

Exploiting Simple Buffer Overflows on Win32

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Calculating the Location of RET Overwrite

TCP Echo Server

```
C:\Documents and Settings\SecurityTube\Desktop\Demos>Echo-Server-Memcpy.exe
*****
          Vulnerable TCP ECHO Server v1.0

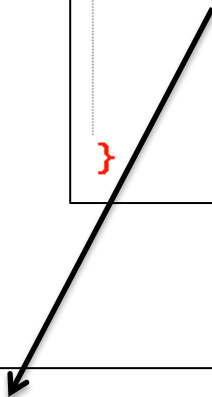
          Mmemcpy(<)

*****

[+] Winsock Init Succeeded!
[+] Server Socket Created!
[+] Server Bind success to port 9000!
[+] Server waiting for connections!
[+] Server got a Connection!
[+] Received Data from Client: 204 Length
[+] Data: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
C:\Documents and Settings\SecurityTube\Desktop\Demos>
```

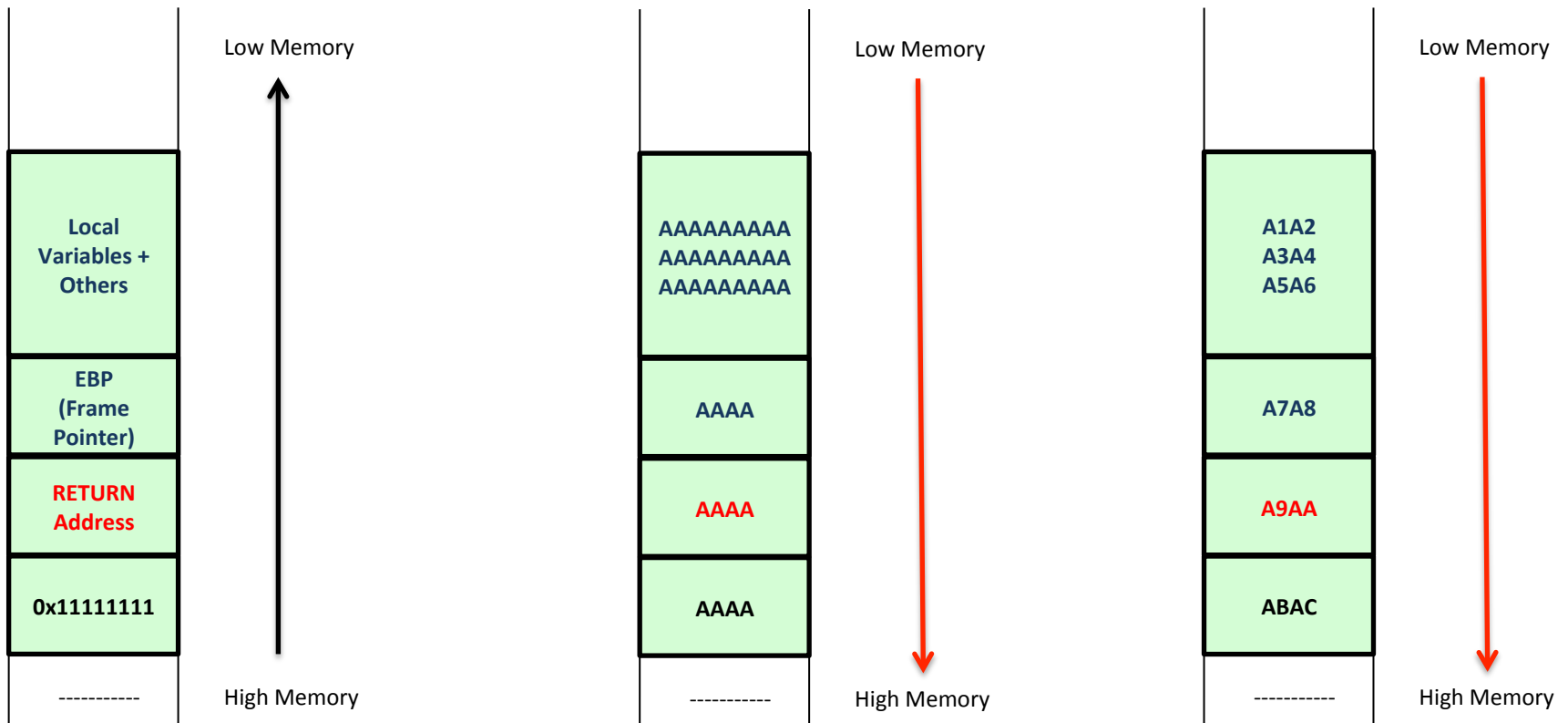
Vulnerable Code

```
while((mlen = recv(clientSock, buffer, len, 0)) > 0)
{
    send(clientSock, buffer, mlen, 0);
    ProcessData(buffer, mlen);
    ZeroMemory(buffer, len);
}
```



```
int ProcessData(char *buffer, int mlen)
{
    char local_buffer[1024];
    memcpy(local_buffer, buffer, mlen);
    printf("[+] Received Data from Client: %d Length\n", mlen);
    printf("[+] Data: %s\n", local_buffer);
}
```

Find RET Position



Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



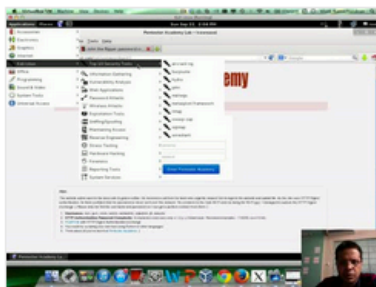
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

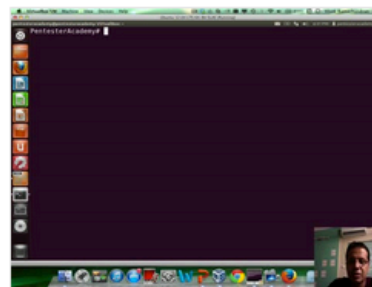
New content added weekly!



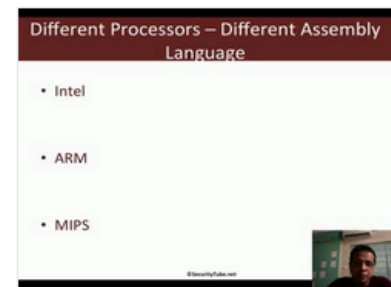
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux