05 January 2022 09:48 PM 1. Required Files:a. Vulnserver: git clone https://github.com/stephenbradshaw/vulnserver.git b. Window 7 or Up (VM or Bare Metal) c. Immunity Debugger: https://www.immunityinc.com/products/debugger/ 2. Spiking:a. Running vulnserver and immunity debugger as Administrator i. vulnserver 10/9/2020 6:10 AM COMPILING c essfunc 10/9/2020 6:10 AM essfunc.dll 10/9/2020 6:10 AM LICE :10 AM Open 📝 read 🌍 Run as administrator :10 AM c vulr Open with Code :10 AM ■ vulr Troubleshoot compatibility :10 AM Share with Add to archive... Add to "vulnserver rar" C:\Users\at0m_b0mb\Desktop\vulnserver-master\vulnserver.exe Starting vulnserver version 1.00 Called essential function dll version 1.00 This is vulnerable software! Do not allow access from untrusted systems or networks! Waiting for client connections... 1) iii. Immunity debugger:-Recycle E Troubleshoot compatibility Open file location Add to archive... Add to "Immunity Debugger.rar" Compress to "Immunity Debugger.rar" and email Run as administrator Open with Code Pin to Taskbar Pin to Start Menu vulnserve Restore previous versions Send to Cut Copy vulnserve Create shortcut Delete Rename **Properties** Immunity Debugger _ 0 X Immunity Debugger - [CPU] File View Debug Plugins ImmLib Options Window Help Jobs 🖿 🐎 🗏 🔣 📢 🖈 ▶ || 🛂 🖊 🔰 → | lemtwhcPkbzr...s 🙎 Immunity: Consulting Services Manager Registers (FPU) Address Hex dump Help Ready iv. Attaching immunity debugger to vulnserver:-Immunity Debugger - [CPU] C File View Debug Plugins Open Ctrl+F1 Attach Detach Exit Alt+X _ D X Select process to attach Listening Window 2268 mscorsvw 3808 vulnserver C:\Users\at0m_b0mb\Desktop|C: Attach Cancel Immunity Debugger - vulnserver.exe - [CPU - thread 00000C8C, module ntdll] File View Debug Plugins ImmLib Options Window Help Jobs lemtwhcPkbzr...s? Immunity: Consulting Services Manager 7767000D 7767000E 7767000F Registers (FPU) EAX 7EFDA000 ECX 00000000 7670010 776FF512 ntdll.DbgUiRemoteBrg 7670011 7670012 ESP 024AFF50 EBP 024AFF88 7670013 670014 ESI 000000000 EDI 00000000 670016 7670017 EIP 7767000D ntdll.7767000D 7670018 002B 32bit 0(FFFFFFF) 7670019 CS 0023 32bit 0(FFFFFFFF) SS 002B 32bit 0(FFFFFFFF) DS 002B 32bit 0(FFFFFFFF) FS 0053 32bit 7EFDA00(FFF) 767001A 767001B 767001C 767001D GS 002B 32bit 0(FFFFFFF) 767001E 767001F 0 0 LastErr ERROR_SUCCESS (0000 7670020 7670021 7670022 EFL 00000246 (NO,NB,E,BE,NS,PE,G STØ empty g 7670023 7670024 empty g 7670025 7670026 T3 empty g iT4 empty g 7670027 3T5 empty g 7670028 ST6 empty g 7670029 ST7 empty g 767002A 3 2 1 0 E S FST 0000 Cond 0 0 0 0 Err 0 0 FCW 027F Prec NEAR,53 Mask 767002B 767002C 767002D 767002E 767002F 7670030 7670031 7670032 7670033 7670034 7670035 7670036 7670037 670038 7670039 67003A 767003B 67003C 767003D 767003E 767003F ECX,DWORD PTR SS:[ESP+4] T BYTE PTR DS:[ECX+4],6 7670040 8B4C24 04 7670044 F641 04 06 7670048 Return to 776FF54E (ntdll.776FF54E) 024AFF50 024AFF60 776FF54E NJow RET 00403000 FF FF FF FF 00 40 00 00 00403008 70 2E 40 00 00 00 00 00 p.@.... 