VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

43

Excel@FIT 2016

Automatizácia Man in the Middle útoku pre SSL/TLS Dešifráciu

Marek Marušic
xmarus05.stud.fit.vutbr.cz

Úvod a motivácia

- Vykonať MitM útok pre dešifráciu SSL/TLS pripojení je náročné
  - Nutnosť spúšťať mnoho nástrojov
  - Nutnosť naštudovať s akými parametrami nástroje spúšťať
  - Dostupné nástroje neponúkajú kompletné riešenie
- MitM sonda zjednodušuje MitM útok
  - Stačí zapojiť do sieťe a spusťit útok
  - Automaticky sa nakonfiguruje a spustia sa všetky potrebné nástroje
  - Používateľ nepotrebuje žiadne znalosti o použitých nástrojoch v pozadí

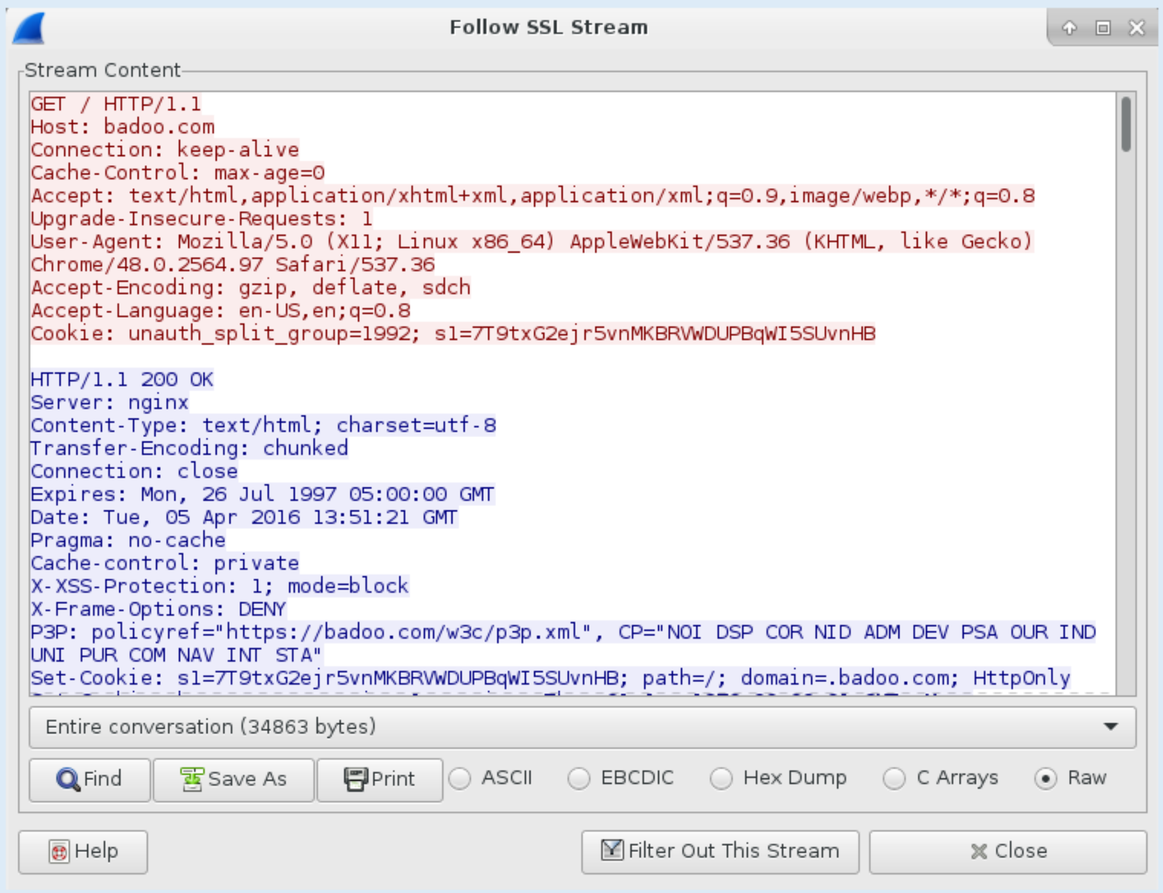
MitM sonda

- Jednoduché spustenie
- Výstup do pcap formátu (najpoužívanejší v sieťovej analýze)
- IPv4
- IPv6
- Dešifrácia Diffie-Hellman šifier pomocou získaných kľúčov SSL/TLS relácií
- Možnosť pracovať ako transaprentné proxy

V budúcnosti by mala sonda tiež poskytnúť:

- Grafické užívateľské prostredie
- Prekonanie HTTP Strict Transport Security
- JavaScript Keylogger

