Low-Level Exploitation Training Sheet

Stage – 1 (Baby Steps):

- Cover C concepts from basics to deep level with debugging: https://www.youtube.com/watch?v=ocbVPeHrHUw&list=PL7B2bn3G_wfD8xy4lUaoItwwJ3zKlpuUe
- X86_64 Assembly Basics: https://github.com/DeathNet123/VRED_REPO/blob/main/Assembly.md
- X86_64 Advanced with some architecture overview: https://www.youtube.com/watch?v=sg3GIXvS36w&list=PL7B2bn3G_wfCC2HDSXtMFsskasZ5fdLXz&index=28 (Lec 28 and onwards)
- Cover the concepts of System Programming in Linux: https://www.youtube.com/watch?v=qThI-U34KYs&list=PL7B2bn3G_wfC-mRpG7cxJMnGWdPAQTViW

Stage – 2 (Toddler Steps):

- ELF Part 1: https://intezer.com/blog/research/executable-linkable-format-101-part1-sections-segments/
- ELF Part 2: https://intezer.com//executable-linkable-format-101-part-2-symbols/
- ELF Part 3: https://intezer.com//executable-and-linkable-format-101-part-3-relocations/
- ELF Part 4: https://intezer.com/blog/malware-analysis/executable-linkable-format-101-part-4-dynamic-linking/
- Stack Behind the Curtain: https://www.youtube.com/watchv=1XbTmmWxHzo&list=PL7B2bn3G_wfC-mRpG7cxJMnGWdPAQTViW&index=9
- Mastering the Art of Stack Smashing with different Mitigation on: https://www.mdpi.com/2076-3417/12/13/6702
- PwnCollege Memory Errors challenges: https://pwn.college/program-security/memory-errors
- More about Memory Erros: https://github.com/DeathNet123/VRED_REPO/blob/main/Memory%20Errors.md
- Heap behind the Curtains: https://www.youtube.com/watch?v=zpcPS27ZQr0&list=PL7B2bn3G_wfC-mRpG7cxJMnGWdPAQTViW&index=10
- Azeria Labs Tutorial about heap: https://azeria-labs.com/heap-exploitation-part-1-understanding-the-glibc-heap-implementation/
- Azeria Labs About Heap Part 2: https://azeria-labs.com/heap-exploitation-part-2-glibc-heap-free-bins/
- More About Heap and Heap Exploitation: https://github.com/DeathNet123/VRED_REPO/blob/main/Dynamic%20Allocators.md
- https://pwn.college/software-exploitation/dynamic-allocator-exploitation
- Heap challenges: https://pwn.college/software-exploitation/dynamic-allocator-misuse
- The art of shellcode: https://github.com/DeathNet123/VRED_REPO/blob/main/Shellcode%20Injection.md
- Sandboxing: https://github.com/DeathNet123/VRED_REPO/blob/main/Sandboxing.md

- Sandboxing with Namespaces: https://drive.google.com/drive/folders/1btC4wapBMHaCPD4yYJcZ3Tb3oJGrzqJC?usp=sharing

Stage – 3 (Scuba Diving):

- Understanding the Kernel Security: https://github.com/DeathNet123/VRED_REPO/blob/main/Kernel%20Security.md
- Kernel Exploitation by LkMidas Part 1: https://lkmidas.github.io/posts/20210123-linux-kernel-pwn-part-1/
- Kernel Exploitation by LkMidas Part2: https://lkmidas.github.io/posts/20210128-linux-kernel-pwn-part-2/
- Kernel Exploitation by LkMidas Part3: https://lkmidas.github.io/posts/20210205-linux-kernel-pwn-part-3/
- Ptr-Yudai Blog: https://pawnyable.cafe/linux-kernel/
- https://sam4k.com/exploring-linux-random-kmalloc-caches/#current-heap-exploitation-meta