00403010 FF FF FF 00 00 00 00 024AFF64 000000000 000000000 [22:37:14] Attached process paused at ntdll.DbgBreakPoint Paused v. Back to kali linux :-1) Created a subfolder and started a nmap scan on the target running vulnserver :nmap -p- -A -T5 192.168.222.146 -oN nmap_win7.txt Starting Nmap 7.92 (https://nmap.org) at 2022-01-10 22:44 IST Nmap scan report for 192.168.222.146 Host is up (0.00052s latency). Not shown: 65534 filtered tcp ports (no-response) PORT STATE SERVICE VERSION 9999/tcp open abyss? MAC Address: 00:0C:29:FC:43:25 (VMware) Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows 8 Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.52 ms 192.168.222.146 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. Nmap done: 1 IP address (1 host up) scanned in 593.04 seconds 2) We found out the port were vulnserver is running:a) Port = 9999 3) Let's try to make a connection using netcat and check what is vulnserver! a) Command: nc -nv 192.168.222.146 9999 -# nc -nv 192.168.222.146 9999 (UNKNOWN) [192.168.222.146] 9999 (?) open Welcome to Vulnerable Server! Enter HELP for help. Valid Commands: HELP STATS [stat_value] RTIME [rtime_value] LTIME [ltime_value] SRUN [srun_value] TRUN [trun_value] GMON [gmon_value] GDOG [gdog_value] KSTET [kstet_value] GTER [gter_value] HTER [hter_value] LTER [lter_value] KSTAN [lstan_value] b) We are going to use generic_send_tcp for spiking:-└# generic_send_tcp argc=1 Usage: ./generic_send_tcp host port spike_script SKIPVAR SKIPSTR ./generic_send_tcp 192.168.1.100 701 something.spk 0 0 ii) The tool requires a custom script ".spk" file, lets create one:stat<mark>s.spk</mark> /home/atom/Targets/at0m_b0mb_W7/ex... 1 s_readline(); 2 s_string("STATS "); 3 s_string_variabe("0"); Code for the file:-STATS FILE.spk s_readline(); s string("STATS") s_string_variable("0"); One. Running generic_send_tcp for stats function in vulnserver Syntax:- generic_send_tcp 192.168.222.146 9999 stats.spk 0 0 generic_send_tcp 192.168.222.146 9999 stats.spk 0 0 Total Number of Strings is 681 Fuzzing Fuzzing Variable 0:0 Fuzzing Variable 0:1 Variablesize= 5004 Fuzzing Variable 0:2 Variablesize= 5005 Fuzzing Variable 0:3 Variablesize= 21 Fuzzing Variable 0:4 Variablesize= 3 Fuzzing Variable 0:5 Variablesize= 2 Fuzzing Variable 0:6 Variablesize= 7 Fuzzing Variable 0:7 Variablesize= 48 Fuzzing Variable 0:8 Variablesize= 45 Fuzzing Variable 0:9 Variablesize= 49 Let's see what is happening at the host side! We are connecting and then disconnecting:-_ O X C:\Users\at0m_b0mb\Desktop\vulnserver-master\vulnserver.exe Send failed with error: 10054 Received a client connection from 192.168.222.131:35008 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35010 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35012 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35014 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35016 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35018 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35020 Waiting for client connections... Recv failed with error: 10054 Received a client connection from 192.168.222.131:35024 Waiting for client connections... After going through the data from immunity debugger, we found nothing