Jobs / Companies Spreadsheet

My Git Repo for OS Class Content

Recommended Trainings (DO CTFs 😀):

Textbooks:

- Yurichev Reverse Engr + Understanding Assembly Book (**purchased**)
- The Secret Life of Programs (**purchased**)
- CODE: Hidden Language of Computer Hardware and Software (**purchased**)
- Network Attacks and Exploitation (**purchased**)
- Operating System Concepts (**purchased**)
- Practical Malware Analysis: The Hands-On Guide

Cohere Technology LLC Internship - CNO Developer Material:

Note: Content no longer available - have git repo & cloned locally, can ask Sam Thode.

- Art of Exploitation Textbook ->
- CMU CS 213 ICS Course + Labs ->
- OMSCS CS 6200 Network Lab 1 ->
- Windows Exploitation Labs

Beginner Malware Analysis Training from overflow (purchased):

Note: There may be an upgrade here - https://www.0ffset.net/beginner/

Zero 2 Automated Malware Reverse Engineering Bundle (purchased):

Art of Malware Analysis - Ahmed Kasmani, VR Lead MSFT (purchased):

Memberships:

- DigitalU - AF Login (**Note: account could be deprecated at any point**)
- Guided Hacking (**purchased - Quantum Tier - Sept. 28, 2025 end**)
- TryHackMe (**purchased - Nov. 24, 2024 end**)

Free Content:

- Pwn.College - CSE 466 (phenomenal entry course)
- Kernel Learning
- Data Structures and Algos Crash Course
- Operating Systems 1
- Operating Systems 2
- Linux Wargames from OverTheWire
- Network Socket Programming from Beej

Interview Prep:

https://www.linkedin.com/posts/thedavidbrumley_zerodays-ctfs-pwn2own-activity-7145797981412159491-4xU_/?utm_source=share&utm_medium=member_desktop
https://malwaremaycry.medium.com/my-malware-analysis-journey-and-ecmap-edd37dade775
https://nixhacker.com/malware-analysis-interview-questions-1/
https://www.reddit.com/r/Malware/comments/dbsn90/interview_questions_for_malwarevuln_research/
https://medium.com/@0xP/offensive-security-getting-your-foothold-in-the-industry-ac0267cf77a0

Beginner General RE Links:

https://github.com/HACKE-RC/awesome-reversing
https://github.com/paulveillard/cybersecurity-exploit-development
https://ir0nstone.gitbook.io/notes/
https://github.com/guyinatuxedo - https://guyinatuxedo.github.io/index.html
https://github.com/RPISEC/MBE
https://0xinfection.github.io/reversing/
https://www.cs.wcupa.edu/schen/malware23/ (CSC 471 Modern Malware Analysis)
https://www.cs.wcupa.edu/schen/ss2023/ (CSC 472 Software Security)
https://maldevacademy.com/
https://blog.ret2.io/2018/09/11/scalable-security-education/
https://intezer.com/blog/malware-analysis/malware-reverse-engineering-beginners/
https://exploit.education/
https://www.begin.re/the-workshop
https://x86re.com/1.html
https://ctf101.org/binary-exploitation/overview/
https://www.ired.team/
CrashCourse CS
brilliant.io

Beginner Windows RE / Windows Exploitation:

https://www.cyberark.com/resources/threat-research-blog/a-modern-exploration-of-windows-memory-corruption-exploits-part-i-stack-overflows
https://imphash.medium.com/windows-process-internals-a-few-concepts-to-know-before-jumping-on-memory-forensics-part-2-4f45022fb1f8
https://redteamer.tips/help-i-need-to-write-code-in-c-part-2-portable-executable-and-nt-functions/
Walking the PEB

Beginner OS & Linux Kernel Exploitation (note: mostly pulled from work):
https://twitter.com/0xor0ne/status/1742157568074465642
https://www.omscs-notes.com/operating-systems/introduction-to-operating-systems/
https://wiki.osdev.org/Expanded_Main_Page
https://sysprog21.github.io/lkmpg/#hello-world
https://gist.github.com/CMCDragonkai/10ab53654b2aa6ce55c11cfc5b2432a4
https://pwning.systems/posts/an-introduction-to-kernel-exploitation-part1/
https://googleprojectzero.blogspot.com/2020/06/a-survey-of-recent-ios-kernel-exploits.html (Understanding Exploit Primitives)
https://blogs.oracle.com/linux/post/linux-slub-allocator-internals-and-debugging-1
https://blogs.oracle.com/linux/post/linux-slub-allocator-internals-and-debugging-2
https://blogs.oracle.com/linux/post/linux-slub-allocator-internals-and-debugging-3
https://blogs.oracle.com/linux/post/linux-slub-allocator-internals-and-debugging-4

