

Reverse Engineering for Ethical Hackers

CAE Tech Talk 20 FEB 20

Dr. Bryson Payne, GREM, GPEN, CEH, CISSP
Director, Center for Cyber Ops Education
Professor of Computer Science

About Me

- Dr. Payne: Ph.D. in computer science from Georgia State University, 6 years as a CIO, 22 years teaching CS/IS/Cyber in the University System
- Author of *Teach Your Kids to Code*, 3rd book *Hacking for Kids* comes out in June
- CISSP, CEH, GPEN, SANS/GIAC Reverse Engineering Malware (GREM)
- Coach for the #1 NSA Codebreaker Challenge team UNG Cyber Hawks (2019)

1st Place 2019 (532 schools)



CHALLENGE ENDS

0 Days 00 Hours 00 Minutes 00 Seconds

Overall Progress

Show 10 entries

Search:

University	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6a	Task 6b	Task 7	Score
University of North Georgia	184	125	162	103	82	66	49	30	230,450.00
Georgia Institute of Technology	114	96	95	46	18	5	4	2	56,050.00
Oregon State University	94	89	81	38	9	2	2	1	40,950.00
Lake Washington Institute of Technology	52	46	42	28	11	0	0	0	27,050.00
University of Cincinnati	66	41	37	21	6	1	1	1	24,000.00
New Mexico Institute of Mining & Technology	50	19	18	12	6	3	3	3	22,650.00
University of Texas at El Paso	15	10	10	7	5	4	4	2	15,600.00
New York Institute of Technology	19	15	14	13	4	2	2	1	14,900.00
University of Maryland, College Park	20	14	15	9	8	0	0	1	13,550.00
North Carolina State University	13	8	8	6	5	5	5	0	11,200.00

University	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6a	Task 6b	Task 7	Score
Showing 1 to 10 of 532 entries									
Previous 1 2 3 4 5 ... 54 Next									

Our Story

- *UNG built an NSA Codebreaker-winning cyber operations team by introducing a special topics course on Reverse Engineering from an ethical hacker's point of view, now a regular part of the course catalog.*
- *From reverse-engineering Solitaire and CMD.exe to disassembling Windows, Linux and Android malware with Ghidra and the FLARE VM, all the way to creating keygens to defeat ransomware and get users' files back, I will share UNG's "secret recipe" for getting students excited about reverse engineering and the Codebreaker Challenge.*

How to Win @ NSA Codebreaker in 6 easy steps



Create a Reverse Engineering course



Make it fun



Place in top 10 (#3 in 2018)



Add more to the RE Course



Win (#1 out of 532, in 2019)



Repeat (hopefully)

The flow of the course

- Day 1: Hack Solitaire and CMD.exe
- Demo RE of malware using all the tools (brbbot: IDA, ProcMon, RegShot, etc.)
- Tackle progressively tougher malware/ransomware starting with strings/floss, then Ghidra/IDA, OllyDbg/WinDbg/x64
- [then x64, Linux, Android, based on pref.]
- Ghidra+python to create decryptors
- Circle back to advanced malware w/tools

Reverse Engineering Resources

- Textbook: Practical Malware Analysis – Michael Sikorski et. al.
- Supplemental Texts:
 - Practical Reverse Engineering, Bruce Dang et.al & Reversing: Secrets of Reverse Engineering, Eldad Eilam et. al.
- Two awesome resources: Point3 Escalate and NSA Codebreaker Challenge
- Team communication: [Discordapp.com](https://discordapp.com)

Free Virtual RE Environment

- Virtualbox.org
- Win10 + FLARE VM, REMnux, Kali
- Modern.ie for FREE Win10 VM
- FLARE setup (includes Ghidra):
<https://www.fireeye.com/blog/threat-research/2018/11/flare-vm-update.html>
- Options: Volatility, CheatEngine (min install), mimikatz, Solitaire from WinXP...

Demo Day 1: Hook 'Em

The screenshot displays the Cheat Engine 6.8.1 MissingSetup application. A Solitaire game window is open, showing a score of 100000010. The game board includes a green circle, a deck of cards, and several piles of cards. The Cheat Engine interface is overlaid on the game, showing a search for the value 100000010 at memory address 0062CB20. The search results table is as follows:

Active	Description	Address	Type	Value
<input type="checkbox"/>	No description	0062CB20	4 Bytes	100000010

The Cheat Engine interface also shows a search bar, an 'Undo Scan' button, and a 'Settings' window with options like 'Unrandomizer' and 'Enable Speedhack'. A file explorer window is visible in the bottom left, showing the 'Local Disk (C:)' with 60 items and 1 item selected. The bottom of the Cheat Engine window shows 'Advanced Options' and 'Table Extras'.

