is not possible to cover all existing exploitation tools, but selectively cover the most fundamental elements. A representative exploitation tool is chosen for demonstration.

7. Project Methodology

This project will be split into three parts. Firstly, it will investigate the standard of iCAST Tester for IT infrastructure testing and web application testing. A qualified tester should be equipped with knowledge of evaluating network infrastructure and web application security [5], while being a supporting member in an iCAST team. It will analyze the exam objective and technical syllabus of accepted certificate, for example CREST Certified Infrastructure Tester, Offensive Security Certified Expert (OSCE), and compare them with other unaccepted certificates like IIS Certified Web Application Security Professional (CWASP). [6]

Secondly, it will investigate iCAST specialist and iCAST Manager. iCAST specialist is built on top of Infrastructure tester and a core member to deliver Simulated Attack [7], whereas iCAST Manager must guarantee that a simulated attack is performed in safe and legal manner with minimized impact to the client’s production system. Therefore, sufficient experience in managing incidents and simulated attack is required. [7] The comparison method will be like that of part one. Accepted certificates like CREST Certified Simulated Attack Specialist, CREST Certified Simulated Attack Manager are compared with unaccepted certificates like EC-Council Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA).

Finally, this project also plans to cover a brief guide for performing iCAST. According to Penetration Testing Execution Standard (PTES), there are seven steps in the penetration test, namely, Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, Reporting. [8] The guide plans to briefly cover it by using Framework Metasploit.
8. What is iCAST?

With reference to figure 1, iCAST (intelligence-led Cyber Attack Simulation Testing) is the final stage of C-RAF (Cyber Resilience Assessment Framework) of the HKMA and is the focus of this project. iCAST is not the same as traditional penetration testing. iCAST is intelligence-led, which involves threat intelligence gathering to guide the simulating attack. [9] Moreover, traditional penetration test often performs on an isolated environment, which is disconnected from the internet. In contrast, iCAST is supposed to perform on production environment, which is currently running system with staff. Human Factors are usually the weakest points in a production system. For example, simulated phishing mail campaigns can be used to access internal staff security awareness. [10]

iCAST is divided into three roles. Firstly, iCAST Manager is responsible for leading the team and general management. Secondly, iCAST Specialist is the core tester. Thirdly, iCAST Tester plays as a supporting tester. [9]

Figure 1. Three stages of C-RAF [11]
9. iCAST Tester

In December 2016, HKMA released the accepted qualifications list for performing iCAST. [4]. Having equivalent certification is viewed as qualified to perform iCAST testing in Hong Kong. On the top of figure 1, HKIB’s CCASP (Certified Cyber Attack Simulation Professional) is developed by HKIB (Hong Kong Institute of Banker) and ASTRI (Hong Kong Applied Science and Technology Research Institute). CCASP is benchmarked with industrial standard with support of CREST, which is an Intelligence-Led Testing Framework from UK. [11]

- **iCAST Tester for IT infrastructure testing**
  - HKIB’s CCASP – Certified Infrastructure Tester
  - CREST Certified Infrastructure Tester
  - GIAC Penetration Tester (GPEN)
  - Offensive Security Certified Expert (OSCE)

- **iCAST Tester for web application testing**
  - HKIB’s CCASP – Certified Web Applications Tester
  - CREST Certified Web Applications Tester
  - GIAC Web Application Penetration Tester (GWAPT)
  - Offensive Security Web Expert (OSWE)

Figure 2. Accepted qualifications for being iCAST Tester by HKMA
9a. iCAST Tester certifications comparison in high level

By comparing all these accepted certifications in high level, with reference to Table 1, HKIB’s CCASP and CREST Certified are the strictest certifications, because their assessments include both written exam and practical exam, whereas GIAC certification is relatively loose, since it only requires written exam. Finally, Offensive Security Certified is in between the above-mentioned certificates, as it puts more focus on practical aspect than theoretical knowledge by examining practical only.