Beginner Linux / Command Line:
Move Fast in Terminal w/ JH
https://vim-adventures.com/
https://kernelgrok.com/
https://levelup.gitconnected.com/a-day-with-vim-tutor-vimtutor-25aa2e6ce52c
https://linuxupskillchallenge.com/
https://linuxjourney.com/
https://github.com/veltman/clmystery

Useful Tools:
Pwndbg & pwntools
https://www.qemu.org/
https://www.shadowsedge.mil/Products/MAPL-PEMR/
https://search.censys.io/
https://gchq.github.io/CyberChef/
https://www.netlimiter.com/
Comodo
https://objective-see.org/products/lulu.html
https://github.com/david942j/one_gadget

Other Textbooks:
https://www.amazon.com/Art-Memory-Forensics-Detecting-Malware/dp/1118825098
https://www.amazon.com/Practical-Reverse-Engineering-Reversing-Obfuscation-ebook/dp/B00IA22R2Y
https://www.amazon.com/One-Hour-Sams-Teach-Yourself/dp/0789757745

CTF/Challenges/Games:
https://wargames.ret2.systems/
https://ctftime.org/
https://247ctf.com/
https://ringzer0ctf.com
https://www.wechall.net/
https://adventofcode.com/
https://squarectf.com
https://cryptopals.com/
https://www.hackthebox.com/
https://academy.hackthebox.com/
https://tryhackme.com/
https://pwn.college/
https://overthewire.org/wargames/bandit/
https://picoctf.com/
https://github.com/veltman/clmystery
Squally (https://store.steampowered.com/app/770200/Squally/)
https://guidedhacking.com/pages/squally-key-with-subscription/
https://huntress.ctf.games/
https://flare-on.com/
https://crackmes.one/
https://imaginaryctf.org/
https://www.acictf.com/

Code Challenges:
https://www.codewars.com/kata/5af31e67252e668be2000120

Events / Competitions::
https://blackhatmea.com/
https://www.cyberwarcon.com/
https://en.wikipedia.org/wiki/Pwn2Own

Setup Stuff:
https://kamransaifullah.medium.com/installing-win-11-on-mac-m1-m2-for-malware-analysis-25aeec725005
https://www.travismathison.com/posts/Windows-11-ARM-Reverse-Engineering/
https://www.youtube.com/watch?v=D0oiaBXOeO0
https://github.com/mandiant/flare-vm#installation
https://muxleet.medium.com/how-to-setup-flare-vm-in-hyper-v-win11-for-reverse-engineering-74152b84fa5e

Cloud / Defensive Cyber / Blue Team / IT / OSINT:
https://www.youtube.com/@MadeByGPS/videos
https://cybersecurity.att.com/blogs/security-essentials/theres-no-such-thing-as-an-entry-level-job-in-cybersecurity
https://github.com/sherlock-project/sherlock
https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
Entire Cyber Security Degree in 15 mins -
https://www.youtube.com/watch?v=AhMSK5GwckU
Symone B - https://www.youtube.com/watch?v=9JKiITtE01s&t=21s
TechTual Chatter - https://www.youtube.com/watch?v=sdQDTh82cJU

John Hammond Certs + Vendor Specific (Azure / AWS/ Splunk / Palo Alto/ Active Directory):
Sec+ -> CEH -> OSCP -> OSCE -> Python PCAP -> OSWE -> eJPT -> eCPPTv2 -> Linux LFCS -> OSEP -> OSED -> OSCE3 -> SANS/SEC -> GIAC

https://medium.com/@0xP/oscp-2022-tips-to-help-you-pass-dddd3563967e

CEH meh, mostly for gov't. OSCP is the GOAT.

