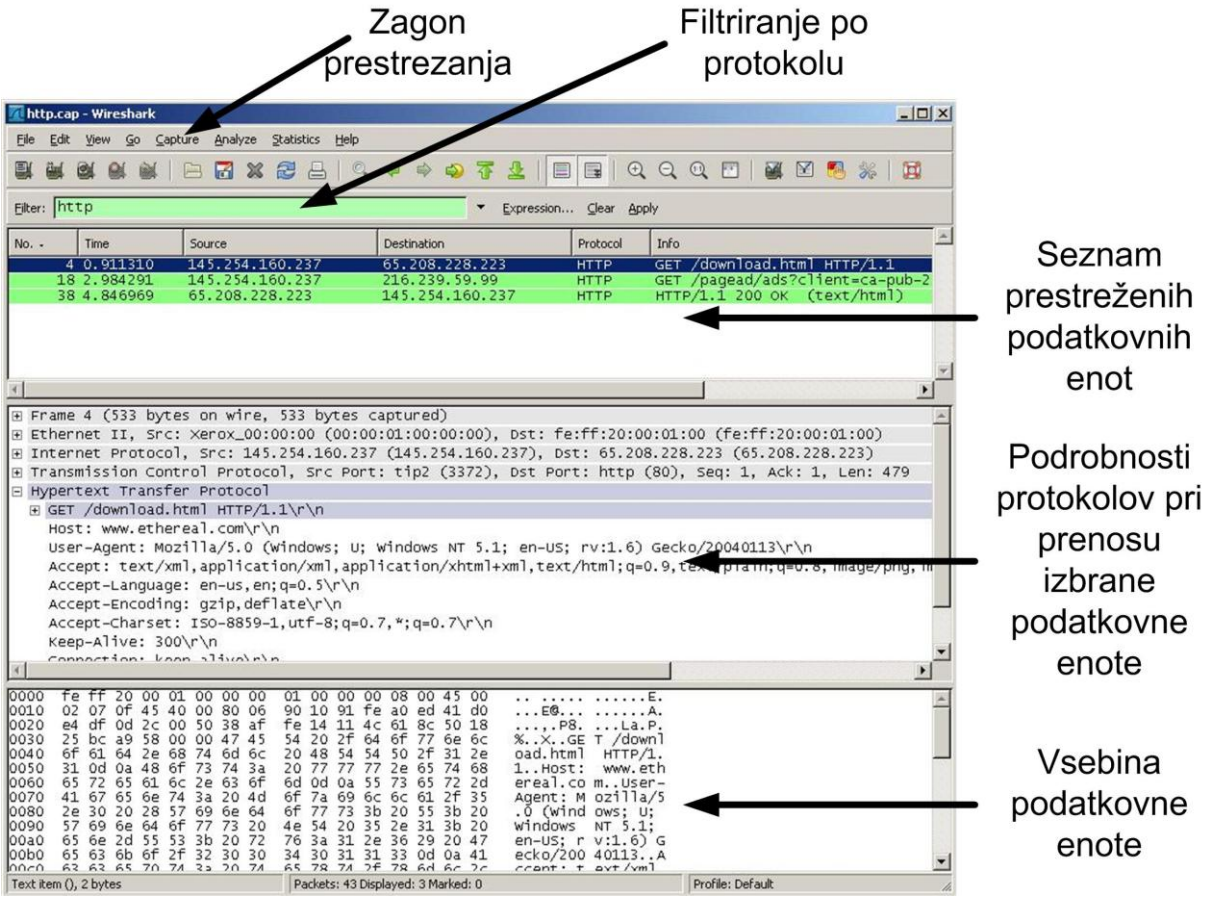
Napad »človeka v sredini« na spletu

1. Uvod

Internet je osnovan na podlagi arhitekture odjemalec - strežnik. Odjemalci so računalniški programi na lokalnih računalnikih, ki komunicirajo s strežniki - računalniškimi programi, ki se nahajajo na oddaljenih računalnikih. Tipični odjemalci na svetovnem spletu so *brskalniki*. Pravila komunikacije med odjemalcem in strežnikom imenujemo protokol. Najpomembnejši protokol svetovnega spleta je protokol HTTP. Komunikacija med brskalnikom in strežnikom navadno poteka kot zaporedje zahtev odjemalca in odgovorov strežnika.



