Reverse Engineering

Beginner to Advance

Rahadul Islam Rahad

লেখকঃ মোঃ রাহাদুল ইসলাম রাহাদ

Group: Emperor Hacker’s Community

Facebook: https://www.facebook.com/rahadinfosec

বইটি সর্বসাধারনের জন্য সম্পুর্ন ফ্রি!

শুরুতেই বলে রাখছি, আমাদের যাত্রাটি মোটেও সহজ হবে না। কারণ যাত্রাপথে অনেক বাধা আসবে। সেসকল বাধা বিপত্তি দেখে অনেকেই মাঝপথে হাল ছেড়ে দিবে। তাই আগেই বলছি ভালো ভাবে চিন্তা করে আগামীতে পথ চলার জন্য আপনার লক্ষ্য স্থির করুন।

লক্ষ্য স্থির করার পর আপনার দ্বিতীয় কাজ আপনার ভিত্তি (বেসিক’স) আরো মজবুত করা। রিভার্স ইঞ্জিনিয়ারিং সম্পর্কে আপনার বেসিক নলেজটুকু থাকা আবশ্যক যাতে করে আপনার আগামী পথ চলায় বড় সর বাধার সম্মুক্ষিন হতে না হয়। আমরা কিন্তু হুট করেই কোনো একটি সফটওয়্যার নিয়ে সেটিকে রিভার্স করা শুরু করতে পারবো না। আমাদেরকে প্রোগ্রামিং থেকে শুরু করে অনেক কিছু শিখতে হবে। সো চলুন শুরু করা যাক আমাদের যাত্রা.....!

রিভার্স ইঞ্জিনিয়ারিং কিঃ

রিভার্স ইঞ্জিনিয়ারিং বিষয়টি ভালো ভাবে বুঝতে হলে আগে জানতে হবে ইঞ্জিনিয়ারিং শব্দটির অর্থ কি। ইঞ্জিনিয়ারিং শব্দটির অর্থ হলো কোনো কিছু তৈরি করা। সহজ ভাষায় রিভার্স ইঞ্জিনিয়ারিং অর্থ হচ্ছে কোনো তৈরি করা বস্তুকে আবার তার আগের অবস্থায় ফিরিয়ে নিয়ে গিয়ে তার খুটিনাটি বিষয় জেনে আবার তাকে তৈরি করা।

রিভার্স ইঞ্জিনিয়ারিং বিষয়টি অনেক জটিল মনে হতে পারে। বিষয়টি কি আসলেই জটিল? আজ আমরা এ বিষয় নিয়েই শুরুতে আলোচনা করে সব ক্লিয়ার করে নিবো।

প্রথমত, নিজেকে প্রশ্ন করুন, কেন আপনি রিভার্স ইঞ্জিনিয়ারিং শিখতে চাচ্ছেন? যদি আপনার লক্ষ্য নির্ধারণ করা না থাকে তাহলে চলুন রিভার্স ইঞ্জিনিয়ারিং এর কিছু ব্যবহার জেনে নিই।

1. যদি আপনি জানতে চান যে, কিভাবে কোনো সফটওয়্যার বা কোনো বস্তু কাজ করে। উদাহারণঃ এমন কিছু টিম আছে যারা বড় বড় পেইড সফটওয়্যারগুলো ক্র্যাক করে বিনামুল্যে দিয়ে থাকে।

2. ম্যালওয়্যার এনালাইসিস এর জন্য। ম্যালওয়্যারটি কি ধরনের, সেটি কিভাবে কাজ করে এসকল আরো নানান বিষয়ে জানতে ম্যালওয়্যার এনালাইসিস এ রিভার্স ইঞ্জিনিয়ারিং ব্যবহার হয়ে থাকে। বড় বড় এন্টিভাইরাস প্রতিষ্ঠান ম্যালওয়্যার এনালাইসিস এর জন্য আলাদা একটা দক্ষ টিম রাখে যেখানে অনেক দক্ষ রিভার্স ইঞ্জিনিয়ার ও থাকে।

3. কোনো সফটওয়্যার, এপস, গাড়ি বা এধরনের বস্তুর দুর্বলতা (Vulnerability) খুঁজে বের করতে। ইত্যাদি...!

এবার আপনি সময় নিয়ে ভাবেন, আপনি কোন কারণে রিভার্স ইঞ্জিনিয়ারিং শিখতে চান।

তবে আপনি যদি এখনো সিদ্ধান্ত নিতে না পারছেন তবে আগে একটু রিভার্স ইঞ্জিনিয়ারিং এর স্বাদ নেন তারপর সিদ্ধান্ত নিতে আরো সহজ হবে।

রিভার্স ইঞ্জিনিয়ারিং (**Beginner To Advance**) শিখার বিষয়বস্তুগুলোকে আমি তিনটি স্তরে ভাগ করে দিচ্ছি। Beginner, Intermediate, Advance ।

আমরা যখন **রিভার্স ইঞ্জিনিয়ারিং** শুরু করব, তখন দুটো বিষয় আমাদের সামনে আসবে।

- Dynamic Program Analysis
- Static Program Analysis

Dynamic Program Analysis (DPA) :

Dynamic Program Analysis (DPA) হলো সফটওয়্যার চলমান (Run) থাকা অবস্থায় প্রোগ্রাম এর কোড পরীক্ষার একটি প্রক্রিয়া।

Static Program Analysis (SPA) :

Static Program Analysis (SPA) হলো সফটওয়্যার বা প্রোগ্রাম না করে সেটির কোড পরীক্ষা করা ।

চলুন এবার আমাদের রিভার্স ইঞ্জিনিয়ারিং শিখার ধাপগুলো জেনে নিই...।

Beginner Tier:

প্রোগ্রামিংঃ

প্রফেশনাল রিভার্স ইঞ্জিনিয়ারিং এর জন্যও প্রোগ্রামিং নলেজ থাকা আবশ্যক। বিশেষ করে আমাদের কয়েকটি প্রোগ্রামিং ল্যাংগুয়েজ শিখতে হবে। যেমনঃ

C++ Programming:

প্রায় সব সফটওয়্যার-ই সি++ প্রোগ্রাম দ্বারা তৈরি করা হয়ে থাকে। এসব সফটওয়্যার এর রিভার্স ইঞ্জিনিয়ারিং করে তার সোর্স কোড এনালাইসিস করতে গেলে সি++ সম্পর্কে ভালো ধারণা থাকলে বুঝতে অনেক সহজ হবে। যা ম্যালওয়্যার এনালাইসিস এর জন্যও কাজে লাগবে। সি++ প্রোগ্রামিং শিখতে নিচের প্লেলিস্ট এবং পিডিএফ বইটি ফলো করতে পারেন।

Youtube Playlist:

https://www.youtube.com/watch?v=0T4mPpbNs_8&list=PLgH5QX0i9K3q0ZKeXtF--CZ0PdH1sSbYL

PDF Book:

https://drive.google.com/file/d/1xmVO9Z3Mn2rKHW4B-YnCFueISkMomINH/view?usp=sharing

Java Programming:

বেশিরভাগ এন্ড্রয়েড এপস তৈরি হয় জাভা প্রোগ্রামিং ল্যাংগুয়েজ দিয়ে। একটি এপস এর রিভার্স ইঞ্জিনিয়ারিং করার পর সেই এপস এর সোর্স কোড আমাদের সামনে আসে। সেই সোর্স কোড এনালাইসিস করার জন্য আমাদের জাভা প্রোগ্রামিং ল্যাংগুয়েজ জানার প্রয়োজন পড়বে। অন্যথায় আমরা কিছুই বুঝবো না। তাই জাভা প্রোগ্রামিং শিখতে নিচের প্লেলিস্ট ফলো করতে পারেন। সাথে বিভিন্ন ওয়েবসাইট থেকেও শিখতে পারেন।

Playlist:

https://www.youtube.com/watch?v=hf4k4OWlBfI&list=PLgH5QX0i9K3oAZUB2QXR-dZac0c9HNyRa

Website:

https://www.sololearn.com

Assembly Language:

একজন দক্ষ রিভার্স ইঞ্জিনিয়ার হতে হলে আপনাকে অবশ্যই এসেম্বলি ল্যাংগুয়েজ শিখতে হবে। তবে আমাদের এসেম্বলি ল্যাংগুয়েজ এ কোনো প্রোগ্রাম তৈরি করতে হবে না। আমরা যখন কোনো সফটওয়্যার কে ডিসএসেম্বেল করবো তখন আমাদের সামনে অনেক ধরনের কোড আসবে। তার মধ্যে এসেম্বলি ভাষায় লিখা কমান্ড বা কোডগুলোই আমাদের বোধগম্য হবে। তবে বোধগম্য তখনই হবে যখন আমরা এসেম্বলি ল্যাংগুয়েজ জানবো । এসেম্বলি ল্যাংগুয়েজ শিখার জন্য নিচের প্লেলিস্টটি ফলো করতে পারেন।

Playlist:

https://www.youtube.com/watch?v=W9G6JgrQZ5U&list=PL8mraTOYjX3yNe0h3NwvFLgObiG0QLXRQ

Website:

http://www.tutorialspoint.com/assembly_programming/

Intermediate Tier:

প্রোগ্রামিং শিখা শেষ। আমরা এখন ইন্টারমিডিয়েট লেভেল এ প্রবেশ করার জন্য প্রস্তুত। এই লেভেল থেকেই আমাদের রোমাঞ্চকর যাত্রার শুরু। এবার আমরা কিছু রিভার্স ইঞ্জিনিয়ারিং এর টুলস এবং এদের ব্যবহার সম্পর্কে জানবো ও শিখবো। রিভার্স ইঞ্জিনিয়ারিং এর জন্য সবচেয়ে জনপ্রিয় টুলস হচ্ছে Ghidra । এটি একটি ফ্রি টুলস। তবে আমাদের শুধু একটি টুলস দিয়ে কাজ চলবে না। অনেক প্রিমিয়াম টুলস এর ও ব্যবহার শিখতে হবে।

রিভার্স ইঞ্জিনিয়ারিং এর বিভিন্ন টুলস এর নাম হচ্ছে:

1. Ghidra
2. Radare 2
3. Binary Ninja
4. IDA Pro
5. X64dbg etc.

এর পাশাপাশি ডিবাগার, ডিসএসেম্বলার কি, কিভাবে কাজ করে এসব সম্পর্কে জানতে হবে। কিন্তু আমরা ইন্টারমিডিয়েট লেভেলে শুধু তিনটি ডিবাগার এবং ডিসএসেম্বলার এর ব্যবহার শিখবো।

Playlist:

IDA Pro -
https://www.youtube.com/watch?v=N_3AGB9Vf9E&list=PLKwUZp9HwWoDDBPvoapdbJ1rdofowT67z

Ghidra –

https://www.youtube.com/watch?v=fBPj5yEJgck&list=PL7iSco3duZcrs-SgnOXaX9qLyB97tnYLO

x64dbg –

https://www.youtube.com/watch?v=17xy6XCx15M&list=PLGaefQX49kgSDQmQtjL_gTDUWBNpDFarU

Advance Tier:

Practical Assembly:

বিগিনার স্তরে আমরা এসেম্বলি ল্যাংগুয়েজ শিখার বিষয়টি দেখেছিলাম। এসেম্বলি ল্যাংগুয়েজ এর বেসিক না জানা থাকলে আমরা প্র্যাক্টিক্যাল এসেম্বলি শিখতে পারবো না। আর রিভার্স ইঞ্জিনিয়ারিং এ এসেম্বলি ল্যাংগুয়েজ এর কোনো বিকল্প নেই তা আগেও বলেছি। আমরা বিভিন্ন সোর্স থেকে প্র্যাক্টিক্যাল এসেম্বলি ল্যাংগুয়েজ শিখবো।

