Pentesting Thick Client Applications

@0xhexninja

PS C:\> whoami

- Anurag Srivastava
- Job involves red teaming and sometimes application penetration testing :p
- Author of buffer overflow based exploit which is now part of rapid7's Metasploit framework – (CVE-2017-13696)
- Remote buffer overflow in All Media Server – (CVE-2017-17932) [msf module]
- I like to pwn AD, evade/bypass AV/EDRs
- Ctf player at hackthebox
- Worked on threat intel, OSINT, reverse engineering, basic malware analysis & investigation
- Also holds some industry recognized certifications like OSCE, OSCP, OSWP, eCPTX, CRTE, CRTP, CREST CRT, CPSA and few more.
- One day, I will be a Red Teamer and I never go back on my words! – Naruto Lover <3
- I blog at - https://www.theanuragsrivastava.in/
- Social media- hexachordanu

Agenda

- Introduction
- Why did I choose this topic?
- Common Architecture
- Testing Thick Client
- Common Vulnerabilities
- Ninja Tools that you need
- Quick Demo
- Common Challenges
- Possible Solutions to our common challenges
- Basic Checklist
- Playground
- Interesting Reads
- References

Thick Client Pentesting ?

- Finding right place to inject our payload
- Reading the sensitive data
- Uncovering the truth behind the fancy UI by decompiling and reversing
- Fuzzing the application
- Checking the signature and integrity of the app
- Testing for vulnerabilities in client's wallet, data storage and data processing mechanism

