Introduction to Information Security

Shellcodes
Shellcodes

- Raw opcodes that open a shell (or more generally, exploit a vulnerability)
- Challenges
  - Development
    - Assembly
    - No standard functions
  - Constraints
    - Null Bytes
    - Encodings (UTF-8)
    - Evasion (Firewalls and Antivirii)
  - Execution resumption
Solutions

• Development
  • Use C
  • Use system calls
  • Jump directly to PLT entries

• Constraints
  • Be creative 😊
  • Polymorphic shellcodes
    • Decoder – smaller and simpler, decodes the payload and jumps to it
    • Payload – the actual (original) shellcode
Polymorphic Shellcode

JMP _END
_START:
POP EBX
MOV ECX, original-shellcode-size
_DECODE:
XOR byte ptr [EBX], 5
INC EBX
DEC ECX
JNZ _DECODE
JMP _SHELCODE
_END:
CALL _START
_SHELCODE:
original-shellcode

Doesn't have to be that clever...

EBX shellcode data + 1
ECX shellcode size - 1

1 3 3 7

XOR byte ptr [EBX+2], 1
XOR byte ptr [EBX+8], 5
XOR byte ptr [EBX+9], 3
...
Attack Vectors

- Remote Code Execution (RCE)
  - Malicious Packet (targets a server)
  - Malicious Attachment (targets a client)
- Privilege Escalation (PE)
  - Rooting (power users)
  - Evolving (rootkit)
- Malware
  - Trojan Horse
  - Ransomware
- Command and Control (C&C) servers
Remote Shell

- Create a socket
- Connect to the C&C server
- Redirect your streams to your socket
- Become a shell