Why I like OSCP as a baseline certificate for roles in my team: to have it, you need a variety of skills that are useful in my line of work. You need:
a bit of networking
a bit of binary analysis
a bit of intrusion methodology a bit of intrusion techniques
a bit of information gathering
a bit of exploitation, a bit of OS, a bit of tenacity, a bit of scripting

Paid Certs / Courses / Trainings in the wild:
https://institute.sektor7.net/red-team-operator-malware-development-essentials
https://www.sans.org/cyber-security-courses/red-team-operations-developing-custom-tools-windows/
https://samsclass.info/126/126_S17.shtml
https://malwareunicorn.org/#/workshops
https://www.linkedin.com/posts/robbe-van-roey-365666195_i-obtained-the-cpts-certificate-by-hack-activity-7087519496990564353-0jZU/ (CPTS RESOURCE)
https://www.offensivecon.org/trainings/
https://redsiege.com/training/
https://margin.re/training/
https://recon.cx/2023/training.html
https://www.sans.org/cyber-security-courses/red-team-operations-developing-custom-tools-windows/

RE Peeps / Youtubers (in order of good training):
Dr. Josh Stroschein
GuidedHacking
OALabs
John Hammond
https://connormcgarr.github.io/paging/
https://twitter.com/0xor0ne
LiveOverflow
LowLevelLearning
David Bombal
Rana Khalil
Crow
The Cyber Mentor
ComputerPhile
Jacob Sorber
Cazz
Mad Hat
UnixGuy
Pwn.cat - cts/basteg0d69
Off By One Security (Stephen Sims)
Chompie1337 (Valentina Palmiotti)
Ryan Montgomery
https://axelp.io/ (Axel Persinger)
https://apurvsinghgautam.me/
https://www.linkedin.com/feed/update/urn:li:activity:7111422229350866944/
https://twitter.com/flyryan
https://en.wikipedia.org/wiki/Charlie_Miller_(security_researcher)
https://www.linkedin.com/in/joshuadugie/
https://perfect.blue/
https://www.linkedin.com/in/ayushanand/
https://www.linkedin.com/in/seth-jenkins-a20b914b/
https://shellphish.net/

Youtube Faves:
Hackers Learn Their Craft - https://www.youtube.com/watch?v=6vj96QetfTg
Zero to Hero - https://www.youtube.com/watch?v=7ySes8NCt78
John Hammond Story - https://www.youtube.com/watch?v=sBuxwMAfGnI

Podcasts / Blogs:
https://darknetdiaries.com/
https://tldrsec.com/

RE Game Stuff:
https://gamehacking.academy/lesson/1/1
https://roganmurley.com/2024/01/02/something-a-lot-like-pokemon-yellow.html
https://blog.the.al/2023/01/01/ds4-reverse-engineering.html
https://wololo.net/2023/08/27/ps5-specterdevs-ps5-exploit-implementation-gets-update-with-ps5-pkg-ps4-fpkg-install-support/
https://www.youtube.com/watch?v=Of_JnlMvyzk
https://www.linkedin.com/in/rohanaggarwal13/
nahoragg.github.io/about/
https://www.unknowncheats.me/forum/anti-cheat-software-and-programming/
https://www.youtube.com/watch?v=tUpa03ZKYsg
https://www.youtube.com/channel/UCrNZGLTDkQ01djqiw0m_eRA/community?lb=UgkxY4_Q4cNDwKS28U_ALqScfkSUXWKROw08
https://twitter.com/raratoman/status/1686544629120806912
https://www.phantomoverlay.io/store/category/17-cod-mw3-warzone-cheat/
https://twitter.com/AntiCheatPD/status/1740887033776943442
https://revers.engineering/fun-with-pg-compliant-hook/

General Stuff:

https://www.reddit.com/r/ExploitDev/
https://www.reddit.com/r/OMSCS/comments/luckff/is_omscs_worth_it_for_experienced_engineers/
https://www.imposecost.net/post/flexing-your-arms-for-a-better-resume
https://roadmap.sh/
https://itnext.io/keyboard-shortcuts-for-a-developer-e6d1203774f6
https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx
https://github.com/geohot/fromthetransistor
https://old.reddit.com/r/ReverseEngineering/comments/n2d631/rreverseengineerings_triannual_hiring_thread/
https://breakingdefense.com/2018/09/cyber-force-fights-training-shortfalls-nsa-ions-riot/
https://twitter.com/0xTib3rius/status/1741940367899943207
https://twitter.com/0xTib3rius/status/1741909583893811606
https://www.soc.mil/528th/PDFs/Title10Title50.pdf
https://www.recruiting.af.mil/News/Article-Display/Article/3590467/reserve-component-launches-direct-commission-program-constructive-service-credi/
https://www.bleepingcomputer.com/news/microsoft/microsoft-launches-defender-bounty-program-with-20-000-rewards/
https://aicyberchallenge.com/
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://interviewing.io/blog/when-is-hiring-coming-back-predictions-for-2024