<table>
<thead>
<tr>
<th>Certification name</th>
<th>Examination Requirement</th>
<th>Exam Fee</th>
</tr>
</thead>
</table>
| HKIB’s CCASP – Certified Infrastructure Tester | Examination consists of two parts  
1. Written Examination  
120 multiple-choice questions  
2 out of 3 longer form questions  
Passing mark = 67%  
Exam length: 3 hours  
Delivered at Pearson Vue test centers  
Close Book in written examination  
2. Practical Examination  
Several mini applications – each with a set of questions  
Passing mark = 67%  
Exam length: 4.5 hours  
Delivered at a CCASP/CREST examination center  
Open book in practical Examination [12] | 3060HKD (~400USD) For Written exam + 13500HKD (~1700USD) For Practical exam [12] |
| HKIB’s CCASP – Certified Web Applications Tester | Examination consists of two parts  
1. Written Examination  
150 multiple-choice questions  
Delivered at Pearson Vue test centers  
Exam length: 2hrs 30mins [14] | 1600 British Pound (~2100USD) + Value Added Tax |
<table>
<thead>
<tr>
<th>Certification</th>
<th>Practical Examination</th>
<th>Cost and Details</th>
</tr>
</thead>
</table>
| CREST Certified Web Applications Tester | 2. Practical Examination  
Hands-on penetration testing examination  
Delivered at CREST examination center [5] |                                                                                  |
| GIAC Penetration Tester (GPEN) | Only Written Exam is needed  
- 1 proctored exam  
- 115 questions  
- Exam Length: 3 hours  
- Passing Score = 74%  
- Open book exam [17] [20] | 1699 USD  
Included  
2 practice tests [19] |
| GIAC Web Application Penetration Tester (GWAPT) | Only Written Exam is needed  
- 1 proctored exam  
- 75 questions  
- Exam Length: 2 hours  
- Passing Score = 71%  
- Open book exam [18] [20] |                                                                                  |
| Offensive Security Certified Expert (OSCE) | Only Practical Exam is needed  
- Compromise a remotely-hosted dedicated vulnerable network within 24 hours by obtaining administrative access  
- Submit a detailed penetration test report consisting of the steps required to exploit each application [21] [22] | 1200 USD  
Included  
30 days lab access [23]  
Currently Unavailable [24] |

Table 1. Comparing all accepted certification for iCAST
9b. CREST Certified Infrastructure Tester and Web Application Tester

CCASP has just been released in late 2016, whereas CREST was first launched in June 2015. [25] CREST syllabus is relatively more detailed and fixed compared to CCASP. More importantly, CCASP is built on top of CREST. As an illustrative, so CREST is selected to be analyzed.

According to the latest CREST Certified Tester Technical Syllabus [5] version 2.2 released in May 2017, CREST Infrastructure Tester and Web Application Tester share a common set of exam topic, but some practical exam focuses are different. Infrastructure Tester is examining the knowledge in checking detailed configuration in operation system and assessing network infrastructure security. In Contrast, Web Application Tester concentrates on assessing web application security. CREST Tester exam’s syllabus is categorized into ten topics. Each exam topic will be briefly explained.

1. Soft Skills and Assessment Management
   This topic covers the knowledge in law and compliance, penetration testing planning, risk related during test and test result reporting.

2. Core Technical Skills
   This topic covers the knowledge in network architecture, firewall setting, cryptography theory and application, file system permissions and audit techniques.

3. Background Information Gathering & Open Source
   This topic involved data collection in technical way, and cover the knowledge in domain name checking (WHOIS), advanced Google search, HTML Web analysis and Email analysis.

4. Networking Equipment
   This topic examines the knowledge in networking tools like Telnet, protocols and network hardware configurations.

5. Microsoft Windows Security Assessment
   This topic covers advanced usage in Windows users, Passwords managements and vulnerabilities.

6. Unix Security Assessment
   This topic covers knowledge in Unix User management, vulnerability, control in File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network File System
(NFS) and Secure Socket Shell (SSH) Management. Securing SSH is important because it gave out access with administrator rights, which grant the rights to do almost everything.

7. Web Technologies
   This topic examines the knowledge in common web server vulnerabilities, web protocol theory, web server-side language like JSP and PHP.

8. Web Testing Methodologies
   This topic covers the knowledge in information gathering from Web mark-up for example, developer comments and hidden form fields, common loopholes in authentication which checks identity and authorization which if this identity has access right or execution rights. Moreover, it also examines the knowledge in vulnerabilities of injection attack and Cross Site Scripting attack (XSS).

9. Web Testing Techniques
   This topic covers the knowledge in session id attack, code injection, data confidentiality and integrity.

