



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ

DEPARTMENT OF INFORMATION SYSTEMS

ODCHYCENÍ COOKIES

IBS - ODBORNÁ PRÁCE NA VYBRANÉ TÉMA

AUTOR PRÁCE

PETER HORŇÁK

BRNO 2020

Obsah

1	Popis útoku	2
2	Realizácia útoku	3
3	Zhodnotenie výsledkov	6
	Literatúra	7

Kapitola 1

Popis útoku

HTTP cookies sú používané ako autentifikačné tokeny u väčšiny webových aplikácií, ktoré využívajú prihlasovanie. Cookies umožňujú stránkam spravovať stav stránky v rámci bez stavového protokolu HTTP, keďže prehliadače posielajú cookies ako súčasť hlavičky HTTP požiadavku [2]. Útočník, ktorý získa autentifikačný token v podobe cookie, môže byť schopný to ho zneužiť pre ukradnutie jeho identity na danej stránke. Toto umožní útočníkovi prístup k citlivým informáciám užívateľa stránky a vykonávať akcie v jeho mene.

Spôsob ako čiastočne ochrániť, užívateľov pred odchytením, je využiť protokol HTTPS, ktorý používa šifrovanú komunikáciu a tým pádom zabráňuje odchyteniu cookies pomocou počúvania komunikácie na sieti, ktorému sa táto práca venuje. Ďalším známym útokom je takzvaný cross site scripting útok, pomocou ktorého je možné získať cookies užívateľov. Je možné sa tomuto útoku vyhnúť a to využitím atribútu `HttpOnly` v hlavičke `Set-Cookie`, ktorú odosiela stránka užívateľovi, pri odpovedi na HTTP požiadavku. Tento atribút spôsobí, že daná cookie nie je prístupná pomocou JavaScriptu na stránke a môže sa s ňou manipulovať iba pomocou hlavičiek.

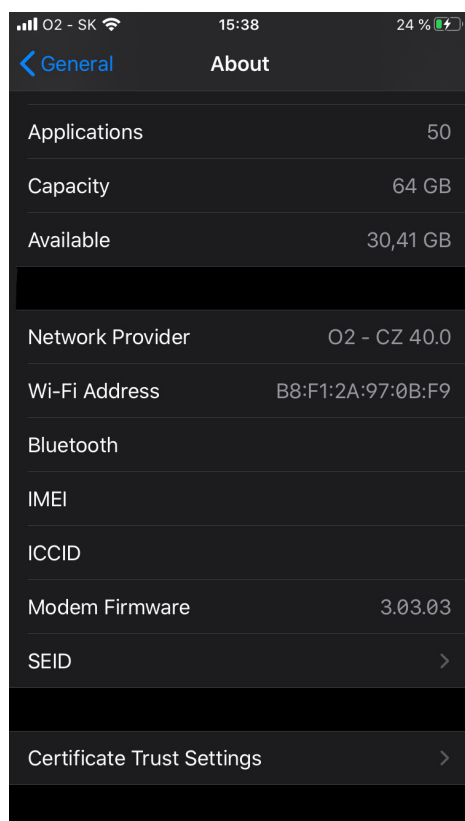
Tento útok sa väčšinou vykonáva na verejných sieťach ako napríklad na sieťach v univerzitnom campuse, kaviarni alebo obchodnom centre [1]. Útočník sa pripojí na vybranú sieť, pričom v prípade, že je zabezpečená musí poznať heslo. Obeť tohto útoku je pripojená na rovnakú sieť pričom bežne prehliada webové stránky. V prípade, že navštívi web, s ktorým komunikuje pomocou protokolu HTTP, útočník, je schopný túto komunikáciu prečítať a poprípade zneužiť.

Kapitola 2

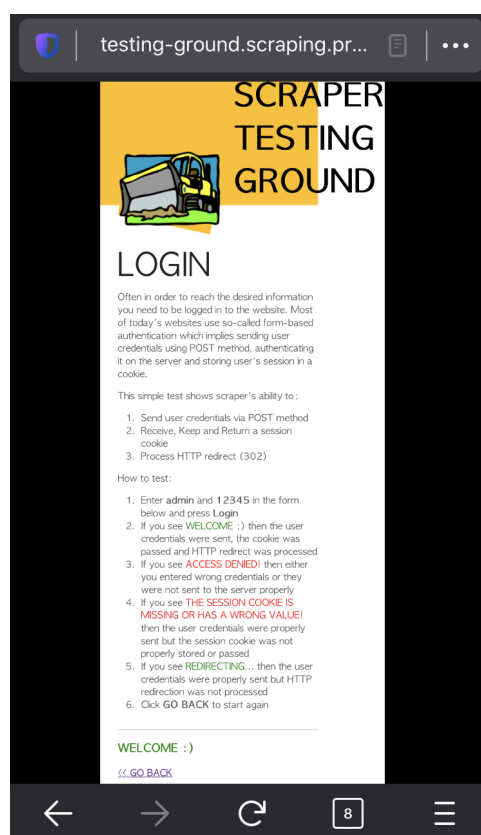
Realizácia útoku

Pre realizáciu útoku som využil zariadenia notebook MacBook Pro a smartphone Iphone 8. Obidve zariadenia boli pripojené na domácu Wi-Fi sieť, pričom notebook počúval komunikáciu na tejto sieti a smartfón bol cieľom útoku.

Pre vykonanie útoku som si zvolil webovú aplikáciu, ktorá komunikuje pomocou protokolu HTTP na adrese <http://testing-ground.scraping.pro> viď. 2.2. Táto webová aplikácia poskytuje pred pripravený účet s prihlasovacím menom 'admin' a heslom '12345', kde sa po prihlásení nastaví cookie s rovnakým menom a rovnakou hodnotou, avšak pre demonštráciu ako útok funguje to je dostačujúce.



Obr. 2.1: MAC adresa zariadenia cieľového zariadenia



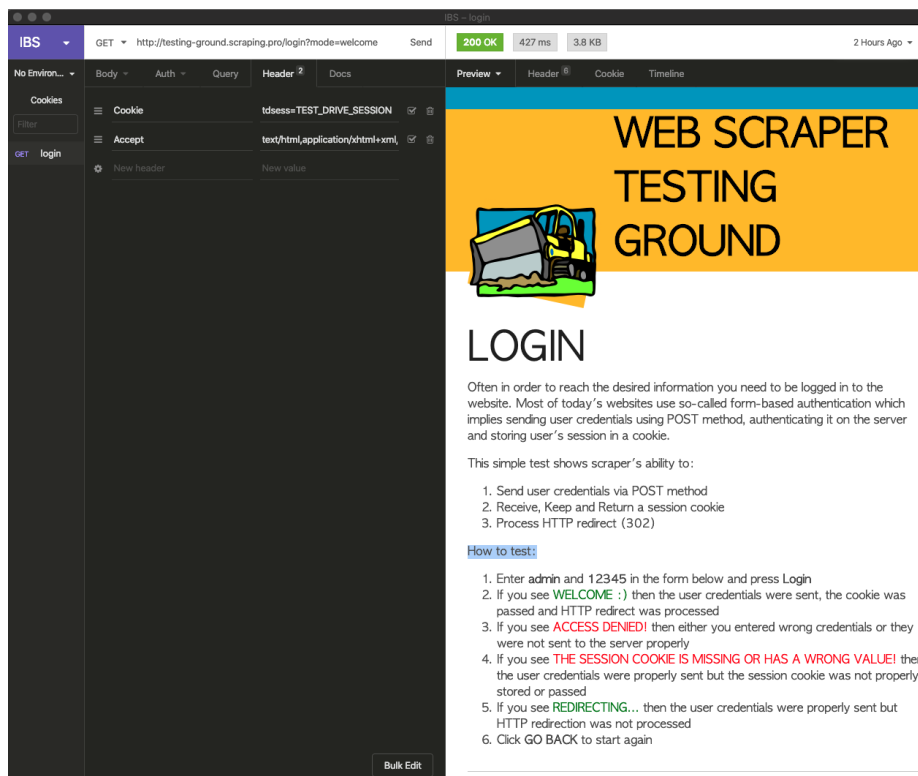
Obr. 2.2: Prihlásenie na web

Výber zariadenia na ktorom beží operačný systém macOS Catalina bol žiaľ trochu nešťastný a to z dôvodu toho, že monitor mód, ktorý je potrebný pre počúvanie komunikácie na celej sieti, je nefunkčný v nástroji Wireshark¹ a rovnako aj pri použití nástroja tcpdump. Preto bolo potrebné využiť vstavaný nástroj Wireless Diagnostics, kde je možné použiť sniffer, pre počúvanie siete v monitor móde, ktorého výstupom je súbor typu pcap. Tento súbor som následne analyzoval pomocou nástroja Wireshark.

Pre správne analyzovanie súboru je potrebné najprv nastaviť kľúč pre dekryptovanie protokolu IEEE 802.11, v tomto prípade som použil kľúč typu wpa-pwd.

Podmienkou pre úspešne čítanie HTTP požiadavkov, je zachytiť aj 4-cestný TCP handshake, ktorý sa vykonáva na začiatku komunikácie. Pre toto je potrebné počúvať dlhšiu dobu, aby zariadenie zachytilo začiatok komunikácie, kde sa tento handshake nachádza.

Následne som použil filter pre HTTP požiadavky a MAC adresu B8:F1:2A:97:0B:F9 vid' 2.1, ktorý mi vyfiltroval komunikáciu môjho smartfónu. Následne som s HTTP požiadavku typu GET na cestu login vid' 2.4 vyextrahoval hlavičku Cookie, kde sa nachádza cookie s názvom tdsess, ktorej hodnota je token pre prihlasovanie do systému.



Obr. 2.3: Replikovanie prihlasovania pomocou nástroja Insomnia.

Pre dôkaz, že je možné sa prihlásiť pomocou tejto cookie, som poslal HTTP požiadavku typu GET s odpočúvacieho zariadenia na adresu <http://testing-ground.scraping.pro/login?mode=welcome>, ktorá v hlavičke správy obsahovala túto cookie. S obrázku 2.3 je možné vidieť, že táto požiadavka, naozaj umožní útočníkovi sa prihlásiť bez znalosti prihlasovacích údajov.

¹<https://ask.wireshark.org/question/14292/how-to-get-monitor-mode-working-in-mac-os-catalina/?answer=16721#post-id-16721>

Peter's MacBook Pro_ch7.2020-05-31_15.34.21.525.pcap

http and wlan.sa == B8:F1:2A:97:0B:F9 or wlan.da == B8:F1:2A:97:0B:F9

No.	Time	Source	Destination	Protocol	Length	Info
19...	192.168.100.8	46.228.223.185	HTTP	454	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
20...	192.168.100.8	46.228.223.185	HTTP	462	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
21...	192.168.100.8	204.15.135.8	HTTP	585	GET /login HTTP/1.1	
22...	192.168.100.8	46.228.223.185	HTTP	454	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
22...	46.228.223.185	192.168.100.8	OCSP	1065	Response	
31...	192.168.100.8	204.15.135.8	HTTP	171	POST /login?mode=login HTTP/1.1 (application/x-www-form-urlencoded)	
31...	204.15.135.8	192.168.100.8	HTTP	668	[TCP Previous segment not captured] Continuation	
31...	192.168.100.8	204.15.135.8	HTTP	682	GET /login?mode=welcome HTTP/1.1	
31...	204.15.135.8	192.168.100.8	HTTP	594	HTTP/1.1 200 OK (text/html)	
38...	192.168.100.8	46.228.223.185	HTTP	454	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
38...	46.228.223.185	192.168.100.8	OCSP	1065	Response	
40...	192.168.100.8	46.228.223.185	HTTP	460	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
40...	46.228.223.185	192.168.100.8	OCSP	1064	Response	
40...	192.168.100.8	204.15.135.8	HTTP	633	GET / HTTP/1.1	
40...	204.15.135.8	192.168.100.8	HTTP	360	HTTP/1.1 200 OK (text/html)	
43...	192.168.100.8	46.228.223.185	HTTP	454	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
43...	192.168.100.8	204.15.135.8	HTTP	620	GET /login HTTP/1.1	
43...	46.228.223.185	192.168.100.8	OCSP	1065	Response	
43...	204.15.135.8	192.168.100.8	HTTP	773	HTTP/1.1 200 OK (text/html)	
46...	192.168.100.8	46.228.223.185	HTTP	460	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
46...	46.228.223.185	192.168.100.8	OCSP	1065	Response	
46...	192.168.100.8	46.228.223.185	HTTP	454	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFH7maudymrP8%2BKIGZGw	
46...	46.228.223.185	192.168.100.8	OCSP	1065	Response	

Frame 17009: 620 bytes on wire (4960 bits), 620 bytes captured (4960 bits)

- Radiotap Header v0, Length 46
- 802.11 radio information**
- IEEE 802.11 QoS Data, Flags: .p.....TC
- Logical-Link Control
- Internet Protocol Version 4, Src: 192.168.100.8, Dst: 204.15.135.8
- Transmission Control Protocol, Src Port: 60155, Dst Port: 80, Seq: 482, Ack: 1649, Len: 468
- Hypertext Transfer Protocol**
 - GET /login HTTP/1.1\r\n
 Host: testing-ground.scraping.pro\r\n
 Cookie: tdsess=TEST_DRIVE_SESSION\r\n
 Connection: keep-alive\r\n
 Upgrade-Insecure-Requests: 1\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
 User-Agent: Mozilla/5.0 (iPhone; CPU OS 13_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) FxiOS/25.1 Mo
 Referer: http://testing-ground.scraping.pro/\r\n
 Accept-Language: en-us\r\n
 Accept-Encoding: gzip, deflate\r\n
 \r\n
 [Full request URI: http://testing-ground.scraping.pro/login]
 [HTTP request 2/2]
 [Prev request in frame: 15501]
 [Response in frame: 17433]

Frame (620 bytes) Decrypted CCMP data (528 bytes)

HTTP Cookie (http.cookie), 35 bytes Packets: 20936 · Displayed: 100 (0.5%) Profile: Default

Obr. 2.4: GET požiadavka prihlasovania s hlavičkou Cookie, obsahujúcou token pre prihlásenie

Kapitola 3

Zhodnotenie výsledkov

V ukážke je možné vidieť, ako nezabezpečená komunikácia na sieti môže mať fatálne následky pre užívateľa, ktorý sa stane obeťou útoku. Z tohto dôvodu sa odborníci snažia presadiť protokol HTTPS a umožniť jeho jednoduchú integráciu na webové stránky. Napríklad z tohto dôvodu, pri požiadavke na stránku [google.com](https://www.google.com) pomocou protokolu HTTP je užívateľ automaticky presmerovaný na web s protokolom HTTPS. Z tohto dôvodu vznikol atribút **Secure** v **Set-Cookie** hlavičke, ktorý umožňuje správanie aby sa cookie neposielala cez nezabezpečenú komunikáciu.

Táto práca ukazuje, že komunikácia cez nezabezpečenú komunikáciu, umožňuje útočníkovi čítať všetky požiadavky a odpovede poslané cez protokol HTTP. Navyše dokáže tieto informácie zneužiť pomocou cookies a to takým spôsobom, že pri použití správnej cookie sa dokáže autentifikovať ako niekto iný. Niektoré cookies môžu útočníkovi poskytnúť ďalšie informácie ako napríklad históriu vyhľadávania na stránke [1].

Pri vypracovávaní tejto práce som sa zoznámil s nástrojom **sniffer**, ktorý je predinštalovaný v najnovších verziách operačného systému macOS. Tak isto som objavil chybu pri používaní monitor módu na tomto operačnom systéme. Vyskúšal som si dešifrovať komunikáciu cez protokol IEEE 802.11 a rozšíriť obzory v oblasti počítačových sietí a ich bezpečnosti.

Literatúra

- [1] SIVAKORN, S., POLAKIS, I. a KEROMYTIS, A. The Cracked Cookie Jar: HTTP Cookie Hijacking and the Exposure of Private Information. In: Máj 2016, s. 724–742.
- [2] ZHOU, Y. a EVANS, D. Why Aren't HTTP-only Cookies More Widely Deployed? Máj 2010.