Write-Ups and Reports:
https://pastebin.com/9Bi4N6AC
https://www.reddit.com/r/ExploitDev/comments/17oafwa/looking_for_exploit_dev_vulnerability_research/
https://security.apple.com/blog/
https://blog.isosceles.com/
https://a13xp0p0v.github.io/
https://blog.badsectorlabs.com/
https://chompie.rip/Home
https://faith2dxy.xyz/
https://1day.dev/
https://blog.lexfo.fr/
https://www.reddit.com/r/ExploitDev/comments/17oafwa/looking_for_exploit_dev_vulnerability_research/
https://malwaretech.com/2019/09/bluekeep-a-journey-from-dos-to-rce-cve-2019-0708.html
https://media.defense.gov/2023/May/09/2003218554/-1/-1/1/JOINT_CSA_HUNTING_RU_INTEL_SNAKE_MALWARE_20230509.PDF
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3511738/government-agencies-report-new-russian-malware-targets-ukrainian-military/
https://www.james-odoherty.com/posts/2023/idekctf-2022-typop/
https://about.gitlab.com/blog/2023/09/19/how-gitlab-supports-the-nsa-and-cisa-cicd-security-guidance/
https://twitter.com/lauriewired/status/1683526964802646016
https://qriousec.github.io/post/vbox-pwn2own-2023/
https://www2.fireeye.com/FLAREWebinar.html
https://blog.ret2.io/2023/08/09/jtag-hacking-the-original-xbox-2023/
https://www.quora.com/What-is-the-most-sophisticated-piece-of-software-ever-written-1
https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing
https://developer.nvidia.com/blog/cuda-pro-tip-the-fast-way-to-query-device-properties/
https://firstbreakfast.substack.com/p/avoiding-too-late
https://www.cisa.gov/sites/default/files/2023-10/Phishing%20Guidance%20-%20Stopping%20the%20Attack%20Cycle%20at%20Phase%20One_508c.pdf
https://www.offsec.com/offsec/bypassing-intel-cet-with-counterfeit-objects/
https://twitter.com/__L4w__/status/1719684484969152841?t=a5naBrdlaWgxYzVDzfKs0Q&s=19 (Linux Kernel Intel CET)
https://www.huntress.com/blog/qakbot-malware-takedown-and-defending-forward
(QakBot from John Hammond)

https://www.vice.com/en/article/g5bq89/muslim-pro-location-data-military-xmode

https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

https://www.usff.navy.mil/Press-Room/News-Stories/Article/3587570/uscybercom-flag-officer-visits-ciwt-to-discuss-cyber-training-initiatives/

https://redteamrecipe.com/Satellite-Hacking-Demystified/

https://0x00sec.org/t/super-stealthy-droppers/3715

https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/

https://twitter.com/sweis/status/1740092722487361809

https://www.mayhem.security/blog/3-security-takeaways-from-the-2021-tesla-hack-for-vehicle-manufacturers

https://www.zerodayinitiative.com/blog/2024/1/4/looking-back-at-the-zdi-activities-from-2023

https://intezer.com/blog/research/stealth-wiper-israeli-infrastructure/

https://twitter.com/flyryan/status/1740124511385632933

https://twitter.com/AndrewOliveau/status/1701236395237392752

https://www.mandiant.com/resources/blog/arbitrary-file-deletion-vulnerabilities

https://eln0ty.github.io/malware%20analysis/IcedID/

https://farghlymal.github.io/Stealc-Stealer-Analysis/#stealc-stealer-analysis

https://twitter.com/TalBeerySec/status/1741478985198944715

https://twitter.com/mcohmi/status/1740783415576989825

https://www.hackster.io/news/sce-s-tinygps-gives-the-flipper-zero-location-tracking-capabilities-for-subdriving-6d506695b927

https://twitter.com/vxunderground/status/1700884899597549941 (Do I need to Code?)