10. Databases
    This topic will assess the knowledge in Microsoft SQL Server, Oracle RDBMS, and database connection management.
9c. EC Council – Certified Ethical Hacker

Certified Ethical Hacker is one of the most popular certifications in the field of penetration test. However, this certification is not accepted by HKMA as qualified iCAST tester. Therefore, this certificate is selected for analysis. The latest version of CEH is version 9 released in 2016. This certificate has 18 topics for examination. Each Topic will be summarized. In table 2, exam format of EC Council Certified Ethical Hacker is illustrated.

1. Introduction to Ethical Hacking

This topic covers Information security overview, Hacking Concepts, Information Security Controls, for example, Vulnerability Assessment and Penetration Testing, and related laws knowledge.

2. Footprinting and Reconnaissance

This topic covers different kinds of footprint Methodologies, for example, email footprinting, competitive Intelligence Gathering and Social Engineering.

3. Scanning Networks

This topic covers different kinds of network scanning technique, for example, Port Scanning, Vulnerability Scanning, and Network Diagrams.

4. Enumeration

This topic covers the concept of Enumeration and a few kinds of Enumeration, for example, NetBIOS, Simple Mail Transfer Protocol (SMTP) and Network Time Protocol (NTP).

5. System Hacking

This topic covers five major part. Firstly, Password Cracking is stealing user password by numerous methods. Secondly, Privilege Escalation is getting administrator right in an unauthorized way. Thirdly, Executing Applications is learning software like RemoteExec and Keylogger, which is used for logging down the keystroke. Fourthly, Hiding Files is to understand different Rootkit which means malicious software, for example, ZeroAccess. Finally, Covering Tracks is learning how to remove the trace of using this computer by using tool like CCleaner.
6. Malware Threats

   This topic covers Trojan, Malware Detection and Malware Reverse Engineering.

7. Sniffing

   Sniffing means listening to a conversation secretly. For example, unencrypted HTTP
   communication channel content can be sniffed off. Sniffing Technique like DHCP Attack,
   ARP Poisoning and DNS Poisoning will be covered.

8. Social Engineering

   Social Engineering is an attack tricking people to disclose confidential information through
   human interaction. It can be performed through emails, phone, in person and Social
   Engineering Tools (SET).

9. Denial-of-Service

   Denial-of-Service is an attack preventing legitimate users from accessing the service by
   making service server malfunction. This topic covers how to perform this attack, its
   protection method and corresponding case study.

10. Session Hijacking

    Session is a token key assigned by server after log in. Session Hijacking means that this
    key is stolen within its valid period. Hacker could use this key to get unauthorized
    information. This topic covers application-level, network-level session hijacking and its
    countermeasures.

11. Hacking Webservers

    This topic covers web server attack methodologies and its countermeasures like Patch
    Management.

12. Hacking Web Applications

    This topic covers Web application attack methodologies, tools like CookieDigger, and its
    countermeasures.

13. SQL Injection

    This topic covers SQL Injection methodologies, tools like SQL Power Injector and its
    countermeasures.
14. Hacking Wireless Networks

This topic covers Wireless Hacking Methodology, Wireless Hacking Tools, Bluetooth Hacking and its countermeasures.

15. Hacking Mobile Platforms

This topic will examine the knowledge in hacking mobile device, for example, IOS and Android, and covers mobile security guidelines.

16. Evading IDS, Firewalls, and Honeypots

Evading IDS is a short term for Evading Intrusion Detection System. It is a skill to keep hacking undetected from detecting system. Firewalls configurations knowledge will also be covered in this topic. Honeypots is a computer system that act as vulnerable system to attract cyber-attack to distract attacker from the system containing valuable data. Knowledge in using famous Honeypot tool like KFSensor will be covered in this topic.

17. Cloud Computing

This topic covers cloud computing attack, cloud security and knowledge in using its tools.

18. Cryptography

This topic covers knowledge in cryptography, Public Key Infrastructure (PKI), Disk Encryption, Cryptography attacks and its tools.