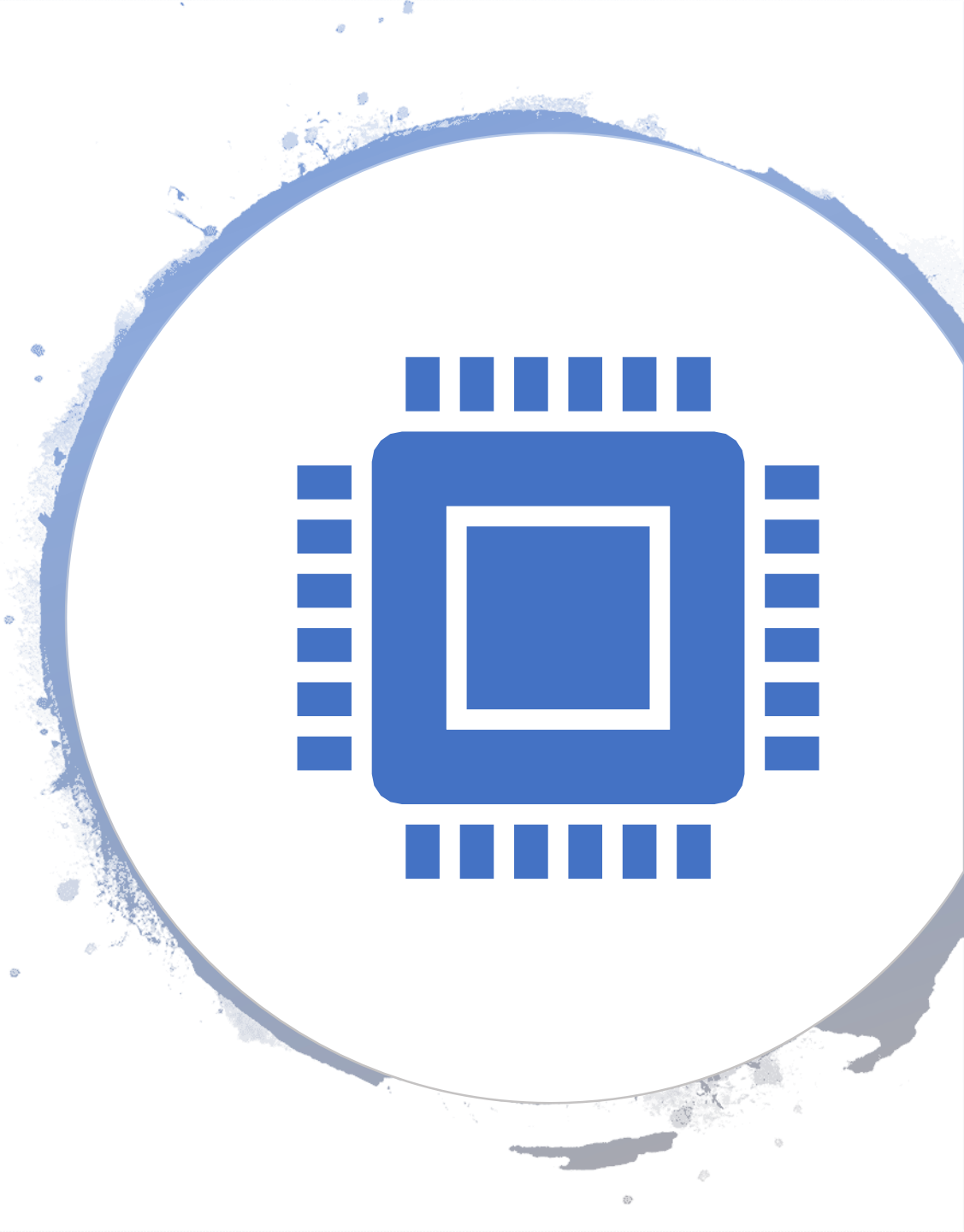
Image source: https://c8.alamy.com

Introduction

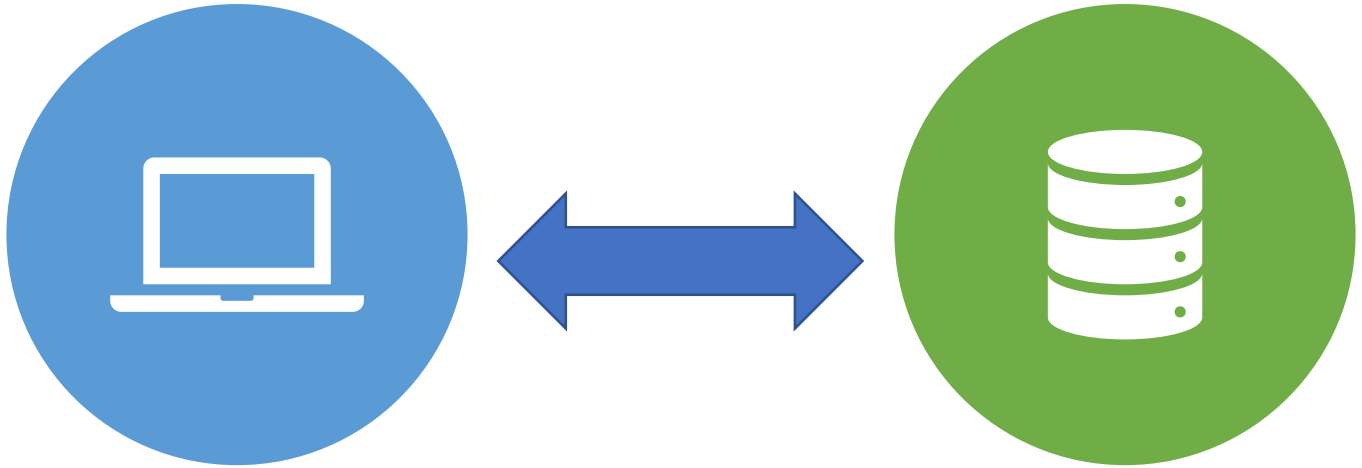
- According to Wikipedia, a fat client/heavy client/rich client/thick client is a computer (client) in client–server architecture or networks that typically provides rich functionality independent of the central server".
- Thick client applications can be developed using various programming languages such as:
  - .Net
  - Java
  - C/C++
  - Microsoft Silverlight
- Example – Skype, Teams, Outlook etc.

Why did I choose this topic?

- Commonly seen that enterprises use thick client for internal purpose
- Organizations mostly focus on web and mobile apps pentesting
- Wider scope
- Less resources on thick client security testing
- Automated Vulnerability assessment is not enough



Common Architecture (Two-tier)



DESKTOP CLIENT

DATABASE

Common Architecture (Three-tier)

DESKTOP CLIENT APPLICATION SERVER DATABASE

Testing Thick Clients

Information Gathering

- **Application Architecture**
  - Business Logic
- **Platform Mapping**
  - Understanding Application & Infrastructure
- **Languages and Frameworks**
  - Common Vulnerabilities

Client Side attacks

- **Files Analysis**
  - Sensitive Information
- **Binary Analysis**
  - Static Analysis (De-compilation)
  - Dynamic Analysis (Run-Time Reverse Engineering)
- **Memory Analysis**
  - Memory Manipulation
  - Sensitive information stored in memory

Network Side Attacks

- **Installation Traffic**
  - Sensitive Installation Information
- **Run Time Traffic**
  - Sensitive Information
  - Vulnerable APIs

Server Side Attacks

- **Network Layer Attacks (TCP UDP Attacks)**
  - Flooding
  - Overflows
- **Layer 7 Attacks**
  - OWASP TOP 10

Common Vulnerabilities

Hardcoded password

Sql Injection

Dll hijacking

Unquoted service path

Denial of Service

Sensitive data in registry keys

Sensitive data in memory

XXE

Deserialization

Source: https://screenrant.com/naruto-powerful-worthless-attacks/

Ninja tools that you need

Static tools – Identify arch, languages & framework	De-compilers and de-obfuscators	Network sniffers – check communication b/w client & server	Proxy tools – sits between client and local/server & allow us to modify requests/response
• CFF Explorer • Peid • Detect It Easy (DIE) • Strings	• dnSpy • ILSpy • DotPeek • Jd-gui • Procyon • De4dot • NeonFuscatorDeobfuscator	• Wireshark • TCPView – part of MS sysinternal • SmartSniff • Tcpdump	• Echo mirage • Burp Suite • Fiddler • Charles Web Proxy

Ninja tools that you need

File analysis – look for sensitive information & files	Binary analysis – Look for code logic, hidden function, validation checks, api keys, and comments etc.	Test for weak GUI control tools	Memory analysis & fuzzing
• Process Monitor • Regshot • Process Explorer • Process Hacker	• Ghidra • IDA Pro • X64dbg • OllyDbg • Immunity Debugger • Radare2 • Frida • Bytecode Viewer • PE Explorer	• WinSpy++ • WinManipulate • Windows Enabler	• Winhex • Volatility • Tsearch • Userdump • Spike • Sulley • AFL • WinAFL

Ninja tools that you need

Miscellaneous
• Attack Surface Analyzer (ASA) • Stunnel • mitm_relay • Robber • Dllspy • sigcheck • Powerup/Sharpup • HeidiSQL • Metasploit • Sqlmap • Sysinternal tools • Canape • Static source code analysis tool etc

Source: https://www.meme-arsenal.com/memes/7ad9746c17bd9452336bb90d66196a78.jpg

Quick Demo

File Settings ?

