Pyhton Web Application Honey pot

Project Mentors	1) Aditya Jain 2)
Project Heads	1) Bhaskar Kataria 2) Nihar Rai 3) Aniruddh Sujish 4) Md Rushad
Mentees	1) 2) Leave this empty for now

[Project Mentors → 4th Years; Project Heads → 3rd Years; Mentees → 2nd years;]

Aim

To contribute to Snare and tanner, a open source web application honeypot

Methodology

- First may be we can start with documentation of all the classes and files
-
-

Timeline

Checkpoint No.	Deadline	Goal/Objective	Comments (if any)
1	*31st August, 2020		
2	*30th November, 2020		
3	*End of January		

Literature Review

Introduction

Honey pots are decoy systems that are used in the network to divert attacks from real systems and/or to study tools and techniques used by “blackhat hackers”
There are variety of honeypots available such as glastopf which was a gsoc project, dionaea, Dshield, kippo etc. These are all different kind of honeypots, we will be focusing on web application honeypots, glastopf is one such honeypot. We will be working on its successor snare and tanner. These honey pots can mimic a web-application or are themselves a vulnerable web application that allows attackers to attack them . Web application honey pots are replica of the real application; it attracts the attackers to attack them. This set of information help in building the defending strategies against such attacks.

Snare and Tanner

SNARE, a web application honeypot sensor, is the successor of Glastopf. SNARE has feature parity with Glastopf and allows to convert existing web pages into attack surfaces.

TANNER is SNARES "brain". Every event is send from SNARE to TANNER, gets evaluated and TANNER decides how SNARE should respond to the client. This allows us to change the behaviour of many sensors on the fly. We are providing a TANNER instance for your use, but there is nothing stopping you from setting up your own instance.

https://github.com/mushorg/snare
https://github.com/mushorg/tanner

References

[1] Kamaldeep Sehgal, Dr. Ali Mansour “Msc project report, Study on web application honey pots. Available online: https://uobrep.openrepository.com/bitstream/handle/10547/302313/Sehgal%5B1%5D.pdf?sequence=1&isAllowed=y

This report is about the design and development of existing web application honey, how well they perform and future work.
Generally honey pots are designed to detect and report attacks against network and network systems like DNS, DHCP, DoS/DDoS etc. Such systems cannot detect and report web applications specific attacks like SQL injection, cross site scripting,

command injection etc. To detect such attacks we need to construct and deploy a different kind on honey pot called web application honey pots.
The web application honeypots make the attackers to peep into the web applications and attack them which is growing day by day. There are also anti-hacking tools that are used against such attacks however they still do grow with new techniques and method. This is where honey pots come into the picture as they are then used as a decoy systems to trap the activities of the attacker.

The best place to deploy honeypot in the network is alongside production web server(s) or in a separate DMZ protected by firewall(s) and IDPS (intrusion detection and prevention system). The logs generated by it can help detect web application attacks against the web servers in the production network and help gather information (such as IP address, tools, techniques etc) related to those attacks. This information can be used to further secure the web application servers and can also detect coordinate attacks against web servers

[2] Hibatul Wafi, Andrew Fiade, Nashrul Hakiem, Rizal Broer Bahaweres
Deptartment of Informatics, Faculty of Science and Technology
UIN Syarif Hidayatullah Jakarta, Indonesia
Implementation of Modern Security systems Honeypot Honey Network on Wireless Networks
https://www.researchgate.net/publication/318577179_Implementation_of_a_modern_security_systems_honeypot_Honey_Network_on_wireless_networks

This paper deals with how modern honeypot or a collection of honeypots called honey net can deployed and used for improving security of different aspects of a system. How different types of honeypot can be used together such as SSH honeypot, web application honeypot and network honeypot to properly utilize the power of honeypots. Paper also describes about the implementation of the scenario and what can be the topology, configuration of different honeypot in those scenario and results based on all these configuration and scenarios.
[

Bill of Materials

Sl No.	Name of component	Cost of component	Quantity Required	Total Cost
1				
2				
3				
				Grand Total: