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

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 pristúpiť k citilivým 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 zabraňuje 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.

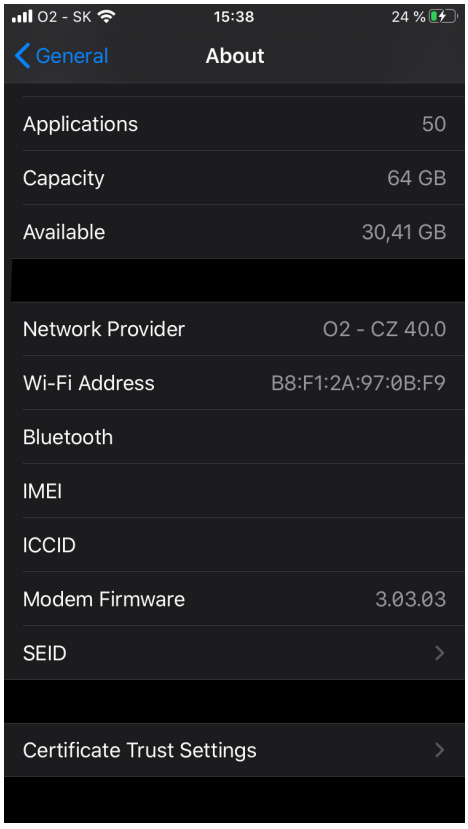
Tento útok sa väčšinou vykonáva na verejných sieťach ako napríklad na sieťach v univerzitnom campuse, kaviarni alebo obchodnom centre [1]. Útočník sa pripojí na vybranú sieť, pričom v prípade, že je zabezpečená musí poznať heslo. Obeť tohto útoku je pripojená na rovnakú sieť pričom bežne prehliada webové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

Kapitola 2

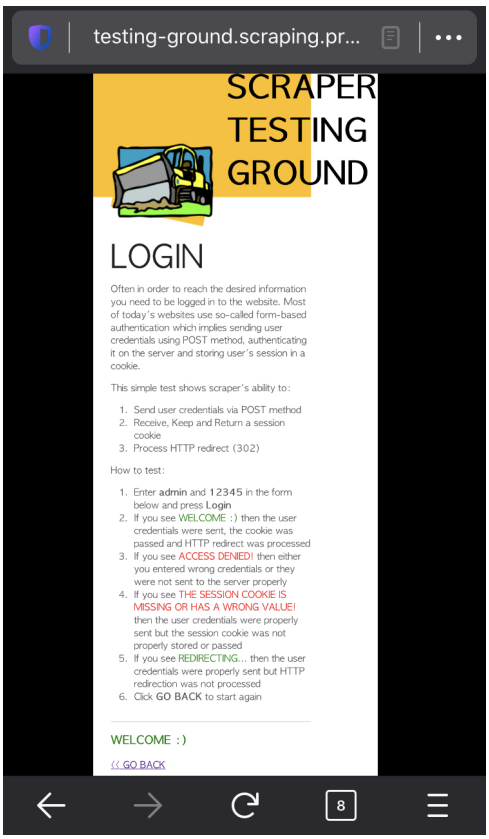
Realizácia útoku

Pre realizáciu útoku som využil zaradenia 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



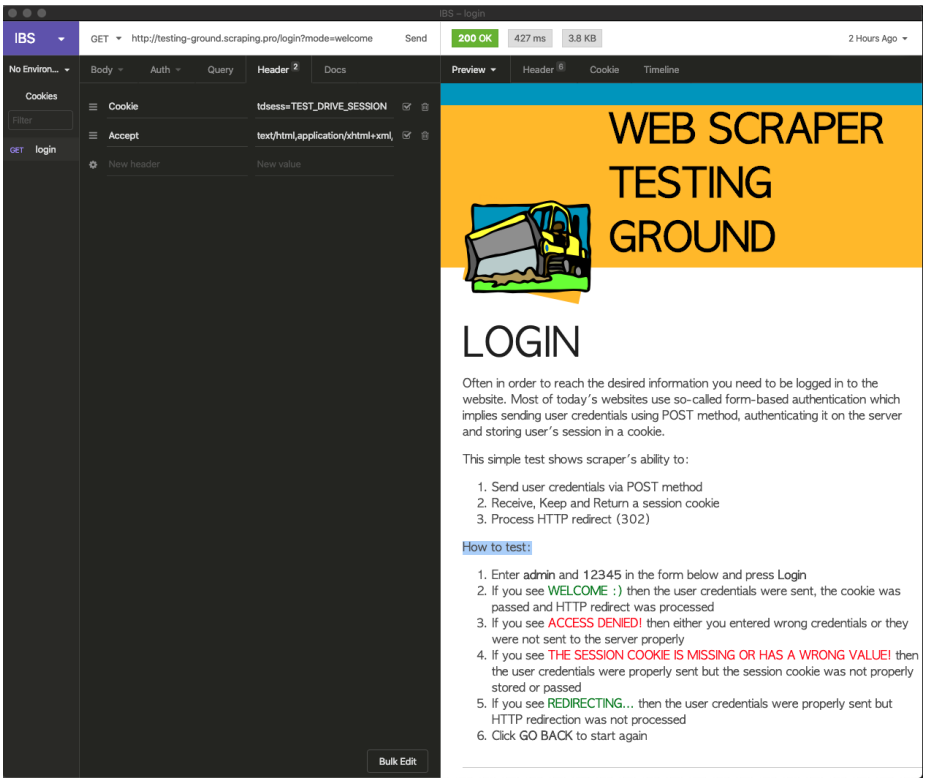
Obr. 2.2: Prihlásenie na web

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 `Wireshark` [1] 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 nástroju `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.

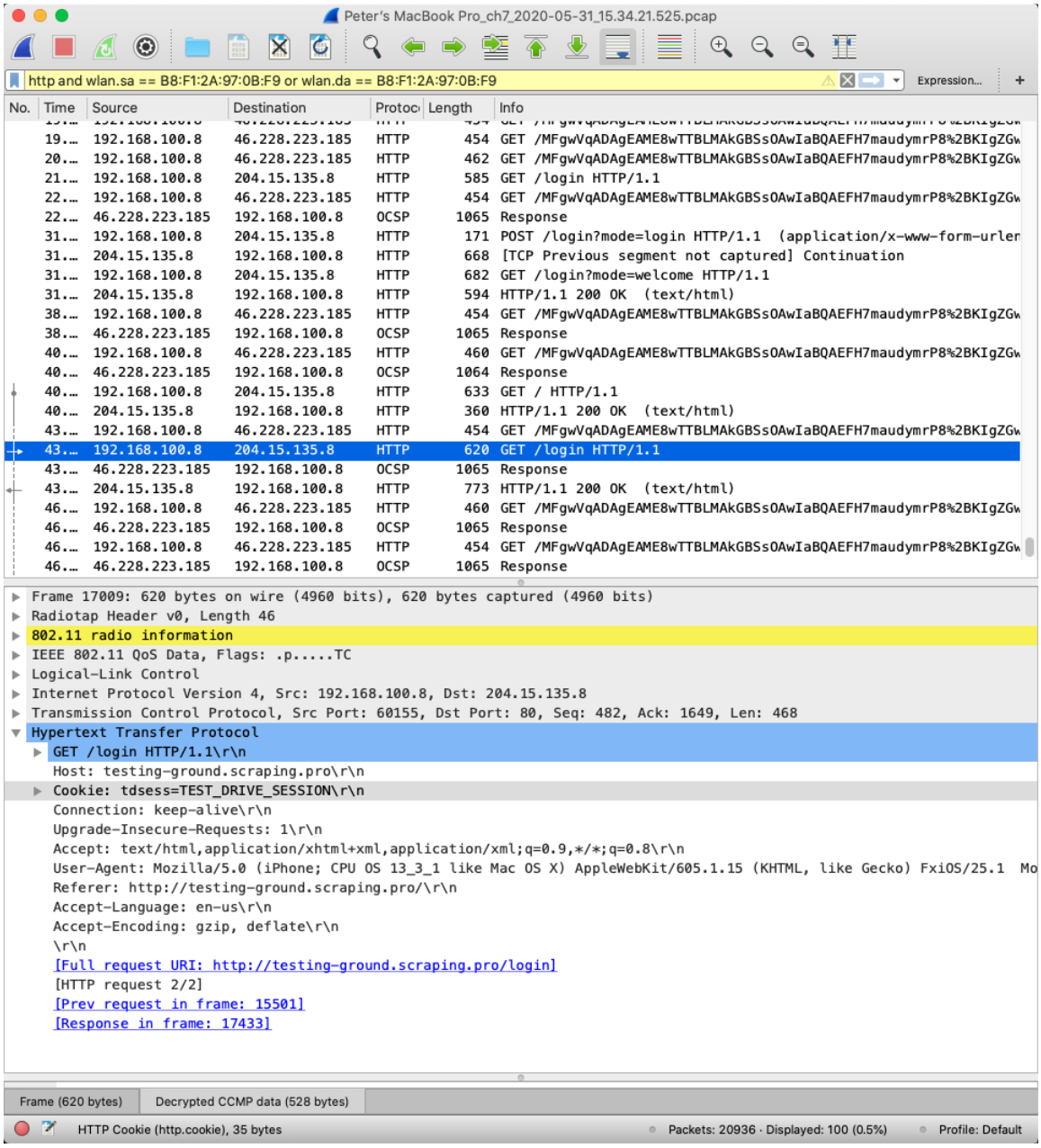
Následne som použil filter pre HTTP požiadavky a MAC adresu B8:F1:2A:97:0B:F9 viď 2.1, ktorý mi vyfiltroval komunikáciu môjho smartfónu. Následne som s HTTP požiadavku typu GET na cestu `login` viď. 2.4 vyextrahoval hlavičku `Cookie`, kde sa nachádza cookie s názvom `tdsess`, ktorej hodnota je token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



Obr. 2.3: Replikovanie prihlasovania pomocou nástroju 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`



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 jednoduché integráciu na webové stránky. Napríklad z tohto dôvodu, pri požiadavke na stránku `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.