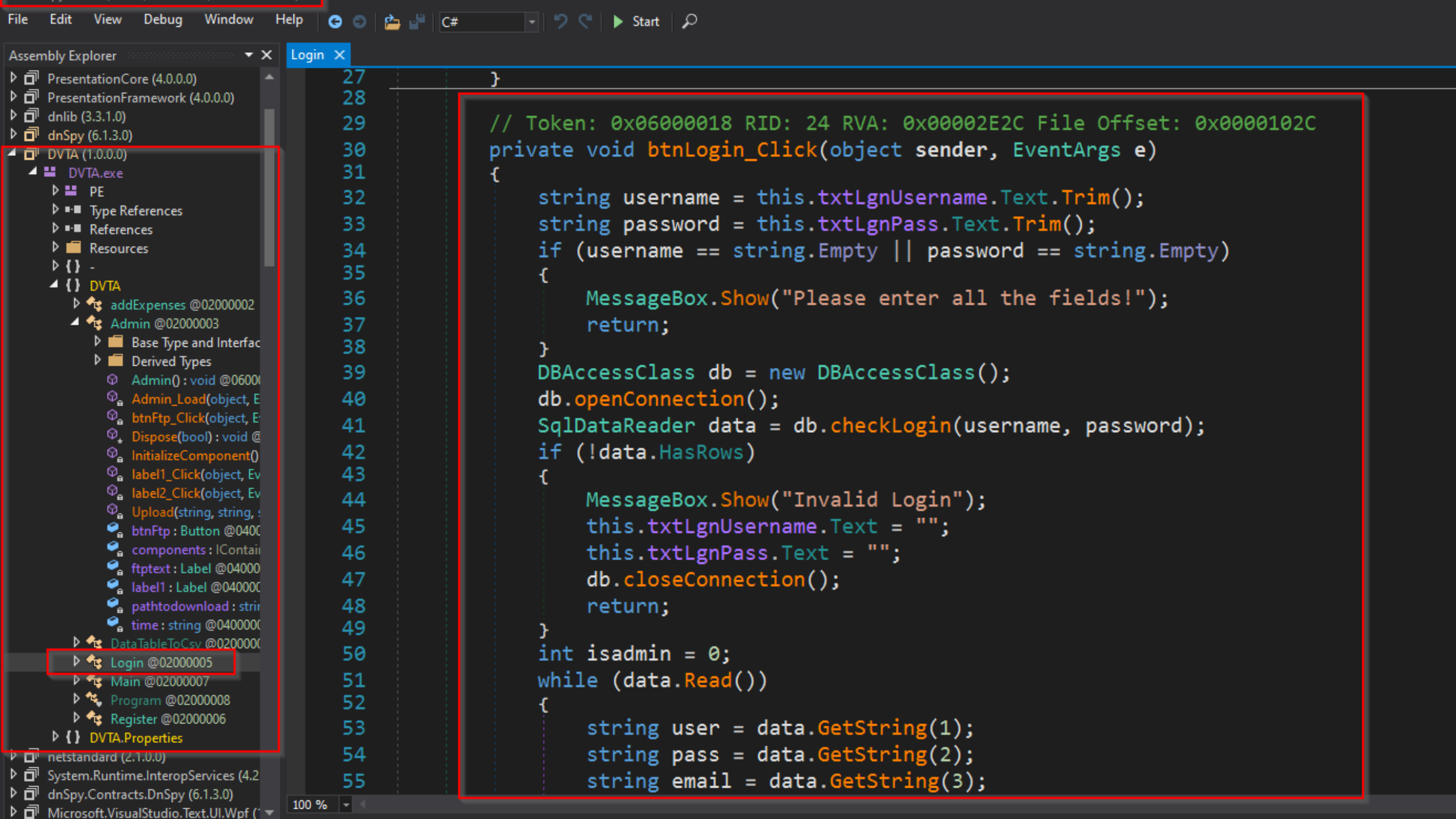


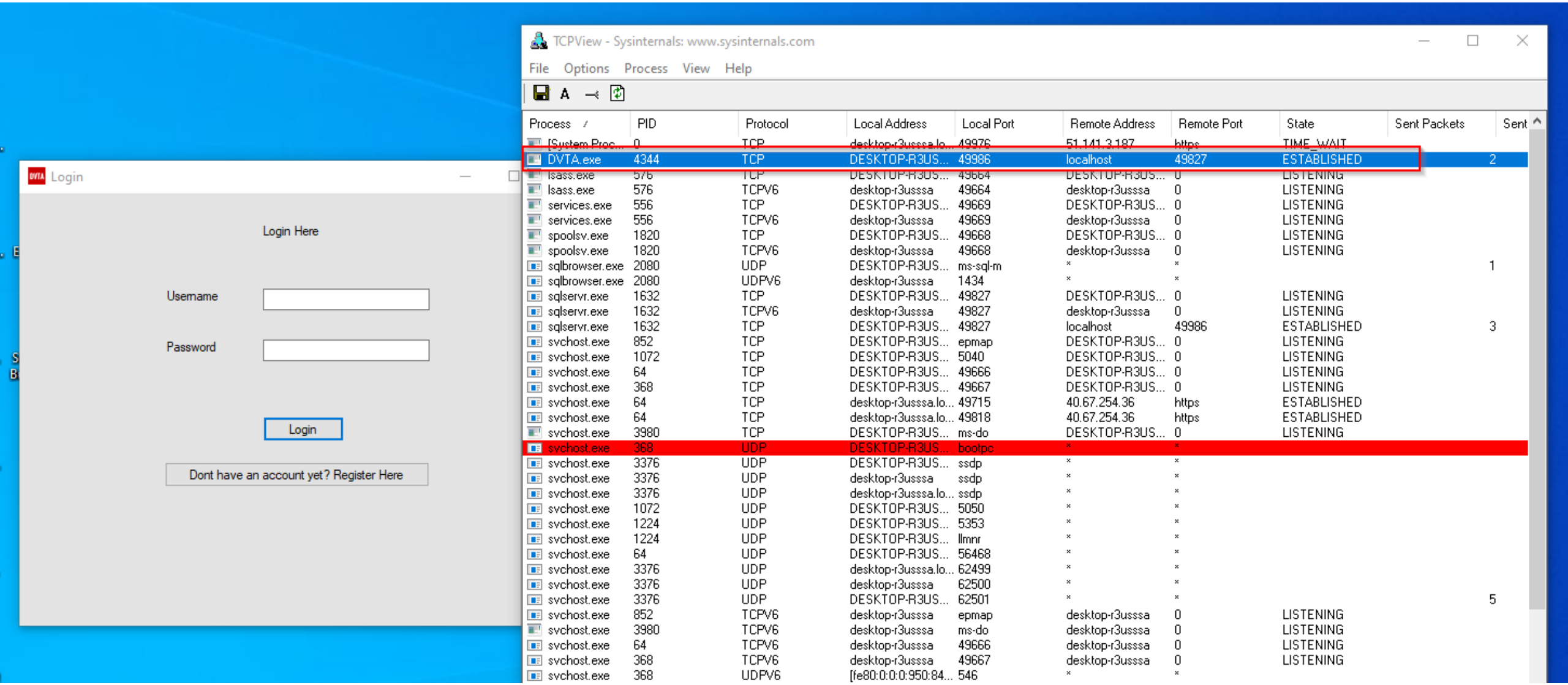
DVTA.exe

Property	Value
File Name	C:\Users\noav\Desktop\dvta\DVTA\bin\Release\DVTA.exe
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	216.50 KB (221696 bytes)
PE Size	216.50 KB (221696 bytes)
Created	Tuesday 04 February 2020, 14.57.49
Modified	Sunday 28 August 2016, 04.15.24
Accessed	Tuesday 26 May 2020, 03.05.25
MD5	9A57726CCB272FE54282C8999E14CEF0
SHA-1	0BD46593E66BE3D7A50DC7C481C4CEB3E9EEF1D9

Property	Value
CompanyName	Microsoft
FileDescription	DVTA
FileVersion	1.0.0.0
InternalName	DVTA.exe

- File: DVTA.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [x]
  - Section Headers [x]
  - Import Directory
  - Resource Directory
  - Relocation Directory
  - Debug Directory
  - .NET Directory
    - MetaData Header
    - MetaData Streams
      - #~
        - Tables Header
        - Tables
      - #Strings
      - #US
      - #GUID
      - #Blob
  - **Address Converter**
  - **Dependency Walker**
  - **Hex Editor**


File Edit View Debug Window Help
C#
Start
Assembly Explorer
Login
PresentationCore (4.0.0.0)
PresentationFramework (4.0.0.0)
dnlib (3.3.1.0)
dnSpy (6.1.3.0)
DVTA (1.0.0.0)
DVTA.exe
PE
Type References
References
Resources
DVTA
addExpenses @02000002
Admin @02000003
Base Type and Interfac
Derived Types
Admin() : void @0600
Admin_Load(object, E
btnFtp_Click(object, E
Dispose(bool) : void @
InitializeComponent()
label1_Click(object, Ev
label2_Click(object, Ev
Upload(string, string,
btnFtp : Button @0400
components : IContai
ftptext : Label @04000
label1 : Label @040000
pathtodownload : stri
time : string @0400000
DataTableToCsv @0200000
Login @02000005
Main @02000007
Program @02000008
Register @02000006
DVTA.Properties
netstandard (2.1.0.0)
System.Runtime.InteropServices (4.2
dnSpy.Contracts.DnSpy (6.1.3.0)
Microsoft.VisualStudio.Text.UI.Wpf
27 }
28
29 // Token: 0x06000018 RID: 24 RVA: 0x00002E2C File Offset: 0x0000102C
30 private void btnLogin_Click(object sender, EventArgs e)
31 {
32 string username = this.txtLgnUsername.Text.Trim();
33 string password = this.txtLgnPass.Text.Trim();
34 if (username == string.Empty || password == string.Empty)
35 {
36 MessageBox.Show("Please enter all the fields!");
37 return;
38 }
39 DBAccessClass db = new DBAccessClass();
40 db.openConnection();
41 SqlDataReader data = db.checkLogin(username, password);
42 if (!data.HasRows)
43 {
44 MessageBox.Show("Invalid Login");
45 this.txtLgnUsername.Text = "";
46 this.txtLgnPass.Text = "";
47 db.closeConnection();
48 return;
49 }
50 int isadmin = 0;
51 while (data.Read())
52 {
53 string user = data.GetString(1);
54 string pass = data.GetString(2);
55 string email = data.GetString(3);
100 %

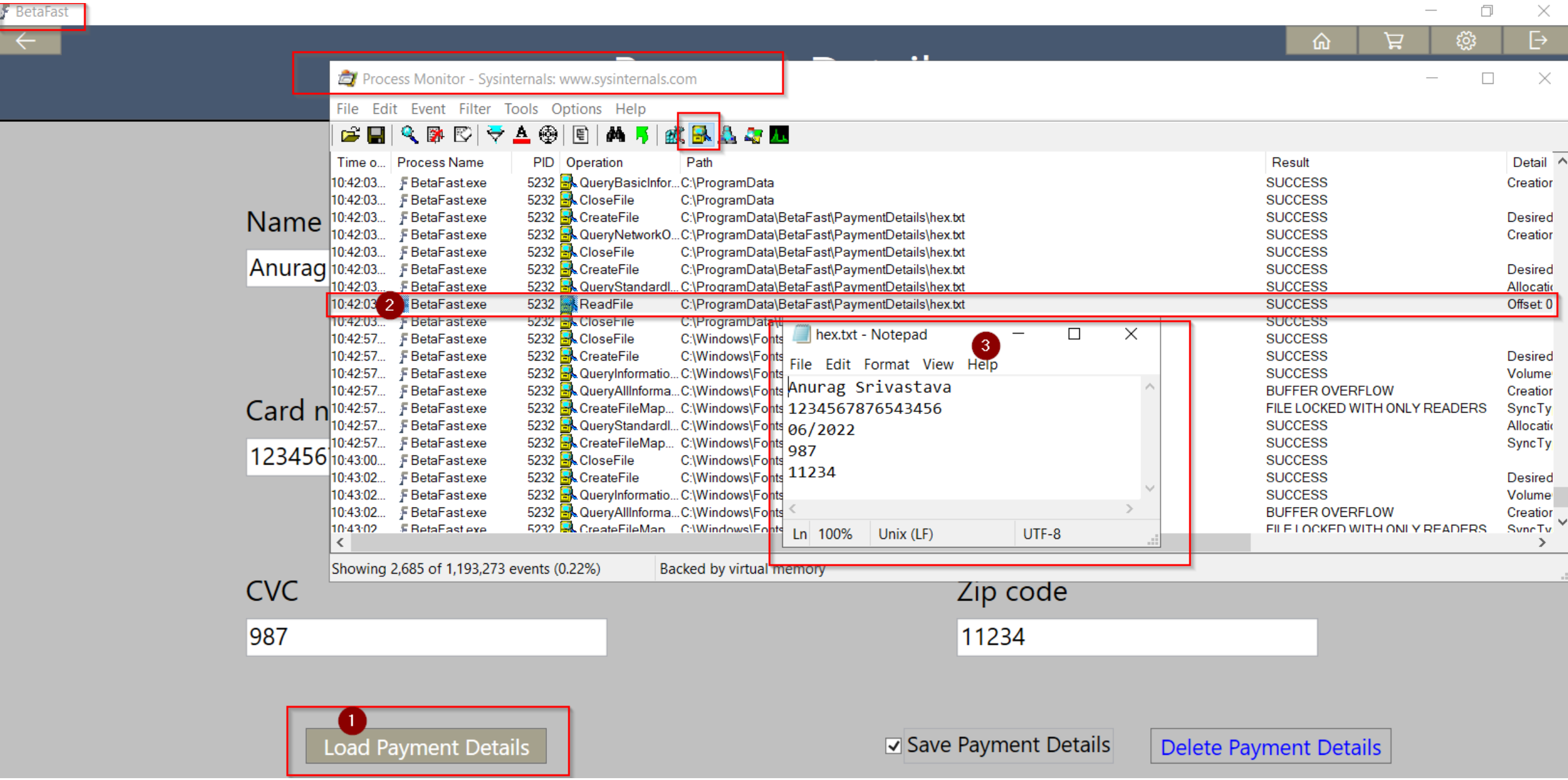

Login
Login Here
Username
Password
Login
Dont have an account yet? Register Here
TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process PID Protocol Local Address Local Port Remote Address Remote Port State Sent Packets Sent
DVTA.exe 4344 TCP DESKTOP-R3US... 49986 localhost 49827 ESTABLISHED 2
lsass.exe 576 TCPV6 desktop-r3usssa 49664 desktop-r3usssa 0 LISTENING
services.exe 556 TCP DESKTOP-R3US... 49669 DESKTOP-R3US... 0 LISTENING
services.exe 556 TCPV6 desktop-r3usssa 49669 desktop-r3usssa 0 LISTENING
spoolsv.exe 1820 TCP DESKTOP-R3US... 49668 DESKTOP-R3US... 0 LISTENING
spoolsv.exe 1820 TCPV6 desktop-r3usssa 49668 desktop-r3usssa 0 LISTENING
sqlbrowser.exe 2080 UDP DESKTOP-R3US... ms-sql-m * * 1
sqlbrowser.exe 2080 UDPV6 desktop-r3usssa 1434 * *
sqlservr.exe 1632 TCP DESKTOP-R3US... 49827 DESKTOP-R3US... 0 LISTENING
sqlservr.exe 1632 TCPV6 desktop-r3usssa 49827 desktop-r3usssa 0 LISTENING
sqlservr.exe 1632 TCP DESKTOP-R3US... 49827 localhost 49986 ESTABLISHED 3
svchost.exe 852 TCP DESKTOP-R3US... epmap DESKTOP-R3US... 0 LISTENING
svchost.exe 1072 TCP DESKTOP-R3US... 5040 DESKTOP-R3US... 0 LISTENING
svchost.exe 64 TCP DESKTOP-R3US... 49666 DESKTOP-R3US... 0 LISTENING
svchost.exe 368 TCP DESKTOP-R3US... 49667 DESKTOP-R3US... 0 LISTENING
svchost.exe 64 TCP desktop-r3usssa.lo... 49715 40.67.254.36 https ESTABLISHED
svchost.exe 64 TCP desktop-r3usssa.lo... 49818 40.67.254.36 https ESTABLISHED
svchost.exe 3980 TCP DESKTOP-R3US... ms-do DESKTOP-R3US... 0 LISTENING
svchost.exe 368 UDP DESKTOP-R3US... bootpc * *
svchost.exe 3376 UDP DESKTOP-R3US... ssdp * *
svchost.exe 3376 UDP desktop-r3usssa ssdp * *
svchost.exe 3376 UDP desktop-r3usssa.lo... ssdp * *
svchost.exe 1072 UDP DESKTOP-R3US... 5050 * *
svchost.exe 1224 UDP DESKTOP-R3US... 5353 * *
svchost.exe 1224 UDP DESKTOP-R3US... llmnr * *
svchost.exe 64 UDP DESKTOP-R3US... 56468 * *
svchost.exe 3376 UDP desktop-r3usssa.lo... 62499 * *
svchost.exe 3376 UDP desktop-r3usssa 62500 * *
svchost.exe 3376 UDP DESKTOP-R3US... 62501 * * 5
svchost.exe 852 TCPV6 desktop-r3usssa epmap desktop-r3usssa 0 LISTENING
svchost.exe 3980 TCPV6 desktop-r3usssa ms-do desktop-r3usssa 0 LISTENING
svchost.exe 64 TCPV6 desktop-r3usssa 49666 desktop-r3usssa 0 LISTENING
svchost.exe 368 TCPV6 desktop-r3usssa 49667 desktop-r3usssa 0 LISTENING
svchost.exe 368 UDPV6 [fe80:0:0:0:950:84... 546 * *

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
10:27:37...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	BUFFER OVERFLOW	Length: 12
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	SUCCESS	Type: REG_SZ, Length: 8, Data: hex
10:27:37...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:27:37...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	BUFFER OVERFLOW	Length: 12
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	SUCCESS	Type: REG_SZ, Length: 8, Data: lol
10:27:37...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:27:37...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	BUFFER OVERFLOW	Length: 12
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	SUCCESS	Type: REG_SZ, Length: 8, Data: hex
10:27:37...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:27:37...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	BUFFER OVERFLOW	Length: 12
10:27:37...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	SUCCESS	Type: REG_SZ, Length: 8, Data: lol
10:27:37...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:28:55...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read/Write
10:28:55...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	BUFFER OVERFLOW	Length: 12
10:28:55...	BetaFast.exe	5232	RegSetValue	HKCU\BetaFast\Credentials\Username	SUCCESS	Type: REG_SZ, Length: 8, Data: hex
10:28:55...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:28:55...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read/Write
10:28:55...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	BUFFER OVERFLOW	Length: 12
10:28:55...	BetaFast.exe	5232	RegSetValue	HKCU\BetaFast\Credentials\Password	SUCCESS	Type: REG_SZ, Length: 8, Data: lol
10:28:55...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:34:19...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read/Write
10:34:19...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Username	BUFFER OVERFLOW	Length: 12
10:34:19...	BetaFast.exe	5232	RegSetValue	HKCU\BetaFast\Credentials\Username	SUCCESS	Type: REG_SZ, Length: 8, Data: hex
10:34:19...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	
10:34:19...	BetaFast.exe	5232	RegOpenKey	HKCU\BetaFast\Credentials	SUCCESS	Desired Access: Read/Write
10:34:19...	BetaFast.exe	5232	RegQueryValue	HKCU\BetaFast\Credentials\Password	BUFFER OVERFLOW	Length: 12
10:34:19...	BetaFast.exe	5232	RegSetValue	HKCU\BetaFast\Credentials\Password	SUCCESS	Type: REG_SZ, Length: 8, Data: lol
10:34:19...	BetaFast.exe	5232	RegCloseKey	HKCU\BetaFast\Credentials	SUCCESS	

Showing 32 of 730,479 events (0.0043%) Backed by virtual memory

Windows Po... C:\Users\no... C:\Users\no... C:\Users\no... DVTA Login DVTA Login Process Mo... BetaFast ENG


