SEH Exploits

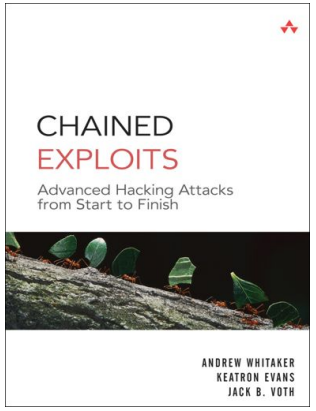
Andrew Whitaker

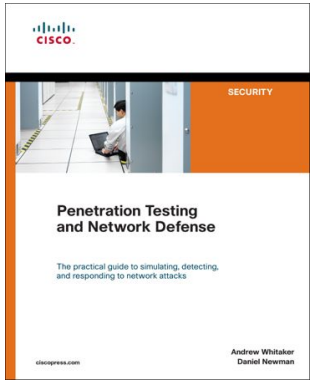
Andrew Whitaker

- Security Researcher / Instructor / Author / Pentester
- EC-Council Master Instructor
- Recipient of EC-Council Instructor of the Year and Instructor of Excellence awards
- M.Sc., CEI, LPT, ECSA, CEH, CHFI, CISSP, CCSP, CCNP, CCVP, CCDP, CCNA:Security, CCDA, MCITP, MCSE, CNE, Security+, Convergence+, A+, Network+, CTP, EMCPA, CEPT, CPT, CEREA, CQS-CATM, CICP

Andrew Whitaker

- Cisco Router Configuration Handbook (Cisco Press
- Chained Exploits: Advanced Hacking Attacks From Start to Finish (Addison-Wesley)
- CCNA Exam Cram, 3rd Edition (Que)
- CCNA Exam Cram, 2nd Edition (Que)
- CCENT Exam Cram (Que)
- CCNA Labs / Simulator (Cisco Press)
- Penetration Testing and Network Defense (Cisco Press)
- Numerous articles, blogs, etc.
- Technical editor for Cisco Press





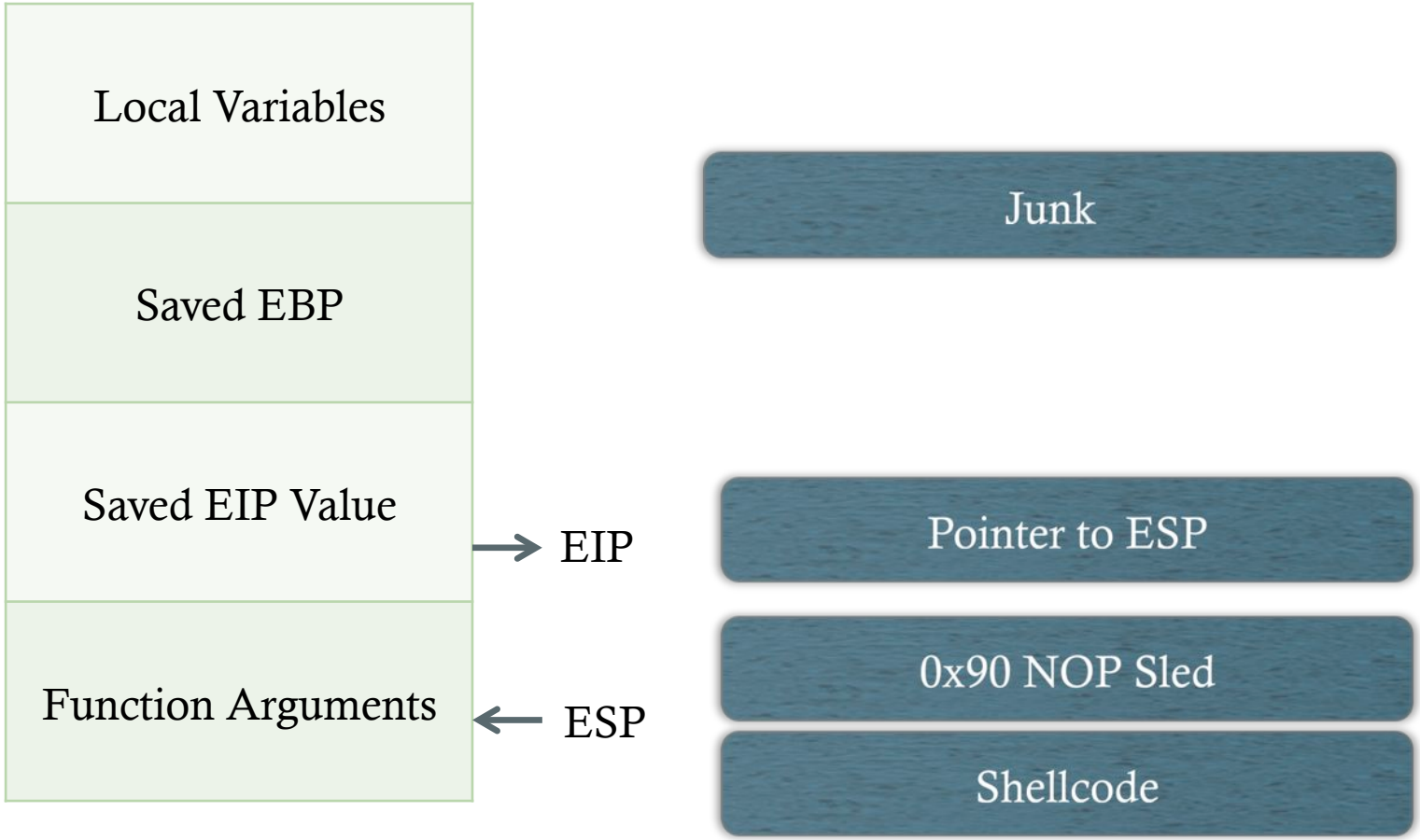
Agenda

- Stack Based Overflow Review
- Structured Exception Handling
- SEH Exploitation
- Demo!

Stack Based Overflows

- Stuffing too much data onto stack and overwriting saved EIP address

Stack Based Overflow Example



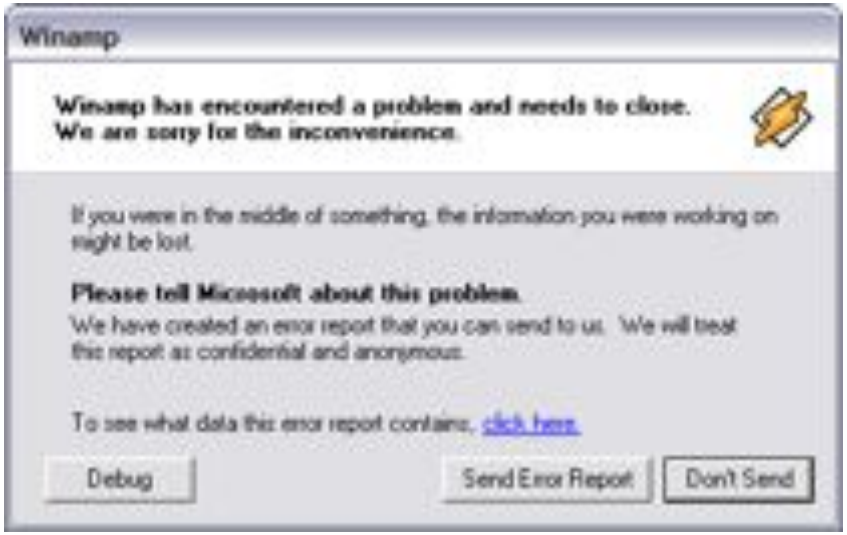
Structured Exception Handlers

- Most exploits today are SEH Exploits
- Just a few exploits discovered in the last two months:
  - 4/21/11 Gesytec ActiveX SEH BOF
  - 4/18 Wireshark SEH BOF (sickness)
  - 4/1/11 Word List SEH BOF (h1ch4m)
  - 3/29/11 IDEAL Administration 2011 SEH BOF (Dr_IDE)
  - 3/18/11 POP Peeper SEH BOF (secuid0)
  - 3/14/11 ABBS Audio Media Player SEH BOF (h1ch4m)

Windows SEH

- Handlers kick in when things go bad

```
__try {
   // guarded code
}
__except {
   // exception handler
}
```



SEH & The Stack

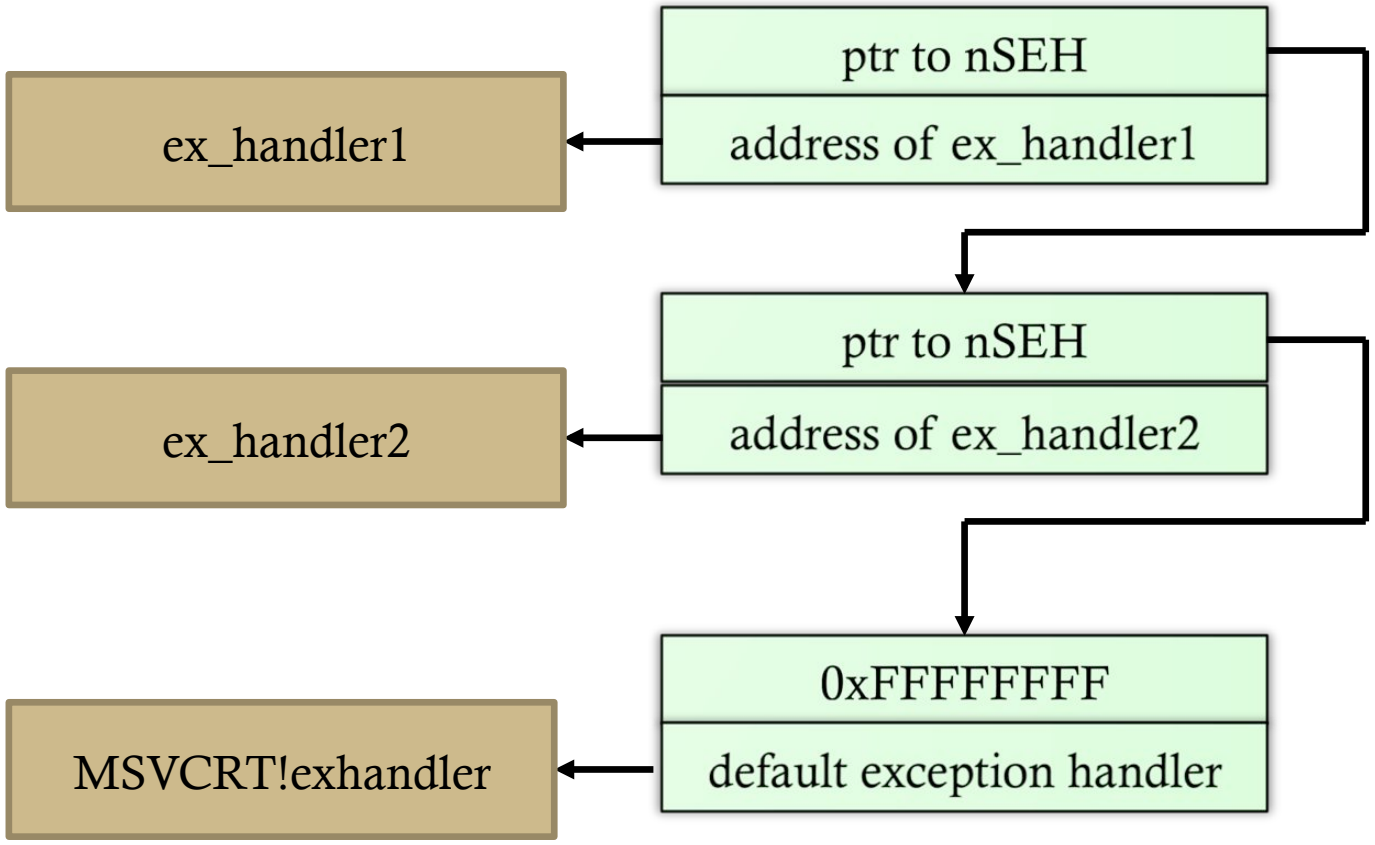
Pointer to exception handler code is pushed onto stack

SEH Records

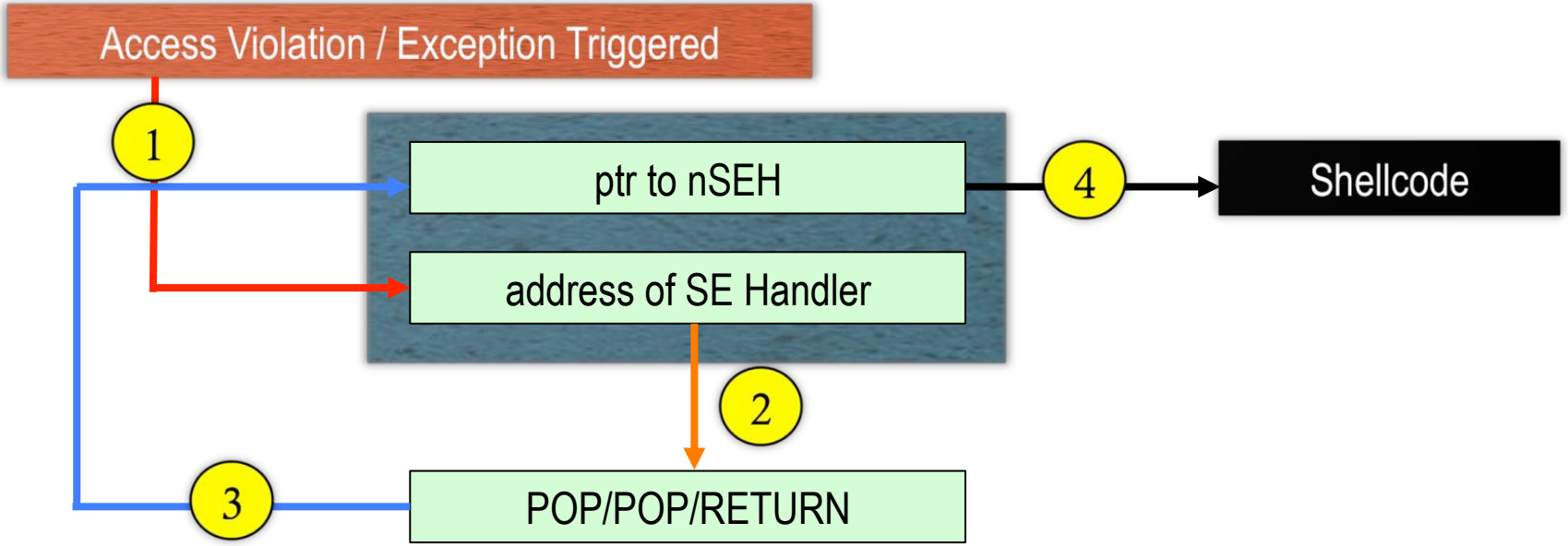
- Each SEH record is 8 bytes
- Stored at high memory addresses

4 Bytes	Pointer to next SEH record
4 Bytes	Address of exception handler code

SEH Chain


ptr to nSEH
address of ex_handler1
ex_handler1
ptr to nSEH
address of ex_handler2
ex_handler2
0xFFFFFFFF
default exception handler
MSVCRT!exhandler

SEH Exploitation



1. Exception handler kicks in
2. Current SE handler is overwritten and points to POP/POP/RETURN
3. POP/POP/RETURN goes 8 bytes back in stack which puts address of nSEH into EIP.
4. Ptr to nSEH is ovewritten with JMP to shellcode.

SEH Exploitation

- Typical payload:

  [Junk][nSEH][SEH][NOP+Shellcode]

  - nSEH = JMP to NOP + Shellcode
  - SEH = reference to POP/POP/RETURN

Demo Time!
Easy Chat Server v2.2 Vulnerability

BID #: 25328
EFS Software Easy Chat Server Authentication Request Handling Remote Buffer Overflow Vulnerability

Easy Chat Server is prone to a remote buffer-overflow vulnerability. Attackers may leverage this issue to execute arbitrary code in the context of the application. Failed attacks will cause denial-of-service conditions.

- Exploit is due to sending long username and/or password to chat.ghp CGI script
- Tools:
  - Python 2
  - Ollydbg
  - OllySEH Plugin
  - Metasploit