Playlist:

- https://www.youtube.com/watch?v=vWlAg-pwMsM&list=PLan2CeTAw3pFOq5qc9urw8w7R-kvAT8Yb
- https://www.youtube.com/watch?v=SL--qoiu7yA&list=PLR2FqYUVaFJpHPw1ExSVJZFNlXzJYGAT1

-PE (Portable Executable):

উইন্ডোজ অপারেটিং সিস্টেম কোনো প্রোগ্রামকে রান করতে Portable Executable (PE) ফাইল ফরমেট ব্যবহার করে থাকে। PE ফাইল ফরমেট মূলত একটি ডাটা স্ট্রাকচার যাতে উইন্ডোজ অপারেটিং সিস্টেম লোডারের জন্য আবৃত এক্সিকিউটেবল কোড পরিচালনার জন্য প্রয়োজনীয় তথ্য থাকে। সো একজন রিভার্স ইঞ্জিনিয়ার হিসেবে আপনাকে এই ফাইল ফরমেট এর সাথে পরিচিত থাকতে হবে । কারণ অনেক ক্ষেত্রে PE ফাইল এর ও রিভার্স ইঞ্জিনিয়ারিং করতে হয়। PE ফাইল ফরমেট সম্পর্কে জানতে নিচের ব্লগগুলো পড়তে পারেন।

PE File-format

https://0xrick.github.io/win-internals/pe2/

Windows API:

https://zetcode.com/gui/winapi/introduction/

Reversing:

আমরা অন্তিম পর্বে চলে এসেছি, এবার আমরা এতোদিন যা যা শিখেছি তা দিয়ে প্র্যাক্টিক্যাল কাজ করার পালা। প্র্যাক্টিক্যাল রিভার্স ইঞ্জিনিয়ারিং শিখার জন্য নিচের প্লেলিস্ট ফলো করতে পারেন।

Playlist:

- https://www.youtube.com/watch?v=Bqh0cZDp2vc&list=PLrYOV5wALzaLsIw6QoBlLhohf7dglJSTK
- https://www.youtube.com/watch?v=Ew3jyr8lIe8&list=PLQ7op-Vg9GdZMJACm1ubD8VDLKZPyOHc7
- https://www.youtube.com/watch?v=247I8E2NLGA&list=PLB3s33AwIuDEcoj0CeLdZmqrMhk79XUTF
- https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN

Blogs:

1. Open Security Training Info: http://opensecuritytraining.info/IntroductionToReverseEngineering.html
2. RPISEC, Modern Binary Exploitation: http://security.cs.rpi.edu/courses/binexp-spring2015/
3. Practical Reverse Engineering: http://ca.wiley.com/WileyCDA/WileyTitle/productCd-1118787315,subjectCd-CSJ0.html
4. Reversing: Secrets of Reverse Engineering: http://ca.wiley.com/WileyCDA/WileyTitle/productCd-0764574817.html
5. Malware Unicorn: Reverse Engineering Malware: https://securedorg.github.io/RE101/

Excercise:

কোনো বিষয়ে এক্সপার্ট হতে গেলে প্রয়োজন দুটো জিনিসের। ধৈর্য্য এবং প্রচুর প্র্যাক্টিস। একজন দক্ষ রিভার্স ইঞ্জিনিয়ার হতে প্র্যাক্টিস এর কোনো বিকল্প নাই। রিভার্স ইঞ্জিনিয়ারিং প্র্যাক্টিস এর জন্য সবচেয়ে ভালো হয় সিটিএফ খেলা। সিটিএফ আপনার রিভার্স ইঞ্জিনিয়ারিং এর দক্ষ্যতাকে আরো কয়েকগুণ বাড়িয়ে তুলবে।