https://twitter.com/I_Am_Jakoby/status/1639022231471751168

https://twitter.com/mcohmi/status/1740783415576989825

[Knowledge sometimes Exploits]
Gamozo Labs Blog - https://gamozolabs.github.io/
Diary of a reverse-engineer - https://doar-e.github.io/
Windows Internals Blog - https://windows-internals.com
Sean Heelan's Blog - https://sean.heelan.io
Tavis Ormandy - https://blog.cmpxchg8b.com/
Artificial truth - https://dustri.org/b/
Considerations on Codecrafting - https://blog.polybdenum.com
Hyper-V Internals - https://hvinternals.blogspot.com/
Tyranid's Lair (James Foreshaw) - https://www.tiraniddo.dev/
The Exploit Laboratory - https://blog.exploitlab.net/
Active Directory Security - https://adsecurity.org
Revers.engineering - https://revers.engineering/

[0dayfans Filtered]
https://0dayfans.com/
F-Secure Labs - https://labs.withsecure.com/blog/
Zero Day Initiative - Blog - https://www.thezdi.com/blog/
Check Point Research - https://research.checkpoint.com/

[Casual Blogs]
SerHack - Security Researcher - https://serhack.me/
Jump ESP, jump! - https://httpscolonforwardslashforwardslashwwwdotzoltanbalazsdotcom.com/
m's blog - https://ludovicianul.github.io//
Tim Blazytko’s Blog - https://www.synthesis.to/
GitHub Security Lab - Research - https://github.blog/tag/github-security-lab/
CERT Blogs - https://insights.sei.cmu.edu/feeds/topic/certcc/atom/?utm_source=blog&amp;utm_medium=rss
anti-virus rants - http://anti-virus-rants.blogspot.com/
xorl %eax, %eax - https://xorl.wordpress.com
Intercept the planet! - https://intercepter-ng.blogspot.com/
Hanno's blog - https://blog.hboeck.de/
nedwill’s security blog - https://nedwill.github.io/blog/
Zeta-Two.com - https://zeta-two.com/
ZeroSec - Adventures In Information Security - https://blog.zsec.uk/
DigiNinja - https://digi.ninja/rss.xml
Blog of Osanda - https://osandamalith.com
ADD / XOR / ROL - http://addxorrol.blogspot.com/

[Research]
[Good Feeds]
watchTowr Labs - Blog - https://labs.watchtowr.com/
Isosceles Blog - https://blog.isosceles.com/
Connor McGarr - https://connormcgarr.github.io/
Haboob - https://blog.haboob.sa/
Blog on STAR Labs - https://starlabs.sg/blog/
MDSec - https://www.mdsec.co.uk/
kylebot's Blog - http://blog.kylebot.net/
Access Vector - Vulnerability Research &amp; Software Exploitation - https://accessvector.net/
Stratum Security Blog - https://blog.stratumsecurity.com/
0x36.github.io - https://0x36.github.io/
Impalabs Blog - https://blog.impalabs.com
Stories by Renwa on Medium - https://medium.com/@renwa?source=rss-3f8ae70e3957------2
GitHub Security Lab - https://github.blog/tag/github-security-lab/
David's Blog (pql) - http://blog.dbouman.nl/
Aleph Research - Posts - https://alephsecurity.com/
Aleph Research - Vulns - https://alephsecurity.com/
jub0bs.com - //jub0bs.com/posts/
Talos - Vulnerability Reports - https://talosintelligence.com/vulnerability_reports
Taszk.io labs - https://labs.taszk.io/blog/
Trenchant - https://trenchant.io/
Youssef Sammouda - https://ysamm.com
Maxwell Dulin's Blog - https://maxwelldulin.com/Blog
SSD Secure Disclosure - https://ssd-disclosure.com/
Assetnote - https://blog.assetnote.io/
Blog - Atredis Partners - https://www.atredis.com/blog/
GRIMM Blog - https://blog.grimm-co.com/
Teddy Katz’s Blog - https://blog.teddykatz.com/
Guido Vranken - https://guidovranken.com
Detectify Labs - https://labs.detectify.com
Raelize - https://raelize.com/blog/
Keen Security Lab (Tencent) - https://keenlab.tencent.com/en/
PT SWARM - https://swarm.ptsecurity.com
Realmode Labs - Medium - https://medium.com/realmodelabs?source=rss----a97a5137a6a4---4
Positive Technologies - learn and secure - http://blog.ptsecurity.com/

