Notes 1.0

- Overview
- Tools
- Troubleshooting
- Networking
- Databases
- IDS
- Gadget
- OSINT
- Malware
- PowerShell
- Red Team
  - Training
  - Pentesting
    - Penetration Testing Tools Cheat Sheet
    - Scapy Cheat Sheet from SANS SEC560
    - CTF
    - OSCP
    - Reversing
    - Privilege Escalation

Pentesting

Summary: Opensource, Security, Tools, Pentesting

Table of Contents

- Offensive Security Journey
- Linux shells
- Kernel exploits
- Static binaries
- Explain Shell
- PWK-CheatSheet
- Adversarial Tactics, Techniques & Common Knowledge
- MS Signed #Mimikatz
- SSHPry spy on ssh connection like it is your terminal
- Firewall detection tool on a web application
- Nmap's XML result parse and NVD's CPE
- CVE-2017-11826
- WordPress Vulnerabilities Database
- Top 500 Most Important XSS Script Cheat Sheet
- Nmap GUI
- Penetration Testing & Hacking Tools List
- Fsociety Hacking Tools Pack
- Cloak - Backdoor In Any Python Script With Some Tricks
- Python script to auto-generate an obfuscated Word DDE payload
- Hiding payload into a picture
- A package of Pentest scripts

- ipv4Bypass: Using IPv6 to Bypass Security
- Tplmap assists the exploitation of Code Injection and Server-Side Template Injection

Shellcodes database

http://shell-storm.org/shellcode/

Pivoting Guide

https://artkond.com/2017/03/23/pivoting-guide/

socat examples

https://github.com/craSH/socat/blob/master/EXAMPLES

Offensive Security Bookmarks

https://jivoi.github.io/2015/07/03/offensive-security-bookmarks/

SQL Injection

http://websec.ca/kb/sql_injection

https://sqlwiki.netspi.com/tab/injectionTechniques/injectionPlacement

InjectX to Find XSS

https://forum.bugcrowd.com/t/tutorial-injectx-to-find-xss/790

Setting Pentesting Lab

https://cyberwardog.blogspot.ie/2017/02/setting-up-pentesting-i-mean-threat.html

user hunter using WinAPI calls only

https://github.com/fdiskyou/hunter

Kali-Linux

https://github.com/hackwith/Kali-Linux

Offensive Security Journey

oscp-certification-journey

Linux shells

escaping-restricted-linux-shells

Kernel exploits

https://www.kernel-exploits.com/

Static binaries

https://github.com/andrew-d/static-binaries

Explain Shell

https://explainshell.com/

PWK-CheatSheet

https://github.com/re-pronin/pwk-cheatsheet

Adversarial Tactics, Techniques & Common Knowledge

https://attack.mitre.org/wiki/Main_Page

MS Signed #Mimikatz

1- https://github.com/gentilkiwi/mimikatz

2- https://github.com/secretsquirrel/SigThief

3- https://specterops.io/assets/resources/SpecterOps_Subverting_Trust_in_Windows.pdf

SSHPry spy on ssh connection like it is your terminal

https://github.com/nopernik/sshpry

Firewall detection tool on a web application

https://github.com/Ekultek/WhatWaf

Nmap’s XML result parse and NVD’s CPE

https://github.com/CoolerVoid/Vision2

CVE-2017-11826

https://www.tarlogic.com/blog/explotando-word-cve-2017-11826/

WordPress Vulnerabilities Database

https://db.threatpress.com/

Top 500 Most Important XSS Script Cheat Sheet

https://gbhackers.com/top-500-important-xss-cheat-sheet/

Nmap GUI

https://github.com/danicuestasuarez/NMapGUI

Penetration Testing & Hacking Tools List

https://gbhackers.com/hacking-tools-list/

Fsociety Hacking Tools Pack

https://github.com/Manisso/fsociety

Cloak - Backdoor In Any Python Script With Some Tricks

https://www.kitploit.com/2018/01/cloak-backdoor-in-any-python-script.html

Python script to auto-generate an obfuscated Word DDE payload

https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads

Hiding payload into a picture

https://www.youtube.com/watch?v=lGmvlyCPouM

A package of Pentest scripts

https://github.com/leonteale/pentestpackage

ipv4Bypass: Using IPv6 to Bypass Security

https://github.com/milo2012/ipv4Bypass

Tplmap assists the exploitation of Code Injection and Server-Side Template Injection

https://github.com/epinna/tplmap

Page last updated: May 23, 2017
Site last generated: Aug 20, 2019
Cloned from idratherbewriting