special is happening! Immunity Debugger - vulnserver.exe File View Debug Plugins ImmLib Options Window Help Jobs 🖿 🐆 🖫 🔣 📢 🗶 💵 👭 🛂 🔰 🔰 🖠 lemtwhcPkbzr...s? Immunity: Consulting Services Manager CPU - thread 00000478, module ntdll - -Registers (FPU) 51 53 8B5D 08 8B43 10 56 8B75 10 773810B 773810D 773810E 773810F 77381E2 77381E5 PUSH ECX PUSH EBX EBX, DWORD PTR SS: [EBP+8] EAX, DWORD PTR DS: [EBX+10] PUSH_ESI ESI, DWORD PTR SS: [EBP+10] 73B1E6 PUSH EDI MOV EDI,EAX EDI,EMO
EDI,3
EDI,3
EAX,DWORD PTR DS:[EAX+ESI*8]
EDI,3F
A ECX,DWORD PTR DS:[ESI*8]
U DWORD PTR SS:[EBP+8],EDI
U DWORD PTR DS:[EBX+10],EAX C1EF 03 8D04F0 83E7 3F 8D0CF5 00000000 773B1EC 773B1EF 773B1F2 773B1F5 773B1FC 773B1FF 897D 08 8943 10 3BC1 73 Ø3 FF43 14 73B202 EAX, ECX 73B204 DWORD PTR DS:[EBX+14] EDX,ESI 773B206 8BD6 773B209 EDX, 1D DWORD PTR DS:[EBX+14],EDX C1EA 1D 0153 14 73B20B 73B20E EDI, EDI 85FF 76 4E 773B211 773B213 EAX, DWORD PTR DS: [ESI+EDI] DWORD PTR SS: [EBP-4], EAX EAX, 40 8D043E 8945 FC 773B215 773B218 83F8 40 72 43 8B4D 0C B8 40000000 773B21B 773B21E ECX, DWORD PTR SS: [EBP+C] EAX, 40 EAX, EDI 773B220 773B223 773B228 2BC7 PUSH EAX PUSH ECX 73B22A 50 51 8D541F 18 LEA EDX, DWORD PTR DS: [EDI+EBX+18] 000000000 022BFFC4 022BFFC8 Address Hex dump 00403000 FF FF FF FF 00 40 00 00 00.00 00403008 70 2E 40 00 00 00 00 00 p.@.... 00403010 FF FF FF FF 00 00 00 00 00 00403018 FF FF FF FF 00 00 00 00 00 00403020 FF FF FF FF 00 00 00 00 00 000000000 022BFFCC 000000000 022BFFD0 000000000 022BFFD4 000000000 022BFFD8 000000000 022BFFDC 00403028 00 00 00 00 00 00 00 00 000000000 022BFFE0 00403030 00 00 00 00 00 00 00 00 000000000 022BFFE4 00403038 00 00 00 00 00 00 00 00 022BFFE8 000000000 00403040 00 00 00 00 00 00 00 00 000000000 022BFFEC 00403048 00 00 00 00 00 00 00 00 00403050 00 00 00 00 00 00 00 00 000000000 022BFFF0 Running New thread with ID 000016A8 created Doing the same thing for RTIME • Code for spk file:s_readline(); s_string("RTIME") s_string_variable("0"); Running generic_send_tcp Syntax:- generic_send_tcp 192.168.222.146 9999 rtime.spk 0 0 tobomb)-[/home/atom/Targets/at0m_b0mb_W7/exploit] generic_send_tcp 192.168.222.146 9999 rtime.spk 0 0 148 × 1 © Total Number of Strings is 681 Fuzzing Variable 0:0 line read=Welcome to Vulnerable Server! Enter HELP for help. Fuzzing Variable 0:1 Variablesize= 5004 Fuzzing Variable 0:2 Variablesize= 5005 Fuzzing Variable 0:3 Variablesize= 21 Fuzzing Variable 0:4 Variablesize= 3 Fuzzing Variable 0:5 Variablesize= 2 Fuzzing Variable 0:6 Variablesize= 7 Fuzzing Variable 0:7 line read=Welcome to Vulnerable Server! Enter HELP for help.

• It also didnt break the application

• Lets use the similar syntax and check what happens!

Now trying Itime function

Now lets move on to srunCode for srun:-

Now lets try trun:-

• Code for trun.spk

• Code for spk file:-

s readline();

s_readline();

s_readline();

Now lets start the exploit:-

s_string("TRUN")

s_string_variable("0");

s_string("SRUN")

s_string_variable("0");Lets run it and see what happens:-Nothing happened

s_string("LTIME ")

Nothing happened

s_string_variable("0");

★4. Exploit Development Section