Microsoft Browser Vulnerability Research - https://microsoftedge.github.io/edgevr/
Synacktiv | Publications - https://www.synacktiv.com/en/publications
research.securitum.com - https://research.securitum.com/
Secfault-Security - https://secfault-security.com/blog.html
Elttam - https://www.elttam.com/blog/
PS C:\Users\itm4n&amp;gt; _ - https://itm4n.github.io/
Sam Curry - https://samcurry.net
Blog on Shielder - https://www.shielder.com/blog/
secret club - https://secret.club/
pi3 blog - http://blog.pi3.com.pl
Rhino Security Labs - https://rhinosecuritylabs.com
Mozilla Attack &amp; Defense - https://blog.mozilla.org/attack-and-defense
Doyensec's Blog - https://blog.doyensec.com//
PortSwigger Research - https://portswigger.net/research
Project Zero - https://googleprojectzero.blogspot.com/
bugs.xdavidhu.me - https://bugs.xdavidhu.me/
Alexander Popov - https://a13xp0p0v.github.io/

[Corporate]

Oversecured - https://blog.oversecured.com/
Qualys Security Blog - https://blog.qualys.com
Researches & Disclosures - Ophion Security - https://ophionsecurity.com/blog/
ZScaler - Security Research/Advisories - https://www.zscaler.com/
RET2 Systems Blog - https://blog.ret2.io/
Datadog Security Labs - https://securitylabs.datadoghq.com/rss/feed.xml
JUMPSEC LABS - https://labs.jumpsec.com
SonarSource - Security - https://www.iot-inspector.com/blog/
Blog | Octagon Networks - https://octagon.net/blog
Technical Blog – NetSPI - https://www.netspi.com/blog/technical/
Ada Logics Blog - https://adalogics.com
Orange Cyberdefense - https://sensepost.com/rss.xml
Quarkslab's blog - http://blog.quarkslab.com/
Insinuator.net - https://insinuator.net
Bishop Fox Labs - https://labs.bishopfox.com/home
NCC Group Research - https://research.nccgroup.com
DEVCORE 戴夫寇爾 - https://devco.re
Payatu - https://payatu.com/blog
SpiderLabs Blog from Trustwave - https://www.trustwave.com/en-us/
r2c website - https://r2c.dev
stolabs - Medium - https://medium.com/stolabs?source=rss----11cfd3349922---4
BlackArrow - http://www.blackarrow.net/

Corelan Team - https://www.corelan.be
Tenable TechBlog - Medium - https://medium.com/tenable-techblog?source=rss----68728ef06732---4
Grsecurity Blog RSS Feed - https://www.grsecurity.net/blog.rss
Immunity Services - http://immunityservices.blogspot.com/
REDYOPS Labs - https://labs.redyops.com
Exodus Intelligence - https://blog.exodusintel.com/
Trail of Bits Blog - https://blog.trailofbits.com
CENSUS - https://census-labs.com/news/
Blog – Praetorian - https://www.praetorian.com/blog/
NotSoSecure - https://notsosecure.com
SonarSource Blog - https://blog.sonarsource.com

[Meta]

Pentester.Land Writeups - https://pentester.land/writeups/
Recent Commits to AppSecEzine:master - https://github.com/Simpsonpt/AppSecEzine/commits/master
ThinkstScapes - https://thinkst.com/ts.html
Maxwell Dulin's Resources - https://maxwelldulin.com/Resources
Bad Sector Labs Blog - https://blog.badsectorlabs.com/

[Individuals]

[Binary]

The Human Machine Interface - https://h0mbre.github.io/
bricked.tech - https://blog.bricked.tech/
random hacks - https://xakcop.com/
SkullSecurity Blog - https://www.skullsecurity.org/
Matteo Malvica - https://www.matteomalvica.com/blog/
phoenhex team - https://phoenhex.re/
gynvael.coldwind//vx.log (en) - https://gynvael.coldwind.pl/
Mogozobo - https://www.mogozobo.com
Alex Plaskett - https://alexplaskett.github.io/
SkyLined - http://blog.skylined.nl//index.html
Brendon Tiszka - https://tiszka.com/
VoidSec - https://voidsec.com/
whtaguy - https://mavlevin.github.io/
Reversing Engineering for the Soul (gbps) - https://ctf.re//
iamelliot’s blog - https://iamelli0t.github.io/
Can.ac - https://blog.can.ac
ETenal - https://etenal.me/
Low-level adventures - https://0x434b.dev/