Slika 1: Analizator mrežnih protokolov Wireshark

2. *Namestitev in uporaba analizatorja mrežnih protokolov Wireshark*

1. S spletne strani http://www.wireshark.org/ prenesite in namestite mrežni analizator Wireshark.
2. Pred začetkom prestrezanja morate izbrati omrežni vmesnik, na katerem želite izvajati prestrezanje. To storite v **Capture/Interfaces.** Za začetek prestrezanja izberite **Start** poleg izbranega vmesnika.
3. Prestrezanje zaključite s **Capture/Stop.**

3. *Komunikacija po protokolu HTTP*

1. Zaženite spletni brskalnik in počistite zasebne podatke (zgodovino, piškotke itd.).
2. Z mrežnim analizatorjem Wireshark začnite snemati sled na omrežnem vmesniku Ethernet. Takoj nato v spletnem brskalniku odprite poljubno spletno stran. Ko se stran naloži, zaključite snemanje.
3. Filtrirajte posneto sled po protokolu HTTP.
4. Ugotovite kateri IP naslov ustreza vašemu računalniku in je kateri naslov strežnika, ki vam je posredoval spletno stran.
5. Viri, ki jih je spletni strežnik poslal vašemu brskalniku, so označeni kot HTTP/1.1 200 OK (*vrsta dokumenta*). Izmed vseh virov, ki jih je spletni strežnik posredoval vašemu računalniku, izberite prvega, ki se nanaša na HTML dokument (*text/html*) (Slika 2).
6. Z desnim miškinim gumbom kliknite na »line-based text data« v srednjem oknu in izberite Copy/Bytes/Printable Text Only.
7. Kopiran tekst shranite v nov HTML dokument in ga odprite z brskalnikom.

HTTP povezava ni zavarovana. Vsakdo, ki ima možnost prestreči promet med vašim računalnikom in spletnimi strežniki, ima vpogled v vsebino komunikacije.

Filter: http | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Length	Info
1092	8.044150	192.168.1.103	94.103.65.2	HTTP	653	GET / HTTP/1.1
1137	8.200853	94.103.65.2	192.168.1.103	HTTP	1185	HTTP/1.1 200 OK (text/html)
1149	8.248023	192.168.1.103	94.103.65.2	HTTP	768	GET /delivery/spc.php?zones=zone_44%3
1152	8.248851	192.168.1.103	94.103.65.4	HTTP	721	GET /_up/upload/2011/04/13/64780857_1
1179	8.283222	94.103.65.2	192.168.1.103	HTTP	1263	HTTP/1.1 200 OK (application/x-javas
1182	8.323837	94.103.65.4	192.168.1.103	HTTP	221	HTTP/1.1 200 OK (JPEG JFIF image)
1184	8.334470	192.168.1.103	94.103.65.4	HTTP	753	GET /_up/upload/2011/11/28/64839354_i
1187	8.356588	94.103.65.4	192.168.1.103	HTTP	212	HTTP/1.1 304 Not Modified
1191	8.359295	192.168.1.103	94.103.65.4	HTTP	774	GET /_up/upload/2011/11/28/64839232_a
1197	8.375001	192.168.1.103	94.103.65.4	HTTP	756	GET /_up/upload/2011/11/28/64839229_c
1199	8.379338	94.103.65.4	192.168.1.103	HTTP	212	HTTP/1.1 304 Not Modified
1203	8.404318	94.103.65.4	192.168.1.103	HTTP	212	HTTP/1.1 304 Not Modified
1215	8.457136	192.168.1.103	94.103.65.2	HTTP	796	GET /delivery/lg.php?bannerid=1174&ca
1217	8.469250	192.168.1.103	94.103.65.2	HTTP	683	GET /_up/vreme_2009.png?t=4408335 HTT
1224	8.503741	94.103.65.2	192.168.1.103	HTTP	480	HTTP/1.1 200 OK (GIF89a)
1228	8.519260	192.168.1.103	94.103.65.4	HTTP	688	GET /modules/content/blog/img/blog.jp
1229	8.520877	192.168.1.103	94.103.65.4	HTTP	714	GET /_up/photos/2011/11/28/u66728-187
1237	8.548959	192.168.1.103	94.103.65.4	HTTP	753	GET /_up/upload/2011/11/28/64839354_i
1254	8.582391	94.103.65.4	192.168.1.103	HTTP	212	HTTP/1.1 304 Not Modified
1262	8.585352	94.103.65.4	192.168.1.103	HTTP	472	HTTP/1.1 200 OK (JPEG JFIF image)
1274	8.603332	94.103.65.4	192.168.1.103	HTTP	1412	HTTP/1.1 200 OK (JPEG JFIF image)
1306	8.706574	94.103.65.2	192.168.1.103	HTTP	1022	HTTP/1.1 200 OK (PNG)

