Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

Reconocimiento

Reconocimiento: consiste en investigar al objetivo de ataque usando información públicamente disponible.

- Reconocimiento de baja tecnología: ingeniería social, acceso físico, hurgar en la basura.
- Búsquedas en Internet (STFW):
  - Google hacking
  - Bases de datos Whois
  - Búsquedas DNS
  - Bases de datos de vulnerabilidades

Baja tecnología

Ingeniería Social: Consiste en explotar las debilidades del "elemento humano" de los sistemas de información, utilizando engaños para obtener información confidencial.

Según Kevin Mitnick se basa en estos cuatro principios:

1. Todos queremos ayudar.
2. La primera reacción es siempre de confianza hacia el otro.
3. No nos gusta decir No.
4. A todos nos gusta que nos halaguen.

Baja tecnología

Acceso físico: Consiste en obtener acceso físico a un equipo en la red. El atacante puede instalar backdoors, escanear la red o sacar información importante.

Hurgar en la basura: Conocido como "dumpster diving", se analiza la basura de la persona u organización en busca de información. Pueden obtenerse diagramas de red, borradores con usuarios y claves, CD's, etc.

Búsquedas en Internet

Whois: es un protocolo TCP basado en petición/repuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet.

Proporciona información sobre:

- Nombre de dominio
- NIC handle
- Direcciones IP
- Teléfono de contacto
- Email de contacto
- Dirección postal
- Fechas de validez
- Servidores DNS

Búsquedas en Internet

DNS: es una base de datos jerárquica distribuida alrededor de Internet que proporciona información principalmente para la "resolución" de nombres de dominio a direcciones IP.

Principales "Resource records":

- **A (Address):** relaciona un nombre de dominio a una dirección IP específica.
- **MX (Mail eXchanger):** identifica los sistemas de correo electrónico válidos para un determinado dominio.
- **NS (Name Server):** identifica los servidores DNS asociados a un dominio.
- **PTR (PoinTeR):** proporciona resolución reversa: de IP a nombre de dominio.
- **TXT (TEXT):** asocia un texto arbitrario con un nombre de dominio.

Búsquedas en Internet

DNS: es una base de datos jerárquica distribuida alrededor de Internet que proporciona información principalmente para la "resolución" de nombres de dominio a direcciones IP.

Principales "Resource records":

- **A (Address):** relaciona un nombre de dominio a una dirección IP específica.
- **MX (Mail eXchanger):** identifica los sistemas de correo electrónico válidos para un determinado dominio.
- **NS (Name Server):** identifica los servidores DNS asociados a un dominio.
- **PTR (PoinTeR):** proporciona resolución reversa: de IP a nombre de dominio.
- **TXT (TEXT):** asocia un texto arbitrario con un nombre de dominio.

Conceptos

Vulnerabilidad: es una debilidad que influye negativamente en un activo y que posibilita la materialización de una amenaza. Se forma mediante la intersección de tres elementos: una susceptibilidad o debilidad (flaw), el acceso del atacante a la debilidad y la capacidad del atacante para explotar dicha falla.

Puede abarcar distintos ámbitos:

- Tecnología
- Procedimientos
- Controles
- Personas

Conceptos
Tipos vulnerabilidades

- **Buffer Overflow:** una anomalía en la que un proceso guarda datos en un buffer fuera del espacio de memoria que el programador tiene para utilizar. Los datos extra sobreescriben la memoria adyacente, lo cual puede contener datos o instrucciones de otros programas.

```
#include <string.h>
void foo (char *bar) {
   char  c[12];
   strcpy(c, bar);  // no bounds checking...
}
int main (int argc, char **argv) {
   foo(argv[1]);
}
```

Conceptos
Tipos vulnerabilidades

```
char code[ ] = "\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb"
"\x16\x5b\x31\xc0\x88\x43\x07\x89\x5b\x08\x89"
"\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d\x53\x0c\xcd"
"\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f"
"\x73\x68\x4e\x41\x41\x41\x41\x42\x42\x42\x42";
```

- **Format String:** surge de utilizar los datos de entrada de un usuario sin que sean filtrados o validados, pasándoselos luego a una función del programa que pueda interpretarlos textualmente.
- **Code Injection:** surge de procesar datos inválidos, y puede utilizarse para introducir (inyectar) código en un programa para cambiar el curso de ejecución.

Conceptos
Tipos vulnerabilidades

- **Directory traversal:** se da cuando no se validan correctamente las entradas de nombres de archivos por parte de los usuarios. Permite cambiar la ruta (path) de los archivos y obtener así información que no debe ser accesible.
- **Race conditions:** se producen cuando procesos separados o threads de ejecución dependen de algún estado compartido. Las operaciones con estados compartidos deben incluir mecanismos de sincronización para evitar colisiones entre procesos o threads.
- **Privilege escalation:** permite obtener acceso a recursos que normalmente han sido restringidos para el usuario en cuestión. Generalmente ocurre cuando una aplicación con privilegios elevados tiene una falla que permite asumir dichos permisos.

Conceptos

Revelación responsable (responsible disclosure)

Se refiere a los procedimientos por los cuales se revela una vulnerabilidad para que sea parchada o solucionada. Hay distintas políticas, pero en general se cumplen los siguientes pasos:

- El investigador que descubre una vulnerabilidad informa en forma confidencial al proveedor (vendor) del software.
- Si el proveedor es receptivo y coopera, el investigador espera a que se publique el arreglo para revelar toda la información, salvo los exploits si existieran.
- Si el porveedor no actúa de forma correcta, el investigador procede con una revelación completa (full disclosure), salvo el exploit.
- En cualquier momento, si se tiene constancia de que circula un exploit, se procede con la revelación de la información sobre la vulterabilidad para proteger a los usuarios.

Vulnerablidades famosas

1. **MS17-010 (Eternal Blue):** uno de los ataques más costosos de la historia. Afecta SMB y WannaCry y Petya se basaron en ella.
2. **CVE-2019-0708 (BlueKeep):** afecta RDP, y permite ejecutar código en forma remota y sin autenticar.
3. **Spectre/Meltdown:** explotan vulnerabilidades críticas en procesadores modernos (mayormente Intel), y permite que un programa robe datos de otros ejecutándose en ese momento.
4. **CVE-2014-0160 (Heartbleed):** afecta la implementación OpenSSL de la extensión TLS Heartbeat, y se basa en una inadecuada validación de la entrada (input validation).
5. **CVE-2014-6271 (Shellshock):** afecta el shell bash y permite tomar el control completo de sistemas Linux, Unix, Mac OS X.

Bases de Datos de Vulnerabilidades

- **Common Vulnerabilities and Exposures (CVE):** `https://cve.mitre.org/`
- **National Vulnerability Database (NVD):** `https://nvd.nist.gov/`
- **Security Focus BUGTRAQ:** `https://www.securityfocus.com/bid`
- **Exploits Data Base (EDB):** `https://www.exploit-db.com/`
- **VulDB:** `https://vuldb.com/`
- **0DAY Today:** `https://0day.today/`
- **Computer Incident Response Center Luxembourg (CIRCL):** `https://cve.circl.lu/`

Más información

- **Tenouk**. *Buffer Overflow Tutorial*. `http://www.tenouk.com/Bufferoverflowc/Bufferoverflow1.html`
- **SKOUDIS, Ed - LISTON, Tom.** *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Prentice Hall. 2005. Capítulo 5.
- **Wikipedia**. *Vulnerability*. `http://en.wikipedia.org/wiki/Vulnerability_(computing)`