Saar Amar (MSFT) Publications - https://github.com/saaramar/Publications/commits/master

a place of anatomical precision - https://ysanatomic.github.io

XPN InfoSec Blog - https://blog.xpnsec.com/

pwning.systems - https://pwning.systems/

McCaulay Hudson - https://mccaulay.co.uk

[Web/Other]

Bill Demirkapi - https://billdemirkapi.me/

Dan Revah’s Blog - https://danrevah.github.io/

Sivanesh Ashok - https://blog.stazot.com/

LuemmelSec - https://luemmelsec.github.io/

Max Justicz - https://justi.cz

Alex Chapman's Blog - https://ajxchapman.github.io/

Randy Westergren - https://randywestergren.com/

WitCoat Security Blog - https://blog.witcoat.com

Carnal0wnage &amp; Attack Research Blog - https://blog.carnal0wnage.com/

enigma0x3 - https://enigma0x3.net

markitzeroday.com - https://markitzeroday.com/

MKSB(en) - https://mksben.l0.cm/

inputzero - https://www.inputzero.io/

spaceraccoon.dev - https://spaceraccoon.dev/

Ezequiel Pereira - https://www.ezequiel.tech/

David Nechuta - https://nechudav.blogspot.com/

0xFFFF@blog:~$ (MLT) - https://0x80dotblog.wordpress.com

dozer.nz - https://dozer.nz/

$BLOG_TITLE - https://blog.deesee.xyz/

Posts on qtc's blog - https://blog.tneitzel.eu/posts/

robertchen.cc - https://robertchen.cc/blog

Stories by Marcos Ferreira on Medium - https://medium.com/@mvinni?source=rss-3252e407fe66------2

Axel Persinger’s Blog - https://axelp.io/

Stories by Cedric Owens on Medium - https://medium.com/@cedowens?source=rss-fd791048dac0------2

Luke Rindels - https://luker983.github.io/

Webbie’s Stuff - https://webbie321.github.io/

Paulos Yibelo - Blog - http://www.paulosyibelo.com/

Geek Freak - https://dhiyaneshgeek.github.io/

acut3 - http://localhost:4000/

Abdulrah33m's Blog - https://blog.abdulrah33m.com

Rhynorater's InfoSec Blog - https://rhynorater.github.io

pmnh - https://www.pmnh.site/

Ryan Gerstenkorn Commits - https://github.com/RyanJarv/ryanjarv.github.io/commits/master
(Web-)Insecurity Blog - https://security.lauritz-holtmann.de/
0day.click - https://0day.click
InfoSec Write-ups - Medium - https://infosecwriteups.com?source=rss----7b722bfd1b8d---4
[Linux]
codeblog - https://outflux.net/blog
Linux Audit - https://linux-audit.com

[Blogs]
[Threat Intel]
Cisco Talos Intelligence Group - Comprehensive Threat Intelligence - https://blog.talosintelligence.com/
Securelist by Kaspersky - Research - https://securelist.com/category/research/
Rendition Infosec - https://www.renditioninfosec.com
Microsoft Security Response Center - https://msrc.microsoft.com/blog/
Secureworks Blog - https://www.secureworks.com/blog
Unit42 - https://unit42.paloaltonetworks.com/
[Assessment Firms]
Blog – JFrog - https://jfrog.com
Horizon3.ai - https://www.horizon3.ai/
Bugcrowd - https://www.bugcrowd.com/blog/
TrustedSec - https://trustedsec.com/
Zimperium Mobile Security Blog - https://zimpstage.wpengine.com/blog/
Offensive Security - https://www.offsec.com/
HackerOne - https://www.hackerone.com/
[Software Companies]
BREAKDEV - https://breakdev.org/
Opera Security - https://blogs.opera.com/security/
Rapid7 Blog - https://blog.rapid7.com/
ColbaltStrike Blog - https://www.cobaltstrike.com/
The Cloudflare Blog - http://blog.cloudflare.com
Mozilla Security Blog - https://blog.mozilla.org/security/
Google Online Security Blog - http://security.googleblog.com/
Microsoft Security - https://www.microsoft.com/en-us/security/blog/
Blog – Snyk - https://snyk.io
Internet Policy Research Initiative at MIT - https://internetpolicy.mit.edu/
EFF - Deeplinks - https://www.eff.org/rss/updates.xml
The Daily Swig - https://portswigger.net/daily-swig