Slika 2. Filtriranje HTTP paketov iz prestreženega prometa.

4. *Napad »človeka v sredini« na spletne piškotke*

Piškotek (*ang. cookie*) je zbirka podatkov o stanju komunikacije med odjemalcem in strežnikom, ki gosti neko spletno mesto. Informacije o stanju lahko obsegajo uporabnikovo avtentikacijo, stanje uporabniške seje, uporabniške nastavitve itd. Prestrezanje in kraja piškotkov je občutljiv varnostni problem na spletu, saj lahko napadalec na ta način ogrozi zasebnost spletnega uporabnika.

Scenarij: Eva[1] s svojim prenosnim računalnikom s posebno brezžično mrežno kartico spremlja in si beleži promet v vašem brezžičnem omrežju. Medtem se prijavite v svoj Facebook račun. Eva prestreže avtentikacijske podatke, shranjene v piškotku, ki ga vaš brskalnik pošlje spletnemu strežniku, ki gosti storitev Facebook. Medtem ko uporabljate Facebook-ove storitve se Eva z uporabo prestreženega piškotka prijavi v vaš račun. Na vašem profilu najde občutljive osebne podatke, ki jih uporabi, da bi vam škodovala. Poleg tega spremeni geslo računa, tako da lahko nemoteno sama uporablja vaš račun in se predstavlja v vašem imenu.

[1] Eva (ang. *Eve*) je dogovorjeno ime, ki se uporablja v opisih scenarijev komunikacijske varnosti. Eva je v angleščini okrajšava za »eavesdropper«, kar pomeni »prisluškovalec«.

V okviru vaje boste svojo prijavo na Facebook prestregli sami. Nato se boste s prestreženimi avtentikacijskimi podatki prijavili v vaš račun na drugemu računalniku ali brskalniku.

1. Zaženite brskalnik Mozilla Firefox in namestite dodatek »Greasemonkey«
2. Na mestu http://dustint.com/code/cookieinjector.user.js dobite skripto, ki jo uvozite v »Greasemonkey«.

---

3. Odprite drug spletni brskalnik (Internet Explorer ali Google Chrome) in počistite zasebne podatke (zgodovino, piškotke itd.).
4. Z mrežnim analizatorjem Wireshark začnite snemati sled na omrežnem vmesniku Ethernet. Takoj nato se v spletnem brskalniku prijavite na Facebook. Ko se stran naloži, zaključite snemanje. Ostanite prijavljeni v svoj račun.
5. Filtrirajte posneto sled z uporabo filtra **http.cookie contains "datr"**
6. V prikazanih paketih poiščite piškotke in preiščite njihovo vsebino.
7. Izberite enega izmed piškotkov, ki vsebuje podatek »c_user«.
8. Z uporabo Copy/Bytes/Printable Text Only kopirajte celotno tekstovno vsebino piškotka.

---

9. Odprite Facebook-ovo spletno stran v brskalniku Mozilla Firefox.
10. Pritisnite **Alt-C** in v okno, ki se prikaže, prilepite vsebino piškotka.
11. Osvežite stran.

Kot smo ugotovili, je bilo napad razmeroma preprosto izvesti, zato vedno, ko se prijavljate v spletne storitve, kot so Gmail, Facebook itd., uporabljajte protokol HTTPS!

12. V svojem Facebook računu izberite Account Settings / Security / Secure Browsing
13. Izberite »Browse Facebook on a secure connection (HTTPS) when possible«
14. Ponovite točke 3 – 8.