The Story of PORT 445

HackersVilla
CYBERSECURITY PVT LTD

whoami

With over 4-5 years of Practical experience in the field, I have good knowledge of Bug Hunting and PenTesting, especially System Hacking.

*Co-Founder of **HackersVilla CyberSecurity Pvt Ltd**, a community where youth can learn and earn.*

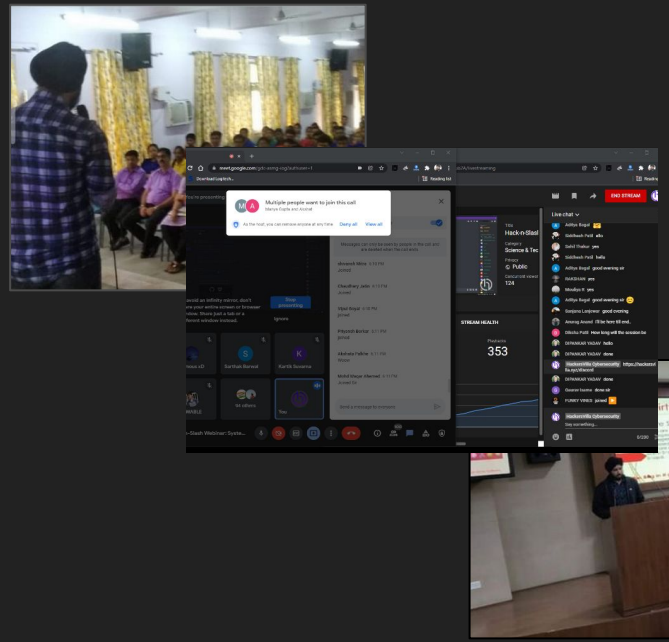
SANCHAY SINGH

CYBERSECURITY EXPERT & TRAINER

HackersVilla
CYBERSECURITY PVT LTD

whoami

I have trained over 300+ Students in last 5 years and have conducted more than 100 Sessions (with 12,000+ Participants) on various fields of cybersecurity in last 6 months.



sanchayofficial

@sanchayofficial

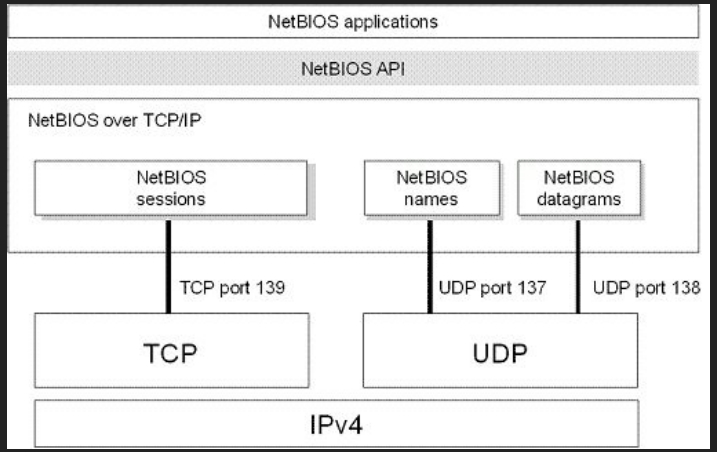
sanchayofficial@gmail.com

LIVE ATTACK

Let’s have a look at our TOC

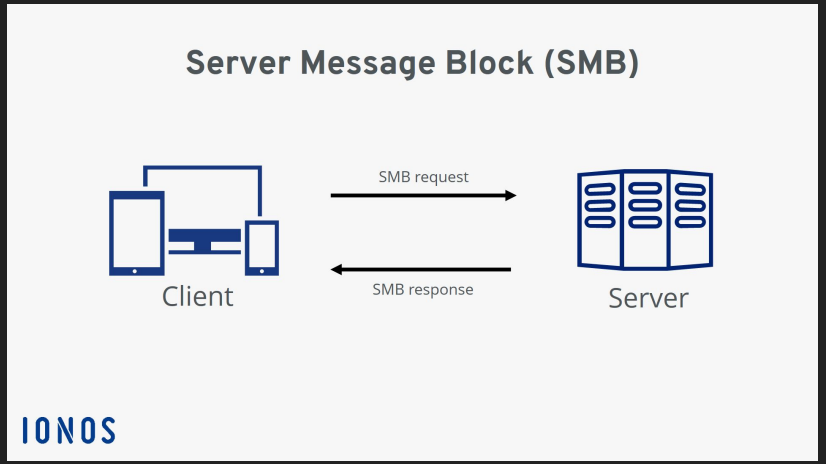
What is NetBIOS?