BetaFast
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
10:42:03... BetaFast.exe 5232 QueryBasicInfor... C:\ProgramData SUCCESS Creatior
10:42:03... BetaFast.exe 5232 CloseFile C:\ProgramData SUCCESS
10:42:03... BetaFast.exe 5232 CreateFile C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS Desired
10:42:03... BetaFast.exe 5232 QueryNetworkO... C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS Creatior
10:42:03... BetaFast.exe 5232 CloseFile C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS
10:42:03... BetaFast.exe 5232 CreateFile C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS Desired
10:42:03... BetaFast.exe 5232 QueryStandardI... C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS Allocatic
2
10:42:03 BetaFast.exe 5232 ReadFile C:\ProgramData\BetaFast\PaymentDetails\hex.txt SUCCESS Offset: 0
10:42:57... BetaFast.exe 5232 CloseFile C:\Windows\Fonts SUCCESS
10:42:57... BetaFast.exe 5232 CreateFile C:\Windows\Fonts SUCCESS Desired
10:42:57... BetaFast.exe 5232 QueryInformatio... C:\Windows\Fonts SUCCESS Volume
10:42:57... BetaFast.exe 5232 QueryAllInforma... C:\Windows\Fonts BUFFER OVERFLOW Creatior
10:42:57... BetaFast.exe 5232 CreateFileMap... C:\Windows\Fonts FILE LOCKED WITH ONLY READERS SyncTy
10:42:57... BetaFast.exe 5232 QueryStandardI... C:\Windows\Fonts SUCCESS Allocatic
10:42:57... BetaFast.exe 5232 CreateFileMap... C:\Windows\Fonts SUCCESS SyncTy
10:43:00... BetaFast.exe 5232 CloseFile C:\Windows\Fonts SUCCESS
10:43:02... BetaFast.exe 5232 CreateFile C:\Windows\Fonts SUCCESS Desired
10:43:02... BetaFast.exe 5232 QueryInformatio... C:\Windows\Fonts SUCCESS Volume
10:43:02... BetaFast.exe 5232 QueryAllInforma... C:\Windows\Fonts BUFFER OVERFLOW Creatior
Showing 2,685 of 1,193,273 events (0.22%)
Backed by virtual memory
hex.txt - Notepad
3
File Edit Format View Help
Anurag Srivastava
1234567876543456
06/2022
987
11234
Ln 100% Unix (LF) UTF-8
Name
Anurag
Card n
123456
CVC
987
Zip code
11234
1
Load Payment Details
Save Payment Details
Delete Payment Details

Cmder

```
C:\Users\noav  top\BetaFast\BetaFast\BetaFast\bin\Debug\BetaFast.exe
λ sigcheck Desktop\BetaFast\BetaFast\BetaFast\bin\Debug\BetaFast.exe

Sigcheck v2.73 - File version and signature viewer
Copyright (C) 2004-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\noav\desktop\betafast\betafast\betafast\bin\debug\BetaFast.exe:
        Verified:       Unsigned
        Link date:      11:20 07/12/1907
        Publisher:      n/a
        Company:        n/a
        Description:    BetaFast
        Product:        BetaFast
        Prod version:   1.0.0.0
        File version:   1.0.0.0
        MachineType:    32-bit

C:\Users\noav
λ file C:\Users\noav\desktop\betafast\betafast\betafast\bin\debug\BetaFast.exe
C:\Users\noav\desktop\betafast\betafast\betafast\bin\debug\BetaFast.exe: PE32 executable (GUI) Intel 80386 M

C:\Users\noav
λ
```

Burp Suite Community Edition v2020.4.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer | Decoder | Comparer | Extender | Project options | User options

Dashboard | Target | Proxy | Intruder | Repeater

1 × ...

Send | Cancel | < | > | Target: http://www.betafast.net:8080

Request

Raw | Params | Headers | Hex

```
1 POST /api/cart/addHTTP/1.1
2 Accept: application/json
3 Content-Type
  application/x-www-form-urlencoded
4 Host: www.betafast.net:8080
5 Cookie: SessionID=
  CfDJ8C-80920EupIhSBSrl3V6MdhPpoO8pK5O
  BFScZeIN9scYygramuo-LOp8vX4r6rPmjPfNR
  kCPNDespd_e9UVLzIePxWqTKBCpNGgyOclcBn
  Co2UgSFSHoWJZ82S7H3xXMbXXcFE1vFwtiHvG
  RRZpCB820sszJSqHgtYIjkf98CxAbAKV4xuVr
  5_fgNebFyQvLOqWZkrnbkBadatO_Xz5KkHfJ-
  DkmjDKx-QvLkWdfC9x4CCgM1yApQ
6 Content-Length 38
7 Connection: close
8
9 Title=Lunchtime+With+Kevin&Quantity=1
```

0 matches | Pretty

Response

Raw | Headers | Hex

```
1 HTTP/1.1 500 Internal Server Error
2 Connection: close
3 Date: Tue, 26 May 2020 21:43:22 GMT
4 Content-Type: application/json;charset=utf-8
5 Server: Kestrel
6 Content-Length: 3453
7
8 {
  "ClassName":"System.Data.SqlClient.SqlException",
  "Message":"Incorrect syntax near 'n'.\nUnclosed
  "Data":{
    "HelpLink.ProdName":"Microsoft SQL Server",
    "HelpLink.ProdVer":"14.00.3048",
    "HelpLink.EvtSrc":"MSSQLServer",
    "HelpLink.EvtID":"102",
    "HelpLink.BaseHelpUrl":"http://go.microsoft.com
    "HelpLink.LinkId":"20476",
    "SqlError 1":"System.Data.SqlClient.SqlError:
    "SqlError 2":"System.Data.SqlClient.SqlError:
  },
  "InnerException":null,
  "HelpURL":null,
  "StackTraceString":"   at System.Data.SqlClient.
  aTable dataTable)\n   at BetaFastAPI.Utilities.
  "RemoteStackTraceString":null,
  "RemoteStackIndex":0,
  "ExceptionMethod":null
```

