NGUYEN

NGUYEN MINH

@PicoCTF @pwn.college

CONTACT

+ 1 9035596201

anhminh.nguyen@ace.tamut.edu

7302 Bringle Ridge, Texarkana, TX 75503

SKILLS

Attention to details

Critical thinking

Improving efficiency

Well-Prepared

Creativity

Thinking outside the box

Collaboration and Communication

Problem solving skills

Patient

Time Management

Adaptability

EDUCATION

Texas A&M University-Texarkana, TX 75503 | 3.85 GPA

Google Cybersecurity Professional Certificate

LANGUAGES

Vietnamese/English

SUMMARY

Having strong skills in mathematics, cryptography, and C++ algorithms, I'm an experienced CTF solver (ranked 160th in picoCTF 2024). I'm also eager to expand my knowledge through certifications from Coursera, like advanced algorithm courses. I'm currently working part-time as an Executive Secretary for the IEEE TAMUT Student Branch, so I'm heavily involved with papers, reports, and communications. Recently, I got invited by a professor to do research paper.

EXPERIENCE

Linux command line and SQL (SQLite, NoSQL, MongoDB including in-depth knowledge of Linux commands that utilize shell variables, manage permissions, handle user groups, chain commands, inject and remove custom commands, link and find files, perform file globbing, and pipe commands)
Programming languages (C++, Pascal, C++ Assembly, Python, JavaScript, and Java)
Web vulnerability scanner (Burp Suite)
Network security (Security+ course from TAMUT | 4.0 GPA)
Strong algorithm foundation using C++ and Python
Framworks and control
SIEM tool (Splunk) and packer sniffer (Wireshark)

PROFESSIONAL EXPERIENCE

Executive Secretary of IEEE TAMUT (recognized by IEEE R5)
7101 University Avenue, Texarkana, TX 75503

- Developing academic opportunities for TAMUT students
- Arranging competitions, events, and communications.

CCNA intern at VnPro
149/1D Ung Van Khiem, District Binh Thanh, Ho Chi Minh, VN

- Configuring switches, routers, and access points (AP)
- Creating VPN tunnel, NAC, STP…
- Understanding subnets and IP addressing

Key Accomplishments

- Ensuring timely reports and event managements.
- Web Communication & Scripting (**pwn.college**):
    - Proficient in using Python, curl, and nc (Netcat) for HTTP communication and automation to send different types of HTTP Requests: send custom host header, set url encoded path, specify multiple arguments using GET method, include form data and complex json data with multiple fields using POST method, follow many HTTP redirect from HTTP response, include multiple cookies from HTTP response, and make multiple requests in response to stateful HTTP responses (updating cookies every requests).
- Cryptography Pen-testing Project (**pwn.college**):
    - Conducted penetration tests using pwntools (automated input sender and output receiver), curl (retrieving data from database), mathematics calculation (XOR bitwise operator on Many-time Pad AES), and SQL injection on various cryptographic algorithms: XOR, Hex, Base64, One-time Pad, Many-time Pad AES (ECB, CBC, CPA, POA), DHKE (to AES), RSA, and SHA.
    - Performed TLS handshakes (using pwntools) with self-signed root certificates and private keys, deriving AES-128 keys from the exchanged secrets.
- Web-security Pen-testing Project (server pen-testing) (**pwn.college**):
    - Proficient in manipulating python requests, netcat (for port listening that can capture httponly cookie), URL (performing path traversal attack, shell commands injection, and SQLite injection), and fake server (created by python to retrieve stolen cookie) to perform XSS and CSRF attacks by stealing cookies (including httponly cookie), password, and username.
- Project: Optimized Port-Scanning & Man-in-the-Middle Attack (**pwn.college**)
    - Tools Used: tshark, tcpdump, scapy, ping, nc, socket.
    - Developed an optimized port-scanning technique using tshark for packet analysis and tcpdump for background traffic capture. Employed scapy to manipulate Layer 2, 3, and 4 headers and establish a TCP handshake. Updated the ARP table using ping and used netcat and socket programming to send precise payloads. Successfully executed a Man-in-the-Middle (MITM) attack via ARP poisoning between two devices within the same collision domain.