- *NetBIOS provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a LAN.*
- *As strictly an API, NetBIOS is not a networking protocol.*



What is SMB?

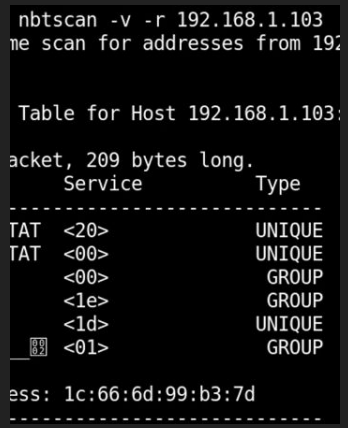
- ***Server Message Block*** *is a communication protocol that Microsoft created for providing shared access to files and printers across nodes on a network.*
- *It also provides an authenticated inter-process communication mechanism.*

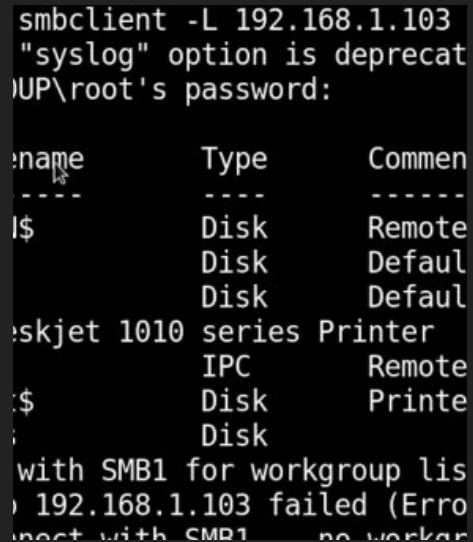


Source: https://www.ionos.com

Enumeration

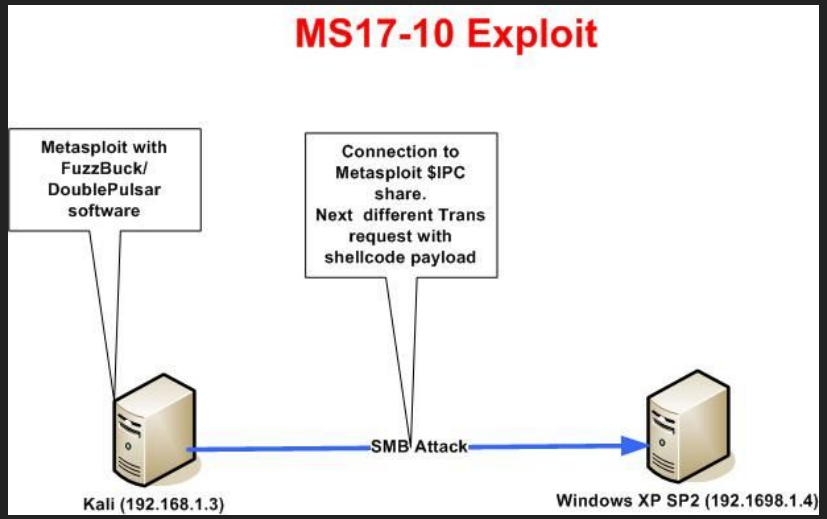
- *Enumerating users for NetBIOS (nbtstat)*
- *Enumerating authentication and null sessions (smbclient)*





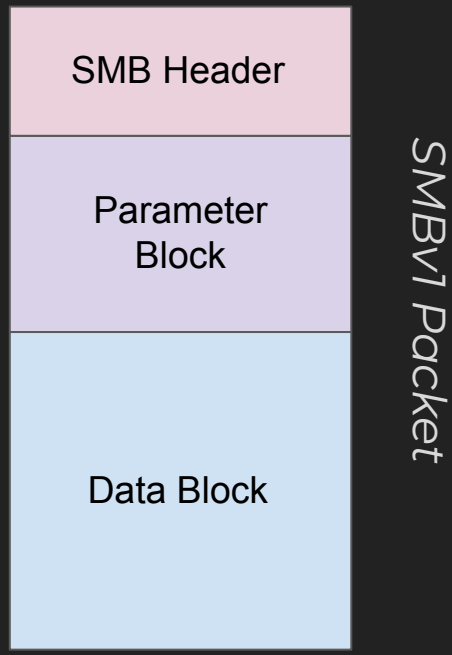
MS17_010_EternalBlue

- *Leaked by Shadow Brokers, this is an exploit that corrupts the core using a powerful buffer overflow attack.*
- *It is well laid-out for overwriting the SMB v1.0 Buffer.*