Search... | 0 matches | Pretty

Kali Linux Rolling

```
ND error-based - WHERE or HAVING clause (IN)' injectable
[22:36:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:36:33] [INFO] automatically extending ranges for UNION query injection
 technique tests as there is at least one other (potential) technique foun
d
POST parameter 'Title' is vulnerable. Do you want to keep testing the othe
rs (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 31 HTTP
(s) requests:
---
Parameter: Title (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: Title=Lunchtime With Kevin' AND 9207=9207 AND 'ctpd'='ctpd&Qu
antity=1

    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING c
lause (IN)
    Payload: Title=Lunchtime With Kevin' AND 8830 IN (SELECT (CHAR(113) CH
AR(118) CHAR(98) CHAR(107) CHAR(113) (SELECT (CASE WHEN (8830=8830) THEN C
HAR(49) ELSE CHAR(48) END)) CHAR(113) CHAR(122) CHAR(98) CHAR(122) CHAR(11
3))) AND 'lqyN'='lqyN&Quantity=1
---
[22:36:42] [INFO] testing Microsoft SQL Server
[22:36:42] [INFO] confirming Microsoft SQL Server
[22:36:42] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[22:36:42] [INFO] testing if current user is DBA
current user is DBA: True
[22:36:42] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 39 times
[22:36:42] [WARNING] it appears that the target has a maximum connections
constraint
[22:36:42] [INFO] fetched data logged to text files under '/root/.sqlmap/o
```

Activate Windows
Go to Settings to activate Windows.

Cmder | Windows Power... | C:\Users\noav\... | BetaFast | Settings | Burp Suite Com... | Kali Linux Rolling | ENG

Burp Suite Community Edition v2020.2.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Extender Project options User

Dashboard Target Proxy Intruder Repe

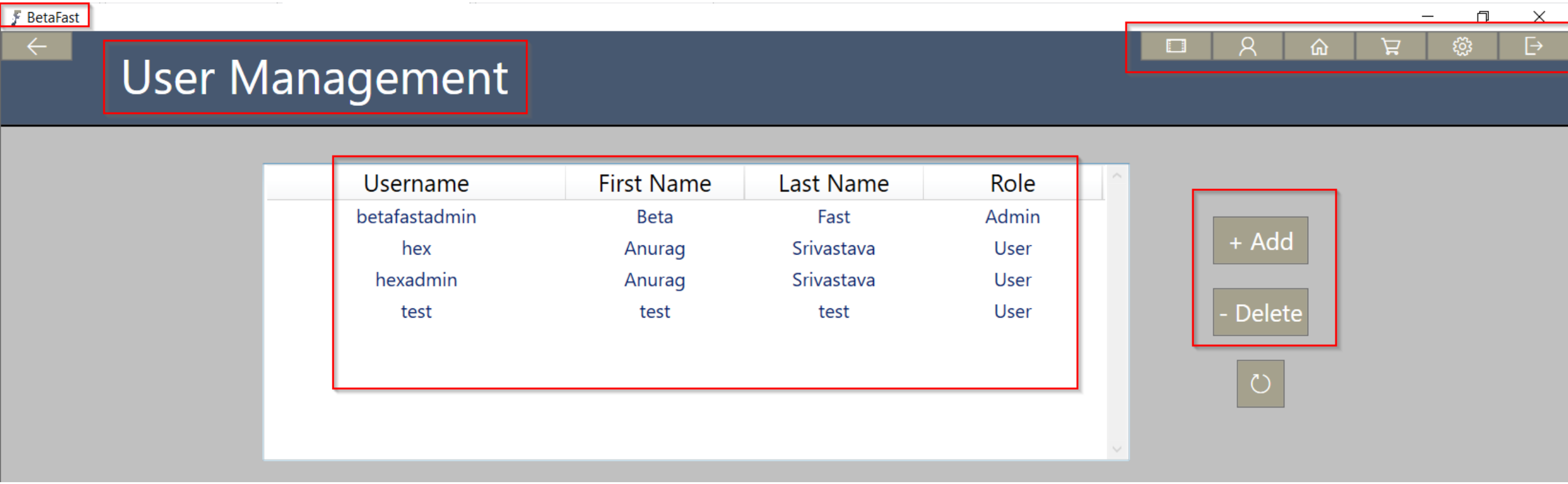
Intercept HTTP history WebSockets history Options

Response from http://www.betafast.net:8080/api/account/usermanagement/isadmin [127.0.0.1]

