MANOJ GHIMIRE

ENTRY LEVEL CYBER SECURITY ENGINEER

PERSONAL PROFILE

- Resourceful Computer Engineer with hands-on approach and mindset for designing, hardening and implementing Network Security,Malware Analysis,Reverse Engineering ,System Programming and Scripting for automation. Looking for the position as Cyber Security Internship.

CERTIFICATION:

- CEH from Neosphere
- LITE- 2019
- Quantum Hack

TRAINING

CEH(Certified Ethical Hacker)

- Neosphere

PROJECTS

- Malware-Detection using Random Forest
  - For PE files only
  - Python-pefile
  - Machine Learning
  - Binary Ninja
  - Radare
  - Ghidra
- ARP Poisioning and Sniffing
  - Python
  - Scapy
- Keylogger
  - Using python socket
- PE_Parser

CERTIFICATION

- CEH Neosphere

GET IN CONTACT

manojghimire983@gmail.com
www.manoj983.com.np
https://github.com/Manoj983
Phone: +977-9861628536

HIGHLIGHTS

- Identify and use tools and techniques to conduct static and dynamic analysis of malware, including building a lab environment
- Proficiency with Windows & Linux.
- Solved challenges of Ropemporium, Protostar, TryHackme and HackTheBox
- Strong understanding of operating systems(Linux) and networking.
- Knowledge of worms, viruses, trojan, rootkits, and botnets
- Experience with open source research and development

SKILLS

- Programming in C/C++,Python,Bash,AWK

MALWARE ANALYSIS

- Ability to use YARA rules based on textual or binary patterns and Snort and Scapy for IDS.
- Technical knowledge of the internals of common file formats such as: PE and ELF file formats.
- Parsing of PE and ELF files according to their headers, sections, imports, and exports
- Experience with program and system analyses through OllyDbg, PCap tools,Ghidra and TCP Dump

REVERSE ENGINEERING

- Experience of Radare,GDB,Ghidra,BinaryNinja,Binwalk for reversing ELF and other binaries.
- Familiar with Squashfs , lzma embedded file format
- Binary Exploitation and Buffer overflow
- Familiar with Docker, Virtualbox, and Sandbox Environment
- Experience with Shellcode analysis and ROP , ROP gadgets.
- Able to read, debug and analyze disassembly of x86 and x64 binaries
- Linux system programming in C.
- Compiler Internals experience(gcc, mingw32)

NETWORKING

- Samba with ADDC
- Linux Privilege Escalation
- Experience with Kali Linux, penetration testing tools and techniques
- Ability to perform basic protocol and network analysis, including TCP/IP, UDP, FTP, HTTP, SSH,SMB,etc
- Worked on industries top tools like Nessus, Burp Suite , Metasploit Wireshark,CiscoPacketTracer and OpenVAS
- Support the creation of a big data analysis program through the identification of attributes and indications of targeted activity for profile development

EDUCATION HISTORY

KANTIPUR ENGINEERING COLLEGE [DHAPAKHEL, LALITPUR]

Bachelor of Computer Engineering

KATHMANDU MODEL HIGHER SECONDARY SCHOOL[BAGBAZAR, KATHMANDU]

+2 Science