Ethical Hacker : sesión 2

- Ethical Hacker : sesión 2

clase

- ASPEN
  - Modulo 06 - System Hacking
  - Modulo 07 - Malware
  - Modulo 08 - Sniffing

Modulo 06, apuntes

Modulo 06 - System Hacking

sección 1

- hash
  - linux con salt
    - `tail -n 1 /etc/shadow | cut -f2 -d: | tr «$» «\n»`
      - 3 campos: algoritmo usado, salt, hash contraseña
  - windows sin salt
    - fichero binario
    - tablas rainbow → precalculado hash para diferentes combinaciones de caracteres
    - pwdump7
    - https://gchq.github.io/CyberChef/
- https://password.kaspersky.com/es/ ← ojo con la información compartida
- Microsoft: NTLM Authentication
  - hash contraseña cifra un texto aleatorio enviado por el servidor.
  - servidor recibe y descifra con el hash de la contraseña que tiene almacenada y si el texto es el mismo, todo OK
- Microsoft: Kerberos Auth
  - maquinas, usuarios, aplicaciones → perro Kerberos de 3 cabezas
  - Autenticar (método anterior) usuario (AS - Authentication Server)
  - generador de tiquets (TGS - Ticket Granting Server)
    - duración limitada
    - solicitado para acceso a servicios...
- Password craking
  - ataques no electrónicos
  - ataques online activos
  - ataques online pasivos (escuchas)
  - ataques offline (rainbow...)
- Ataques online activos
  - https://www.hivesystems.com/blog/are-your-passwords-in-the-green (tiempo en reventar pass)
  - diccionario: trabajo previo de recabar información, lista de palabras
    - https://blog.segu-info.com.ar/2024/07/rockyou2024-10-mil-millones-de.html (contraseñas filtradas)
      - https://github.com/RickdeJager/stegseek
  - fuerza bruta
  - por reglas
  - pregunta de seguridad

- Envenenamiento LLMNR (DNS) /NBT-NS (NETBIOS) (Windows)
  - solución: deshabilitar
- Ataques a Kerberos
  - AS-REP
  - Kerberoasting (Cracking TGS)
  - Pass the ticket attack
  - NTLM Relay
- SSH Brute force con shellgpt
- Spray de passwords
  - después de obtener un listado de passwords, atacar con contraseñas habituales para tener un pie dentro
- Password-cracking tools:
  - l0phtCrack
  - THC-Hydra
- EXAM: tener claro el caso de uso de las herramientas de la documentación
- EXTRA: UNICODE Linux: CRT+SHIFT u, XXXX
  - https://unicodeplus.com/
- Windows `systeminfo`
  - python wes systeminfo.txt
- Metasploit Framework (MSF)
  - muy modular
  - interfaces: msf* (casi todas)
  - Modulos:
    - Exploit: base para crear uno
    - Payload: comunicación
    - Auxiliary
    - NOPS: instrucciones que no hacen nada (overflow)
    - Encoder: codificar para evitar detección
    - Evasion: modificar características para no ser detectado
    - Post-exploitation: interactuar maquina comprometida
- Nebula
- DeepExploit

- Buffer Overflow
  - malloc - asignación memoria dinámica en C
    - C y Rust
  - Stack (pila) - LiFo
    - registro EIP - dirección de retorno, cambiar para ejecutar codigo malicioso
    - error de segmentation fault
  - Heap (montón) - FiFo
    - error malloc(): corrupted top size
- `readerlf –headers /usr/sbin/sshd` ← leer formato ELF
- `xxd`: volcado HEX fichero
- Windows Buffer Overflow Explotation
  - Perform Spiking: paquetes TCP/UDP manipulados para detectar aplicaciones o servidores
  - Perform Fuzzing: gran cantidad de datos aleatorios. Averiguar los bytes requeridos para ajustar la modificación del EIP
  - Identificar Offset
    - se cargan en zonas aleatorias de memoria para evitar que esten «localizables» (incluso lo mueven cada x minutos)
  - Identify bad characters
  - Identificar el módulo adecuado (modulos no protegidos)
- ROP attack
- Mecanismos de seguridad ASLR / DEP
  - ASLR: cargar en zonas de memoria aleatoria
  - DEP: prevención de ejecución de datos (declarado como datos y no como ejecutable)

    - JIT Spraying
- Bloodhound: mapea un AD, relación de recursos de un AD

sección 2: escalada de privilegios

- si no se especifica el path completo de la libreria, se puede colocar una maligna en un directorio con prioridad de path
- Spectre / Meltdown: ejecución especulativa: calcula posibles respuestas para adelantarse a la respuesta «humana»
    - malignamente se puede mirar esas respuestas almacenadas temporalmente para obtener información, se puede leer desde cualquier hilo
    - `spectre-meltdown-checker.sh` → https://github.com/speed47/spectre-meltdown-checker
- pipe
    - `mkfifo`
- pivoting and relaying, movimiento lateral
- UAC = User Account Control
- Abusar de Boot o Logon al inicializar
- `curl ipconfig.io`
- ADCS: gestor de claves y certificados en AD