Forward Drop Intercept i... Action Comment this item

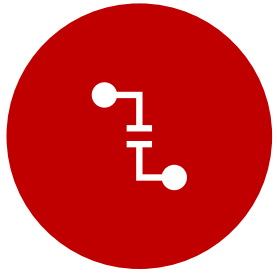
Raw Headers Hex Render

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Tue, 26 May 2020 22:49:01 GMT
4 Content-Type: html/text
5 Server: Kestrel
6 Content-Length: 5
7
8 true
```


BetaFast
User Management
Username
First Name
Last Name
Role
betafastadmin
Beta
Fast
Admin
hex
Anurag
Srivastava
User
hexadmin
Anurag
Srivastava
User
test
test
test
User
+ Add
- Delete

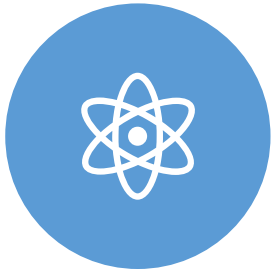
Common Challenges

PROXY UNAWARE



UNABLE TO INTERCEPT COMMUNICATION FROM TOOLS LIKE BURP, ECHO MIRAGE ETC.

SSL BASED ISSUES



CUSTOM PREOPERATORY PROTOCOL LIKE FIX

Possible Solution to our common challenges

Use	• Use Burp Invisible proxy and non-http proxy extension to intercept tcp based traffic
Capture	• Capture packet on Wireshark and write a custom script(client) to send custom requests (can be written in python, ruby etc)
Use	• Use mitm relay embeds every request into a HTTP POST Request so you can relay it through burp
Use	• Use stunnel to intercept ssl based request for clients using ssl over non-http protocol
Add	• Add Proxy's certificate to the Java "System" store using the keytool application to solve java based certificate issues
Decompile and update	• Decompile and update certificate in code and recompile
Use	• Use Detours to hook win32 APIs calls in order to solve issues with preoperatory softwires which uses custom/shared key cryptographic implementation

Basic Checklist

- Check application signing
- Check for Config File
- Test the authentication mechanism
- Test the session management mechanism
- Test access controls
- Test the encryption control
- Test for input-based vulnerabilities
- Test for business logic flaws
- Test for sensitive data storage on files and registries
- Sensitive data Exposure in memory
- Test for response modification
- The reverse engineering method to test backdoors and hardcoded creds
- Test for DLL hijacking vulnerability
- Try to bypass license check/validation check or application patching

Playground

DVTA -
https://github.com/secvulture/dvta

Beta Bank -
https://github.com/NetSPI/BetaFast/tree/master/BetaBank

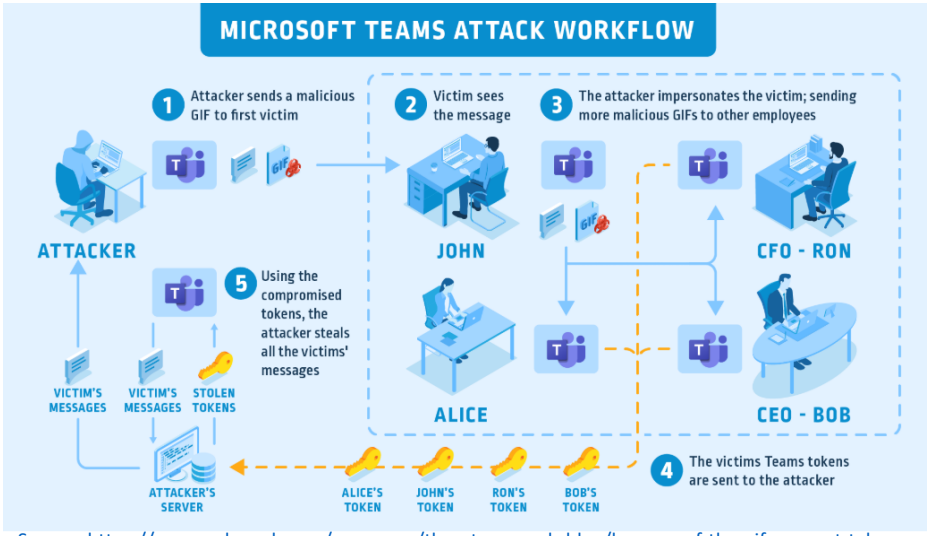
Beta Fast -
https://github.com/NetSPI/BetaFast

DVJA -
https://github.com/appsecco/dvja

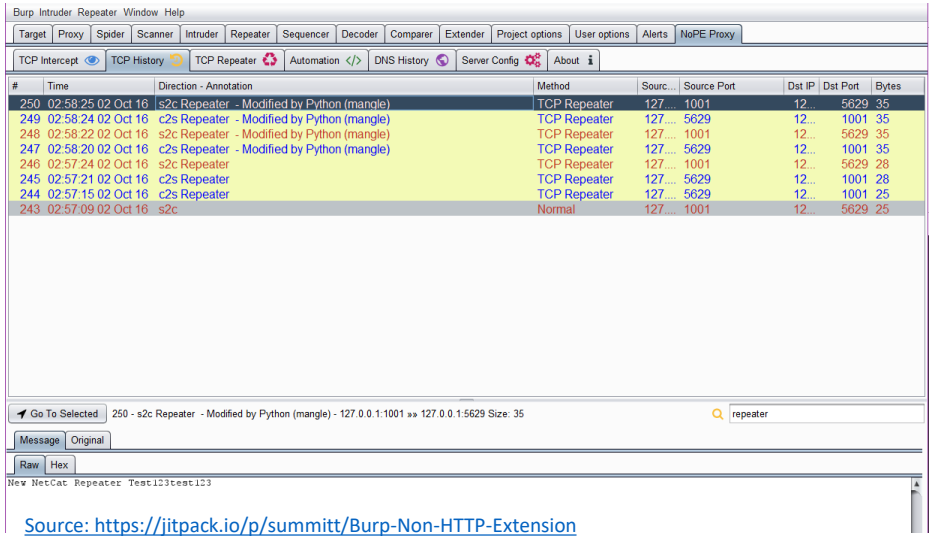
Fatty Machine -
https://www.hackthebox.eu/home/machines/profile/227

Interesting reads

- https://parsiya.net/categories/thick-client-proxying/ (Part 1-10)
- https://medium.com/@mantissts/more-thick-client-fun-73196809493d
- https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams
- https://www.optiv.com/blog/ssl-relay-proxy-a-creative-solution-to-a-complex-issue
- https://jitpack.io/p/summitt/Burp-Non-HTTP-Extension
- https://blog.netspi.com/introduction-to-hacking-thick-clients-part-1-the-gui/
- https://owasp.org/www-pdf-archive/Thick_Client_%28In%29Security_-_Neelay_S_Shah_-_Mar_24.pdf
- https://medium.com/@gdieu/build-a-tcp-proxy-in-python-part-1-3-7552cd5afdfe
- https://blog.appsecco.com/from-thick-client-exploitation-to-becoming-kubernetes-cluster-admin-the-story-of-a-fun-bug-we-fe92a7e70aa2



Source: https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams



Source: https://jitpack.io/p/summitt/Burp-Non-HTTP-Extension

References

- https://www.cyberark.com/resources/threat-research-blog/thick-client-penetration-testing-methodology
- https://resources.infosecinstitute.com/practical-thick-client-application-penetration-testing-using-damn-vulnerable-thick-client-app-part-1/#gref
- https://blog.securelayer7.net/thick-client-penetration-testing-1/
- https://wiki.owasp.org/index.php/OWASP_Windows_Binary_Executable_Files_Security_Checks_Project
- https://github.com/NetSPI/BetaFast


ANY QUESTIONS ?

https://static.zerochan.net/Uzumaki.Naruto.full.1818648.jpg

Credit and Thanks

- Aakash Shukla
- Rahul Singh
- DevJeet singh
- Nipun Jaswal
- Ramandeep Singh
- Deepankar Arora
- Nebu Varghese
- Adhokshaj Mishra
- Deep Shankar Yadav
- Nitin Pandey
- Niv Levy
- Austin Altmann
- NetSpi
- Cyberark
- My mentors and friends – Dhairya giri, Avinash Kumar Tripathi, Manish Kishan Tanwar, Vivek Chauhan, Raghav Bisht, , Kishan Sharma, Harpreet Singh, Himanshu Khokar, Ravi Kiran, D3, Faisal Shadab, Sultan Anwar, Spirited Wolf, Atul, Lakshay, Vardan Bansal, Chaitanya, Pragya Varshney, Pragti, Santhosh, Shubham Gupta, Sudhir Sahni and there is a big list.