Security Problems in Telecommunication Networks

Table of contents

Introduction 2
Threats in telecommunications networks 2
What is Kali Linux ? 3
Protection 3
Pentesting automatization using reinforcement learning 3
Sources 6

Guichard Nicolas 190ADM040

Introduction

Now a days technology is everywhere, it is used by everyone in every kind of situation. It keeps growing just like telecommunication network. It is something very important and used in our every day life. But with the raise of users and technologies we are looking how to deal the question of security on these networks. Technologies using telecommunication software are too many and used in to many sensible entities (government, hospital, school, …).

Information Security is based on the **CIA triad:**

Confidentiality: Only authorized people have access to the data

Integrity: Assurance that data is trustwhorthy

Availability: Data need to be available when needed

The present document will discuss about employed solutions with regards to threats which weigh on telecommunication networks.

Threats in telecommunications networks

Telecommunications networks sudden a lots of attacks just like regular networks. The main threats are

DOS: Make the target unreachable, unavailable by for example by flooding with excessive amount of request. There is also DDOS attack which is the same but made by many sources at the same time.

Man in the middle : When someone intercepting all your transmission transparently. The attacker has all the control of your communication.

Zero day attack : Attack on a unknown vulnerability and which no security patch

There is a lot of threats/attack and the problem that this is not a predefined lists, every day their tons of new vulnerabilities discovered and new techniques/attacks created.

What is Kali Linux ?

Kali Linux is a Linux distribution based on Debian. The main purpose of it, is to regroup essential tools (more than 600 preinstalled) in order to realise pentest, forensic or search in security and more. This distribution is reputed among professionals and it possess also a big community.

Protection

To prevent any attacks on any kind of information system it's recommended to pass some official certification in order to have a security standard. For example in France, we do it one base on a risk analysis (EBIOS) then we will define all the security measures. One step important of this risk analysis and which can help to secure your system is to realise pentests on your information system. The goal of it is to attack your system in order to reveal all vulnerabilities. The task request a lot of skills and it's something very wanted these days.

Pentesting automatization using reinforcement learning

In the future, the goal is to use reinforcement learning (RL) and pentest in order to make the pentest autonomous, the task will be more easily and. But the big difficulty is that attack techniques are improving days after days that why it will be interesting to use RL, thereafter we will be able to let the system make the pentest and apply security patch to secure the system. Then the system will probably detect autonomously an intrusion perform and secure it.

Example :

- Gather HTTP responses :

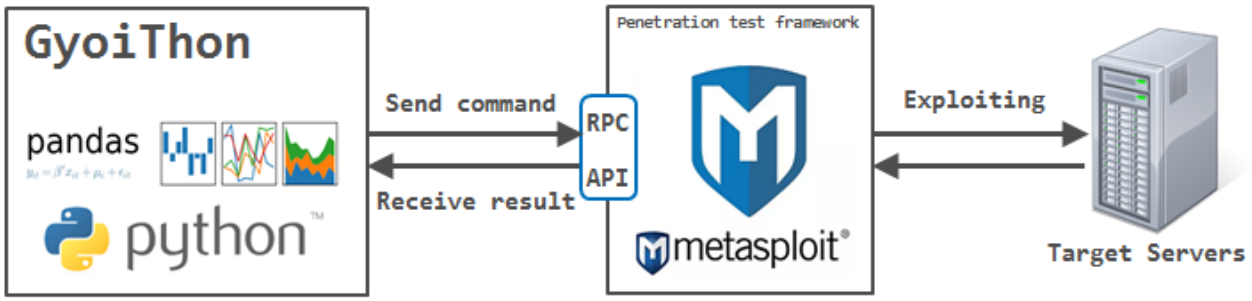
```
HTTP/1.1 200 OK
Date: Tue, 06 Mar 2018 03:01:57 GMT
Connection: close
Content-Type: text/html; charset=UTF-8
Etag: "409ed-183-53c5f732641c0"
Content-Length: 15271

...snip...
```

- Software identification :
  Gyoithon will use machine learning(Naïve Bayes) and the Etag found thanks to http responses to identify the software.

```
Etag: "409ed-183-53c5f732641c0"
```

- Exploit using Metasploit :
  Once the software is identified, it will run exploit using Metasploit.



- Generate scan report :
  And a scan report is generate with all the vulnerabilities found, if it works or not.

GyoiThon scan Report

Index	Item	Value
1	IP address	192.168.220.145
	Port number	21
	Product name	vsftpd
	Vuln name	VSFTPD v2.3.4 Backdoor Command Execution
	Type	shell
	Description	This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
	Exploit module	exploit/unix/ftp/vsftpd_234_backdoor
	Target	0
	Payload	payload/cmd/unix/interact
	Reference	[OSVDB] 73573 [URL] http://pastebin.com/AetT9sS5 [URL] http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

Sources

https://www.simplilearn.com/telecommunications-and-network-security-rrt3co34vd101-video

https://www.buckeyetelecom.com/blog/what-exactly-is-telecommunication-network-security

https://www.marketreportgazette.com/how-network-security-policy-management-market-development-is-changing-business-needs-palo-alto-networks-inc-algosec-inc-check-point-software-technologies-ltd-forcepoint-llc-firemon-llc-hewle

https://medium.com/brandon-lammey-intro-to-ai/cyber-defense-and-ai-automating-penetration-testing-91ccb56dd93a

https://resources.infosecinstitute.com/machine-learning-in-offensive-security/

https://arxiv.org/ftp/arxiv/papers/1905/1905.05965.pdf

https://www.securitynewspaper.com/2018/06/02/gyoithon-tool-make-penetration-testing-machine-learning/

https://securityonline.info/gyoithon/

https://github.com/gyoisamurai/GyoiThon.git