sección 3: ocultar huellas

- pentesting: documentar todo, dentro del ámbito contratado, no se oculta nada.
- programas maliciosos: ...
    - keylogger
    - spyware:
        - avast antivirus free tenía spyware - recopilatorio de información
        - norton grauito (avisando): minado de cripto
- rootkits
    - reinstalar BIOS, reinstalar OS
- NTFS Data Stream (o Alternate Data Stream)
    - `notepad myfile.txt:otros-datos.txt` ← `dir /R`
    - en linux la partición ha de estar montada con ()
    - `streamdetector`
- Esteganografia: es la práctica de ocultar información dentro de otro mensaje u objeto físico para evitar su detección
    - `snow`
    - EXAM: métodos de detección
- Sticky Keys:
    - cinco pulsaciones shift
    - sustituir el ejecutable para colocar otra cosa e invocarlo así
- Ejecución remota
    - DPAPI: protección API
    - `krptgt`
    - Ataque llave maestra (skeleton key attack)
    - Golden ticket attack (cualqier ticket)
    - Silver ticket attack (para usuario concreto)
    - ..
    - WMI
- Linux, comandos

sección 04: ocultar

- auditpol: cambio auditorias
- borrar logs
    - manual o script
    - instalar o desinstalar en windows tiene más privilegios que un admin
        - utiliza ADS (alternate data stream) para guardar desde donde lo he descargado
- Registro Windows MRU (Most Recently Used)
- `history`

Modulo 7: malware

sección 1

- troyanos
- virus
- ransomware
- gusanos

sección 2: fileless malware

- vivir de lo que ha encontrado en la máquina víctima (- Living-off-the-hand)
- persistencia:
- taxonomia:
    - hardware - sin actividad a nivel de fichero
    - ejecución / inyección - usa ficheros
    - exploit
- APUNTES FERNANDO, sección FILELESS

sección 3: AI-based malware

- FakeGPT
- WormGPT
- FraudGPT

sección 4: Analisis malware

- estático: analizar código
- dinámico: en máquina virtual (sandbox)
- testbed (9 pasos)
    - https://www.hackplayers.com/2020/04/listado-de-sandboxes-de-analisis-de-malware.html - Listado de sandboxes de análisis de malware gratuitos y online
    - https://github.com/kevoreilly/CAPEv2 - CAPEv2, es un derivado de Cuckoo Sandbox (actualmente abandonado). Es un script que se instala en una MV Ubuntu 20.04 LTS..
    - https://github.com/mandiant/flare-vm - Flare-VM, parecido a lo anterior, pero en Windows
- `string <file>`
- ofuscación
    - **PEid**: indica de que tipo es (windows)
    - **file** para Linux
- Portable Executables
    - compendio de todos los ficheros necesarios para ejecutar en cualquier máquina sin instalar
- Dependencias
- desensamblar

- ejecutables ELF
  - `readelf`
- ejecutables Match-0 (mac)
- Analizar MS Office (como contenedor de otros archivos)
- PDF
  - incrustar distro Linux
  - Doom (javascript)
- Dangerzone
  - https://dangerzone.rocks/
  - 2 contenedores, uno ejecuta, el otro lee por OCR

sección 05: contramedidas

- https://www.elespanol.com/omicrono/software/20170101/ejecutar-programas-viejos-windows/182732154_0.html - Ejecutar un programa en Windows con una versión anterior del mismo
- https://www.adslzone.net/esenciales/windows-10/ejecutar-programas-antiguos/ - ejecutar programas antiguos
- https://www.hackplayers.com/2024/08/windows-downdate-downgrade.html - Windows Downdate: desactualiza tu Windows, y reporta que está actualizado.
- https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-linux - Microsoft Defender ATP for Linux

Modulo 8: sniffing

- hub reparte entre todos los puertos, los switch no ← problema para el modo promíscuo
- switch SPAN Port (modo promíscuo)

sección 2

- MAC: 3 primeros fabricante, 3 siguientes
- http://standards-oui.ieee.org/oui/oui.txt - Listado de fabricantes y sus MACs asociadas
- ARP:
  - broadcast, no sale a internet, solo LAN, solo IPv4
    - en IPv6 es ND, integrado en ICMP → https://es.wikipedia.org/wiki/Neighbor_Discovery - Neighbor Discovery (ND) protocolo de IPv6, equivalente al protocolo Address Resolution Protocol (ARP) en IPv4. Está integrado en ICMPv6.
- tabla CAM
  - si se llena la tabla, no se reparte tráfico
  - saturar para cambiar a modo HUB → `macof`
- Switch Port Stealing
  - hacer creer que la máquina ha cambiado de puerto, recibir el tráfico y redirigir a la original
- DHCP Starvation Attack
  - hambruna
  - DoS
- Rogue DHCP Server Attack
- ARP Spoofing attack
- Capsa Portable Network Analyzer
- IRDP Spoofing
- VLAN Hopping
  - ver todas las VLAN
- STP Attack
- DNS Poisoning
  - punto débil de internet

    - https://blog.cloudflare.com/es-es/oblivious-dns/
- Detección
    - modo promíscuo
    - nmap detecta (script)

Examen

- udemy test
- examtopics (pago)
- ProxMox