Reverse Engineering CTF এর জন্য Tryhackme অনেক ভালো একটি প্লাটফর্ম।

নিচের রুমটি সলভ করার চেষ্টা করুন নিজের দক্ষতা দিয়ে।

Reverse Engineering Room:

https://tryhackme.com/room/reverseengineering

Crackme:

https://crackmes.one/

A Big Resources for A to Z Rerverse Engineering:

এখন শুধু রিসোর্স এর পালা। এই পর্বে রিভার্স ইঞ্জিনিয়ারিং নিয়ে নানান ধরনের এর রিসোর্স পাবেন।

Best Github Repo (RE):

https://github.com/wtsxDev/reverse-engineering

Blogs:

- Introduction to Reverse Engineering Software — Dartmouth
- CSCI 4974 / 6974 Hardware Reverse Engineering
- Starting from Scratch?
- Introduction to Reverse Engineering Software
- Reverse History Part Two — Research
- mammon_’s tales to his grandson
- Reversing Prince Harming’s Kiss of Death

- Theorem prover, symbolic execution and practical reverse-engineering
- Jailbreaks and Pirate Tractors: Reverse Engineering Do's and Don'ts

Tools:

Binary Visualization Tools

- binglide & binvis.io
- visual analysis of binary files
- cantor.dust

General

- Binwalk
- Pip3line, the Swiss army knife of byte manipulation
- Frida
- Binacle
- Construct2

De/Obfuscators/Unpackers

- de4dot
- Universal Extractor
- Stunnix C/C++ Obfuscator
- asar

ELF/Related Tools

- Rdis
- readelf

Emulators

- Unicorn-Engine
- pegasus — Windbg extension DLL for emulation

Packers

- UPX — the Ultimate Packer for eXecutables

PE32/Related Tools

- Dependency Walker
- PPEE(puppy)
- PEStudio
- PEview

OLE

- python-oletools
- http://www.decalage.info/python/oletools

Static Analysis Tools

- Bindead — static binary binary analysis tool
- Static binary analysis tool
- Statically Linked Library Detector

IDA Tutorials/Help

- TiGa's Video Tutorial Series on IDA Pro
- IDA PLUG-IN WRITING IN C/C++
- How to Identify Virtual Table Functions with IDA Pro and the VTBL Plugin
- Reversing C++ programs with IDA pro and Hex-rays
- IDAPython The Wonder Woman of Embedded Device Reversing Maddie Stone — Derbycon7
- IDA FLIRT In Depth

IDA Plugins

- A list of IDA Plugins
- IDA Python — Ero Carrer
- Kam1n0-Plugin-IDA-Pro
- FLARE-Ida
- toolbag
- Dynamic IDA Enrichment (aka. DIE)
- HexRaysCodeXplorer
- Ida Pomidor.
- idaConsonance
- Lighthouse — Code Coverage Explorer for IDA Pro
- NRS
- Ponce

Debuggers

All platforms

- Voltron
- GDB — GNU Debugger
- PEDA — Python Exploit Development Assistance for GDB
- gdbgui
- GEF — GDB Enhanced Features
- Docs
- edb
- LLDB
- PulseDBG

আমি মনে করি যে আমার কাছে যা জ্ঞান আছে তা যথেষ্ট নয় কাউকে রোডম্যাপ দেয়ার জন্য। তবে নিজের কিছু এক্সপেরিয়েন্স এবং এই সাইবার সিকিউরিটি জগতে ক্যারিয়ার তৈরি করা কিছু ব্যক্তিদের থেকে তথ্য নিয়ে একটা সঠিক গাইডলাইন দেয়ার চেষ্টা করছি। ভুল ত্রুটি হলে ক্ষমাসুন্দর দৃষ্টিতে দেখবেন।

সমাপ্ত