Community Sharing

# SNORT

* SSH into IP Address
  + ssh <user>@<ipaddress>
* Check SNORT version
  + Snort –V
* Directory of SNORT configuration
  + /etc/snort
* Configure SNORT
  + vi /etc/snort
  + nano /etc/snort
* Include your custom SNORT rule custom.rules
  + Include $RULE\_PATH/custom.rules
* Sample of a SNORT Rule
  + Alert tcp $EXTERNAL\_NET any -> 192.168.1.0/24 80 (msg: “Intrusion Alert!”; content: “Intrude”;)
    - Alert – accept for SNORT
    - Tcp – protocol
    - $EXTERNAL\_NET – variable for source
    - Any – port
    - -> – Direction
    - 192.168.1.0/24 – Destination
    - 80 – Port
    - Msg:”Intrusion Alert!” – Message displayed
    - Content: “Intrude” – Type of content SNORT is looking for (SNORT allows Hexadecimal encoding to be insert in this portion of the snort rules for example: content: “|696e7472756465647ca|” )
  + Alert icmp 192.168.2.0/24 any -> 192.168.1.0/24 any (msg: “ICMP Scan echo”; dsize:16 ; itype:16; content:”|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|”;)
    - Dsize:16 – packet payload size (16 Bytes)
    - Itype:16 - ICMP type value
  + Source: <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node33.html#SECTION00467000000000000000>

# Tripwire

* Command for viewing tripwire report file
  + Twprint
  + Source: <https://manpages.debian.org/testing/tripwire/twprint.8.en.html>

# Web Application Vulnerabilities

## SQL INJECTION

* ‘ OR 1=1--
* ‘ OR 1=1 #
* There is a difference between – and #, both function as the same (comment), however # is only for MSSQL and -- is applicable to all databases
* Source 1: <https://www.owasp.org/index.php/SQL_Injection>
* Source 2: <https://portswigger.net/web-security/sql-injection/cheat-sheet>
* Beware there might be a validator on client side
  + In order to bypass the client side use burp suite
    - Edit values or parameters within the burp suite interceptor to alter the SQL injection
* Practice Practical 6 Exercise 7: SQL Injection

## Checking For Hidden Attribute in Web Application

* Open up “Mozilla FireFox” Broswer -> Right click on any part of the web page -> Inspect Element
* Do take a look at all Hidden Field

## Cross Site Scripting

* Do make sure to check every single textbox for cross site scripting by entering <script>alert(“XSS Test Message”)</script>

## Authentication Flaws (Authentication Bypass)

* Make sure you use burp suite and configure it to intercept the GET/POST request
* Check on any cookie value that is particularly interesting
* Try changing that value to see what is there and changes to the response of your website
* Practice Practical 6: Exercise 13

## Robots.txt

* Do Check the website’s robots.txt

## Local File Inclusion

* Do check up on the a ? in the URL
  + For example www.hackme.com/home.html**?page=1**
    - Any after the ?page= might be able to access certain paths
    - For example
      * www.hackme.com/home.html?page=/etc/passwd
      * www.hackme.com/home.html?page=../../../etc/shadow

Most Importantly PLEASE REDO all your practical 6 and practical 7