[26]

<table>
<thead>
<tr>
<th>Exam paper information - EC Council – Certified Ethical Hacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Questions</td>
</tr>
<tr>
<td>Test Duration</td>
</tr>
<tr>
<td>Test Format</td>
</tr>
</tbody>
</table>

Table 2. Exam format of EC Council – Certified Ethical Hacker [27]
10. CREST Threat Intelligence Analyst

CREST Threat Intelligence Analyst examination is firstly issued on 1 June 2017. This exam will cover knowledge in collecting and analyzing information in support of threat intelligence. Threat intelligence is an important phrase in Intelligence Led Penetration test. In the following sections, it will briefly cover four important parts of this exam, namely, Direction and Review, Data Collection, Data Analysis and Product Dissemination.

10a. Direction and Review

1. Developing Terms of Reference
   This topic covers the knowledge in writing typical Terms of Reference to understand the objective of this threat intelligence task.

2. Importance of Project Review
   This topic covers the knowledge in assessing intelligence output, for example, timeliness and accuracy, and understanding the importance in output feedback.

3. Dealing with Intelligence Gaps
   Intelligence Gap is defined that some critical information is missing to perform intelligence analysis. This topic covers the knowledge in intelligence gap and identifying likely sources of information to fill an intelligence gap.

10b. Data Collection

1. Function & Use of a Collection Plan
   This topic covers knowledge in writing and interpreting data collection plan.

2. Use of a Collection Worksheet
   This topic covers knowledge in using data collection worksheet. For example, what sources were checked, what search terms were used and when the search were performed.

3. Types of Sources
   Open-source intelligence(OSINT) is the information collected from public for intelligence analysis. It is not related to open source software. OSINT can be defined into 6 fields,
namely, Media, Internet, Public Government Data, Professional and Academic Publications, Commercial Data, Grey Literature.

This topic covers the knowledge in classifying different types of data source. For example, Open-source intelligence (OSINT), Human intelligence (HUMINT) and Signals intelligence (SIGINT).

4. Source Reliability and Grading
This topic covers the knowledge in source and information reliability grading.

5. Specific Sources
This topic covers the knowledge in retrieving data from typical technical sources such as WHOIS, DNS, malware analysis, social media, document metadata and interpreting the corresponding information.

6. Boolean Search Strings
This topic covers the knowledge in using boolean search string. For example, searching "bigtable -site:google.com" which means searching "bigtable" but exclude the information from google site.

7. Basic Source Analysis
This topic covers knowledge in recognizing biased or inaccurate online sources.

8. Operational Security (OPSEC)
OPSEC is a security control to prevent several pieces of individual data from leaking confidential data after grouping these pieces of data. Generally, separating personal web use from work use is a basic approach. This topic covers the knowledge in OPSEC and anonymization tools such as Tor and i2p.

10c. Data Analysis

1. Hypothesis Testing
This topic covers the knowledge in proving and disproving a hypothesis.

2. Facts, Assumptions, Premises & Inferences
A premise is a proposition supporting or helping to support a conclusion. Inferences are steps reaching conclusions with support of evidence and reasoning. This topic covers the knowledge in distinguishing and understanding facts, assumptions, premises and inferences.
3. Expressing Likelihood / Certainty
This topic covers the knowledge in applicability of terms such as ‘possible’, ‘probably’ and ‘certainly’.

4. Circular Reporting
Circular reporting is a situation that a piece of data appears to come from different independent sources, but actually from one same source. One typical example is that Wikipedia and press quoting each other dependently resulting in false information publication. This topic covers the knowledge in circular reporting and its prevention.

5. Cognitive Biases
Cognitive Bias is an obstacle in correct intelligence analysis. This topic covers the knowledge in major types of bias like Confirmation bias and Halo effect, and its counter-measure.

6. Analytical Techniques
This topic covers the knowledge in interpreting graphical data like timeline and network diagram.

10d. Product Dissemination

1. Structured / Machine Readable Threat Intelligence
Structured Threat Information Expression (STIX) is a standardized XML programming language for sharing cyber threat information which can be is easily readable by software and humans. Since STIX version 2.0, Cyber Observable Expression (CYBOX) is also integrated into STIX.

This topic covers the knowledge in STIX, CYBOX and Trusted Automated eXchange of Indicator Information (TAXII). It also covers details of STIX message format and machine-readable TI pros and cons.

2. Unstructured / Human Readable Threat Intelligence
This topic covers the knowledge in selecting appropriate dissemination mechanism, for example, comparing written report and verbal briefings. It covers Human Readable Threat Intelligence pros and cons and importance of report accuracy, brevity, clarity.
3. Intelligence Sharing

This topic covers the knowledge in ‘Need to Know’ and ‘Need to Share’ concepts and ability of classifying confidential information. It also covers knowledge of common intelligence sharing initiatives.

[28]
11. CREST Simulated Attack Manager and Specialist

These two certifications are also examining the following topics with different depth. In the following paragraphs, it will briefly discuss some important related skills and requirement, which makes Intelligence-led penetration test different than traditional pen test.

CREST Simulated Attack Technical Syllabus

11a. Soft Skills and Assessment Management

1: Threat Intelligence

Threat Intelligence is about information of the potential threat and critical hints to hack into a system. It is required to use intelligence to form a simulated attack and justify the correctness of data.

2: Operations Security (OpSec)

Operation security is to prevent sensitive data leakage because of user’s careless behavior. For example, sharing a snapshot from working environment, share company status in social media, and using insecure communication channels like HTTP.

3: Social Engineering Attacks

If the system found no observable vulnerability, human behavior may give a hint or even breaking point. Social Engineering attacks will trick people to collect intelligence. For example, email/phone-based phishing attack with “cover story”.

4: Physical Security

Physical security need to identify the entry point weakness. For example, badge usage for identify verification, CCTV and alarm usage.

11b. Core Technical Skills

1: Network Mapping & Target Identification

It examines the skills to scan the network and create a target list.
2: Filtering Avoidance Techniques

Advanced server usually has network flow monitoring. It examines how to make the data packet be undetected.

3: Packet Crafting

It examines crafting a packet with modifying source IP and port, TTL, fragmentation and generating ICMP packets.

4: Audit Techniques

Audit technique is to assessing process socket status like port opening and the application patch level. If the patch level is found vulnerable, it is an important threat intelligence.

5: Automation and Scripting

It examines the skills of scripting like Windows batch, Unix Shell and Python.

6: VPN Technologies

It examines the VPN knowledge and practical configuring experience, for example, IPSEC, L2TP, OpenVPN.

11c: Background Information Gathering & Open Source

1: Customer Web Site Analysis

It examines the skill in inspecting html source code with developer content, and API analyzing.

2: Web Enumeration and Social Media

It requires effective use of search engine to retrieve target’s information from social media and understanding the implication of the collected data. Moreover, it examines the knowledge in specialist search engine, for example, Shodan.

3: Document Metadata

It examines the skills in retrieving meta data from different file format, for example, PDF, MS doc, JPEG. Tools like Exiftool would be useful for this task.
11d. Enumeration/Reconnaissance

1: Enumeration of missing security updates

It requires the skills in listing software version and finding corresponding software missing patches with security vulnerabilities.

2: Enumeration of sensitive files

It examines the skills of conducting complex searches for sensitive data by command.

11e. Trojan Delivery

1: Email Spoofing

Email spoofing can be done by using direct SMTP protocol. It also examines the ability to deliver phishing campaigns.

2: Anti-Spoofing Countermeasures

It examines knowledge in anti-spoofing techniques, for example, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

3: Trojanised Legitimate Binaries

It examines the skills in adding malicious code on signed library without compromising the original function, for example, DLL side loading.

11f. Client-Side Exploitation Skills

1: Exploitation of common document formats

It examines the skills in creating trojanised documents, for instance, Adobe Acrobat, MS doc. It can be done by executing code from those document in unpatched software or exploiting latest software with social engineering attack.

2: Exploitation of rich content

It can require the skills in using Adobe Flash or Java Applet to exploit a web browser.
12. Intelligence Led Penetration test case study

12a. Case 1. Social engineering - Credential harvester

The Credential Harvester method will utilize web cloning of a website that has a username and password field and harvest all the information posted to the website.

Finished set up. Wait for victim connect and submit credential.

Figure 3. Snapshots for Credential Harvesting
Result:

![Image of login interface](image)

**Figure 4. Snapshots for Credential Harvesting Result**

Account name and password are collected.
This case study API is modified on VM IMF. [31]
12b. Case 2: OSINT and Social engineering - Spoof number attack

Supposed there is ABC victim company with IP 192.168.1.116

Figure 5. Nmap result

Only port 80 is found. Found a login page: http://192.168.1.116/login/

Contact information found from http://192.168.1.116/contact.php (Open source intelligence)

Figure 6. Snapshots for different login credential [31]

In the next step, A spoof admin phone number is calling back to office and ask to reset password to 123456. [32] This case study UI is modified on VM IMF. [31]

Supposed there is ABC victim company with ip 192.168.1.123.