[Vuln Reports and Papers]
    [Technical Reports]
        Project Zero - Root Cause Analysis - https://googleprojectzero.github.io/0days-in-the-wild/rca.html
        GitHub Security Lab - Advisories - https://securitylab.github.com/advisories/
        Project Zero Bug Tracker - https://bugs.chromium.org/p/project-zero/issues/list?q=&amp;can=1&amp;sort=-id
        Files ≈ Packet Storm - https://packetstormsecurity.com/
        Full Disclosure - https://seclists.org/#fulldisclosure
        Open Source Security - https://seclists.org/#oss-sec
        HackerOne Recently Disclosed - https://hackerone.com/hacktivity?querystring=&amp;filter=type:public&amp;order_direction=DESC&amp;order_field=latest_disclosable_activity_at&amp;followed_only=false
    [Academia]
        Recent Commits to FuzzingPaper:master - https://github.com/wcventure/FuzzingPaper/commits/master
        University of Minnesota - Computer Science and Engineering - https://cse.umn.edu/cs/latest-research
        IACR Transactions on Cryptographic Hardware and Embedded Systems - https://tches.iacr.org/index.php/TCHES
        SSLabs [Georgia Tech] - https://gts3.org/pages/publications.html
        Kangjie Lu [U. Mn] - https://www-users.cs.umn.edu/~kjlu/

Interview Prep Summary:
Resume Review
Review Bomb & Attack Lab from CMU Course
DEP/ASLR - What are they?
Different Exploit Techniques like ret2libc, format string exploits, etc.
Understanding Shellcode
Function callbacks and function pointers
Different data types such as size_t, unsigned vs signed
Different build templates for app. Development: make, makefile, gcc
Linking Process - DLLs, Header, Object Filles
User Defined Data Types such as typedef and enum
Keywords like extern
MT Lab - POSIX API, Deadlocks, Mutexes
AV Heuristics
Decompilers: https://ctf101.org/reverse-engineering/what-are-decompilers/

Bomb Lab Solutions:
http://zpalexander.com/binary-bomb-lab-phase-4/
Attack Lab Solutions:
https://github.com/magna25/Attack-Lab/tree/master

Interview for Kudu from Tech Lead:

As for specific pointers that would help, make sure that you are comfortable reading and writing C code. This includes conceptual understanding of the heap, the stack, and how a binary is laid out in memory. Understand the difference between a local variable in a function, a global variable, and a malloc allocated variable as they are located in memory.

Understanding of assembly, interrupts and syscalls, and calling conventions like cdecl and stdcall are also a plus. If you are comfortable in assembly, you could be asked to reverse engineer some assembly code.

Resume Review from Sam:
change "Reverse Engineer Skillbridge Intern" to "CNO Developer"

some thoughts / edits for the bullets: for ATL, theyre only going to ask you about what you have listed on your resume. so its better to have bullets you can talk to inside and out, then try and add things you think they want to hear about. for example, you've got Expanded knowledge on CNO topics - Windows System Programming, Windows Kernel, and Kernel Drivers

Bypassed modern security mitigations such as stack cookies, DEP, and ASLR
This is pretty good. I'd cut the word "modern," cookies/DEP/ASLR have been around since early 2000s now.

Developed an Importer with the ability dynamically load DLL modules and retrieve functions
Youll want to hit some more "keywords" here. I'd also make this the first bullet. Keywords here are import table,PEB,dynamically resolved,bypass AV. Did your solution use string compares or hashing?

"Developed a program with an empty import table that dynamically resolved and imported functions at runtime via PEB walk to bypass AV"

Worked hands on with debuggers and RE tools such as gdb, IDA Pro, and pwntools
have you gotten hands on much yet with windbg?
this could go in your "Relevant Coursework" section

Something you could add-
"Wrote a PE file Parser in C (or C++, depending which you use)"
-> This is from the first part of your current module. I'm pretty sure you'd be able to have at least that section done by the time you interview. Ideally you'll have the entire module done and then you can talk to it when you interview, but I wouldnt put the manual mapping project down until youve finished it.