Získané dešifrované pakety zobrazené vo Wireshark



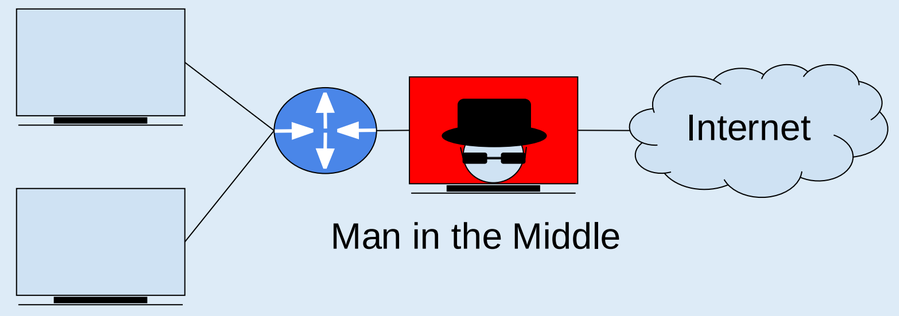
Tieto dešifrované dáta je možné použiť pre analýzu chovania používateľa v sieti a pre získanie jeho údajov.

Porovnanie s voľne dostupnými nástrojmi

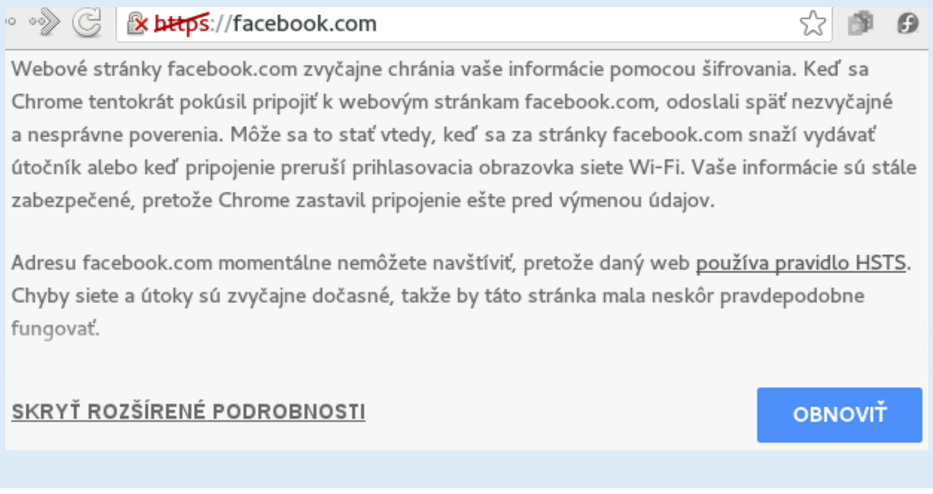
	SSLsplit	Mitmproxy	MITMf	Bettercap	**Naša Sonda**
IPv4	✓	✓	✓	✓	✓
IPv6	✓	✗	✓	✓	✓
ukladanie kľúčov relácií	✗	✓	✗	✗	✓
HSTS prekonanie	✗	✗	✓	✓	✗*
SSLsplitting	✓	✓	✗	✗	✓
SSLstripping	✗	✗	✓	✓	✗*
Arpspoof	✗	✗	✓	✓	✓
Transparentné proxy	✗	✗	✗	✗	✓
CA certifikáty	✗	✓	✗	✗	✓
Pcap výstup	✗	✗	✗	✓	✓
Auto presmerovanie	✗	✗	✓	✓	✓

(* v búducnosti bude taktiež naimplementované)

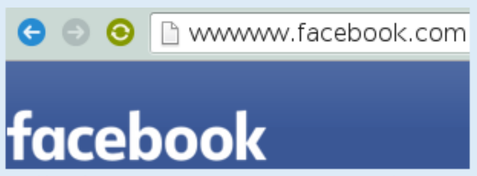
Zapojenie sondy ako transparentné proxy.



HSTS varovanie pocas MitM útoku



Prekonanie HSTS na Facebook



Prekonať HSTS je možné pomocou zmeny domenového mena, špeciálneho DNS servera a odstránením HTTPS šifrácie

Ukážka súboru so získanými kľúčmi SSL/TLS relácií.

```
CLIENT_RANDOM 86AC6E9A658C87C8058B873D2D8B9A9A5D1952F81FEA69B10A2FB036793E6EEC 06AF36EC2AD0BF56C378511D6FC585185DFC578
CLIENT_RANDOM BDE6984C9FCA187A8D853093A20B3E88AD3AB37090D236F300C2787A65A8220B E16301E5F4802F1FC07E61E96F59443ED41C81C
CLIENT_RANDOM 99F7A70D64A82A2D028B802F87AE0026696DE8B6344CCB8FCC6A5412978113C6 8C7B90A665298D27144A06A2880002B2436FA58
```

Táto funkcionalita je doimplementovaná v MitM Sonde. Kľúče slúžia pre dešifráciu zachytených paketov. Ponúkajú možnosť dešifrovať aj šifrovacie sady s Diffie-Hellman výmenou kľúčov.