“ExifTool by Phil Harvey”, which is a tool for handling meta data, is used to analyses this pdf meta data.

After using ExifTool on that pdf file, a statement “Creator Tool: Adobe InDesign CC 2017 (Windows)” is found, which is critical for threat intelligence. This product name will bring a lot more hidden information than the file itself. Product name can be derived version number and ,more importantly, corresponding vulnerabilities.


![Vulnerability Details: CVE-2017-11302](image)

Figure 7. Version number from product name [33]

![Vulnerability of corresponding version](image)

Figure 8. Vulnerability of corresponding version [34]

**Description:** A vulnerability was reported in Adobe InDesign. A remote user can cause arbitrary code to be executed on the target user’s system.

A remote user can create a specially crafted file that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system.

Honggang Ren of Fortinet’s FortiGuard Labs reported this vulnerability.

**Impact:** A remote user can create content that, when loaded by the target user, will execute arbitrary code on the target user’s system.

Figure 9. Description and impact of the vulnerability [35]
Finally, a severe vulnerability with 10.0 CVSS score is found. If the remote victim machine installed 11.4.1 exactly version. The vulnerability “Execute Code Overflow Memory corruption” could be used to exploit the remote machine. Meta information of a file presents in a silent way without user notice, but it can be interpreted to be useful by pen tester.
12d. Case 4: OSINT – Q&A site & Operation Security (OpSec)

Supposed there is ABC victim company with ip 192.168.1.112 with http 80 port.

Using command “dirb http://192.168.1.112/” with common words list to scan its web content. However, nothing useful is found.

Figure 10. Dirb result

With the help of threat intelligence, a critical information is collected. A junior software developer indirectly disclosed API link to a question and answer site for programmer.

Figure 11. Question example [36]


Figure 12. Curl result [37]

The remote system can be accessed by posting reverse shell in PHP. Afterward, it can be further exploited by privilege escalation with the vulnerabilities found inside. The threat intelligence drives the penetration test in a quick and effective direction instead of using brute force or dictionary attack. The question idea is inspired by a real question. [36] This case study idea is inspired by VM sickos. [37]
14. Limitations

1. Time Limit
   The best way to understand Intelligence Led Penetration test is to take the certified exam. However, most certification take at least 3 years practical experience. There is insufficient time to investigate into that level.

2. Budget Limit
   There are many useful and paid lab course that teaching practice for specific certification exam. [29] However, these courses are valuable and expensive. Alternatively, only free online source is selected as study materials.

3. Time Changing Factor
   Intelligence Led Penetration test standard may be changing over time. Because there are new security loopholes found out every day and best practice will be updated as well. This paper aims to understand current scope.
15. Project Schedule and Plan

<table>
<thead>
<tr>
<th>Date</th>
<th>Task</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>September</td>
<td>Phase 1: A Detailed Project Plan</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>Phase 1: Project Web Page</td>
<td>Completed</td>
</tr>
<tr>
<td>October</td>
<td>iCAST Tester (IT infrastructure &amp; Web)</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>iCAST Tester certifications comparison</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>CREST – Certified Tester</td>
<td>Completed</td>
</tr>
<tr>
<td>November</td>
<td>EC Council – Certified Ethical Hacker</td>
<td>Completed</td>
</tr>
<tr>
<td>December</td>
<td>CREST Threat Intelligence Analyst</td>
<td>Completed</td>
</tr>
<tr>
<td>January</td>
<td>Phase 2: First Presentation &amp; Interim report</td>
<td>Completed</td>
</tr>
<tr>
<td>February</td>
<td>iCAST Specialist</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>iCAST Manager</td>
<td>Completed</td>
</tr>
<tr>
<td>March</td>
<td>Case Study for Intelligence Led Penetration test</td>
<td>Completed</td>
</tr>
<tr>
<td>15 April 2018</td>
<td>Phase 3: Final Report</td>
<td>Completed</td>
</tr>
<tr>
<td></td>
<td>Project Presentation</td>
<td>-</td>
</tr>
<tr>
<td>2 May 2018</td>
<td>Project exhibition</td>
<td>-</td>
</tr>
</tbody>
</table>

12. Conclusion

This project aims to study Intelligence Led Penetration test through iCAST. After reviewing CREST basic certifications, both technical theoretical knowledge and practical skills are being examined. Unqualified certifications usually put most focus on practical skills, for example, knowledge in using a software, instead of theoretical knowledge.