Day 2: Hack CMD.exe

The screenshot displays a Windows desktop environment. At the top, there are icons for Recycle Bin, README.txt, and OpenVPN GUI. Below these, a terminal window is open with the following text:

```
C:\Users\IEUser\Desktop>eggo howdy, y'all
howdy, y'all

C:\Users\IEUser\Desktop>EGGO this isn't supposed to be spelled this way?
this isn't supposed to be spelled this way?

C:\Users\IEUser\Desktop>
```

Below the terminal, the 010 Editor application is open, editing the file `C:\Users\IEUser\Desktop\cmd.exe` (Read Only). The editor's interface includes a menu bar (File, Edit, Search, View, Format, Scripts, Templates, Tools, Window, Help) and a toolbar with various icons. The main editing area shows a hex dump with the following columns: 0-9, A-F, and 0123456789ABC. The hex data is as follows:

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABC
3:0CB0h:	54	00	00	00	00	00	00	00	50	00	41	00	54	00	48	00	T.....P.A.T
3:0CC0h:	00	00	00	00	00	00	00	00	52	00	4D	00	44	00	49	00R.M.D
3:0CD0h:	52	00	00	00	52	00	44	00	00	00	00	00	00	00	00	00	R...R.D.....
3:0CE0h:	4D	00	4B	00	44	00	49	00	52	00	00	00	4D	00	44	00	M.K.D.I.R...M
3:0CF0h:	00	00	00	00	00	00	00	00	50	00	52	00	4F	00	4D	00P.R.O
3:0D00h:	50	00	54	00	00	00	00	00	50	00	41	00	55	00	53	00	P.T....P.A.U
3:0D10h:	45	00	00	00	00	00	00	00	53	00	45	00	54	00	00	00	E.....S.E.T
3:0D20h:	45	00	47	00	47	00	4F	00	00	00	00	00	00	00	00	00	E.G.G.O.....
3:0D30h:	52	00	45	00	4E	00	00	00	52	00	45	00	4E	00	41	00	R.E.N...R.E.N
3:0D40h:	4D	00	45	00	00	00	00	00	43	00	48	00	44	00	49	00	M.E....C.H.D
3:0D50h:	52	00	00	00	00	00	00	00	43	00	4F	00	50	00	59	00	R.....C.O.P
3:0D60h:	00	00	00	00	00	00	00	00	54	00	59	00	50	00	45	00T.Y.P
3:0D70h:	00	00	00	00	00	00	00	00	44	00	45	00	4C	00	00	00D.E.L
3:0D80h:	45	00	52	00	41	00	53	00	45	00	00	00	00	00	00	00	E.R.A.S.E....
3:0D90h:	44	00	49	00	52	00	00	00	63	00	6D	00	64	00	2E	00	D.I.R...c.m.d
3:0DA0h:	65	00	78	00	65	00	00	00	00	00	00	00	00	00	00	00	e.x.e.....
3:0DB0h:	6E	00	74	00	64	00	6C	00	6C	00	2E	00	64	00	6C	00	n.t.d.l.l...d

The hex editor also features a Workspace panel on the right, showing a list of files: Open Files (cmd.exe (Read Only), helowrld.exe), Favorite Files, Recent Files, and Bookmarked Files. Below the Workspace panel is the Inspector panel, which displays the following data:

Type	Value
Signed Byte	71
Unsigned Byte	71
Signed Short	71

The Windows taskbar at the bottom shows the Start button, search icon, task view icon, and several application icons, including the terminal and 010 Editor. The system tray on the right shows the time as 2:50 PM.

Progressing through levels of RE

- Start with static analysis: strings and floss
- Progress to IDA/Ghidra for disassembly/decompiling
- Move to Dynamic analysis (debuggers, changing values in memory, changing program flow, rewriting code in memory)
- Build back up to Behavioral analysis with ProcMon, ProcessHacker, RegShot, ProcDot

Payne's Pyramid of RE

Automated

- HybridAnalysis.com, Malwr.com, Cuckoo Sandbox

Behavioral

- ProcHack, ProcMon, RegShot, ProcDot
- Wireshark, fakedns, INetSim

Dynamic Analysis

- x64dbg, WinDbg, OllyDbg, edb, IDA debugger, Android Studio and adb, etc.
- Volatility, Redline

Static Analysis

- Quick: strings, floss, PE Studio, VirusTotal
- Slow: IDA, Ghidra


One option: Point3 ESCALATE

- Paid CTF platform with Win, Linux, Android, x86/x64, ARM and more
- Academic discount w/reassignable seats
- Start with static analysis: strings and floss
- Progress to IDA/Ghidra, then debuggers, tools, then disassembly, decompiling
- Can build your own 'malware' by hiding flags, but ESCALATE has all the levels

Malware Reversing: Decryptors

- Most firms/individuals won't be able to do REM, so one goal is to write a key generator (keygen) or decryptor (especially for ransomware)
- Once we reverse a malware (disassemble or decompile first with automated tools), we can use Python to automatically search for the key/password/flag and decode it
- Then, anyone can run it 😊

Next Steps/Staying up to Date

- Previous years' Codebreaker Challenges
 - BleepingComputer, ID-Ransomware
 - REM mailing lists/forums
 - Consider joining **Bugcrowd** and **Hackerone** and other bug bounties
 - Firmware RE, Car Hacking, IoT, Medical Devices, Exploit development...
- 

Thanks!

- Thanks to the NSA, CBC and CAE teams!
- Thank you for attending today, and see you in Codebreaker 2020!
- Q&A
- Bryson.payne@ung.edu
- [small book plug:
Hacking for Kids is on presale now at Amazon 😊
]