“The difference between this and conventional technical assessments of network security is that ILPT is based upon rich contextualised intelligence.” [37]

Threat intelligence gathering is an expensive task through a lot of ways, for example, HUMINT, OSINT, even physical security. The intelligence leads the penetration test in a right and effective direction. It could find out more vulnerabilities that traditional penetration test cannot. It is a better security defense policy which we should apply nowadays in order to fix the loopholes before the real hacker.
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Three stages of C-RAF</td>
<td>5</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Accepted qualifications for being iCAST Tester by HKMA</td>
<td>6</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Snapshots for Credential Harvesting</td>
<td>22</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Snapshots for Credential Harvesting Result</td>
<td>22</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Nmap result</td>
<td>23</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Snapshots for different login credential</td>
<td>23</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Version number from product name</td>
<td>24</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Vulnerability of corresponding version</td>
<td>24</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Description and impact of the vulnerability</td>
<td>24</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Dirb result</td>
<td>26</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Question example</td>
<td>26</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Curl result</td>
<td>26</td>
</tr>
</tbody>
</table>

List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Comparing all accepted certification for iCAST</td>
<td>8</td>
</tr>
<tr>
<td>Table 2</td>
<td>Exam format of EC Council – Certified Ethical Hacker</td>
<td>13</td>
</tr>
</tbody>
</table>
References


[2] CREST - Certified Simulated Attack Specialist

[3] EC-Council - Certified Ethical Hacking Certification (CEH)
https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/


[5] CREST Certified Web Applications Tester and CREST Certified Infrastructure Tester – technical syllabus

http://www.iisecurity.in/courses/cwasp.html

[7] CREST Certified Simulated Attack Manager and Certified Simulated Attack Specialist – technical syllabus p.4

[8] PTES Technical Guidelines

[9] CRA report

[10] HKMA speech in 20160518 – p.11
http://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160518e2.pdf

https://www.astri.org/cybersecurity-training/

[13] - CREST Certified Infrastructure Tester

[14] - CREST examination information at Pearson VUE
http://www.pearsonvue.com/crest/

[17] – GIAC Penetration Tester (GPEN)
https://www.giac.org/certification/penetration-tester-gpen

[18] – GIAC Web Application Penetration Tester (GWAPT)
https://www.giac.org/certification/web-application-penetration-tester-gwapt

[19] – GIAC Cert Attempt Pricing
https://www.giac.org/registration/cert-attempt#pricing

[20] – GIAC Proctor Exam
https://www.giac.org/exams/proctor


[22] - Offensive Security Web Expert

[23] - Cracking the Perimeter (CTP) (Course for Offensive Security Certified Expert)
https://www.offensive-security.com/information-security-training/cracking-the-perimeter/

https://www.offensive-security.com/information-security-training/advanced-web-attack-and-exploitation/

http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

[26] - Certified Ethical Hacker Course Outline
https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/course-outline/
[27] - Certified Ethical Hacker Exam Format
https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

[28] - CREST Threat Intelligence Analyst Syllabus

[29] - CREST accredited courses
http://www.crest-approved.org/uk/partners/crest-accredited-training-courses/index.html


[31] - Vulnhub VM IMF
https://www.vulnhub.com/entry/imf-1,162/

[32] - Spoof card
https://www.spoofcard.com/

[33] - Adobe InDesign Information in wiki
https://en.wikipedia.org/wiki/Adobe_InDesign

[34] - Vulnerability CVE-2017-11302

[35] - Vulnerability 1039785
https://securitytracker.com/id/1039785

[36] - Example of Stackoverflow question

[37] - Vulnhub VM sickos 1.2
https://www.vulnhub.com/entry/sickos-12,144/

[37] - Intelligence-led penetration testing services from BAE