Let us dive into the **Exploit**

- *EternalBlue exploits 3 bugs to achieve RCE:*
  - *Wrong Casting Bug*
  - *Wrong Parsing Function Bug*
  - *Non-Paged Pool Allocation Bug*



WRONG CASTING BUG

Windows Data Types

- *WORD* → *2 bytes*
- *DWORD* → *4 bytes*
- *QWORD* → *8 bytes*

Extended Attributes

- **MetaData attached to files**
  - *Key/Value Pair*
- **OS/2**
  - *Joint Microsoft/IBM OS*
  - *EA concept introduced*
- **Windows NT**
  - *OS for Workstations & Servers*
  - *NTFS & WSL Support*
  - *EA for file permissions and case sensitivity*

```
SMB_FEA_LIST
{
    ULONG SizeOfListInBytes;
    UCHAR FEAList[size];
}
```

FEALIST structure

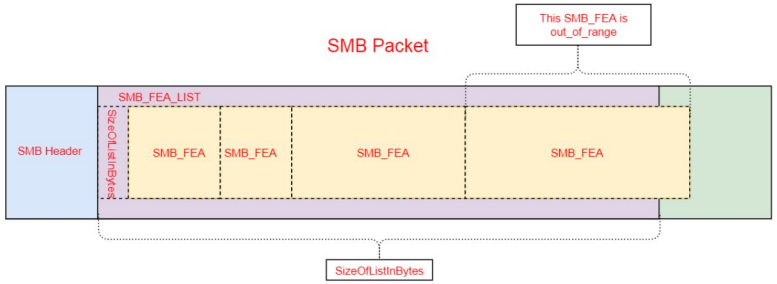
```
struct Os2Fea{
    UCHAR   ExtendedAttributeFlag; // Flags
    UCHAR   AttributeNameLengthInBytes; // Length of the AttributeName field
    USHORT  AttributeValueLengthInBytes; // Length of the AttributeValue field
    UCHAR   AttributeName[AttributeNameLengthInBytes + 1]; // Extended attribute name
    UCHAR   AttributeValue [AttributeValueLengthInBytes]; // Extended attribute value
}

struct Os2FeaList{
    ULONG   SizeOfListInBytes; // The total size of the FeaRecords + 4 bytes
    UCHAR   Os2FeaRecords[SizeOfListInBytes-4];// A concatenated list of Os2Fea
}
```

```
struct NtFeaList{
  ULONG  NextEntryOffset; // offset to the next NtFea record of NtFeaList type
  UCHAR  Flags;
  UCHAR  NtFeaNameLength;
  USHORT NtFeaValueLength;
  CHAR   NtFeaName[NtFeaNameLength];
  CHAR   NtFeaValue[NtFeaValueLength];
}
```

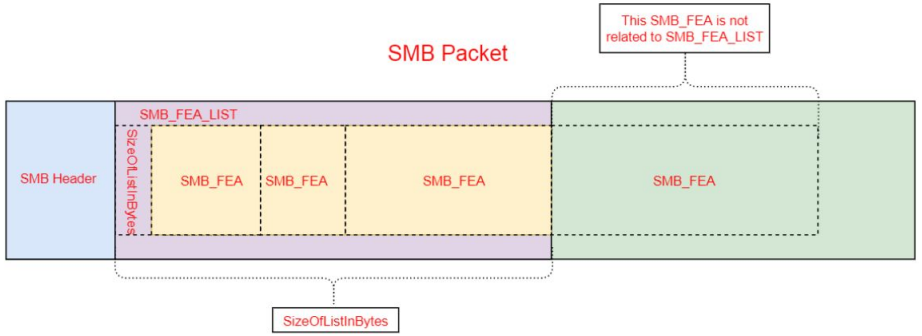
Exploitation

- Set the size for *SizeOfListInBytes* as **0x10000**.
- Although *SizeOfListInBytes* is **DWORD** but while shrinking, it is treated as a **WORD** and updates only the 2 Least Significant Bytes.
- Craft SMB_FEA structures such that the size is **more than 2^16**.
- Due to wrong casting, instead of shrinking the *SizeOfListInBytes* to correct size, it **enlarges** causing Out of Bound write.

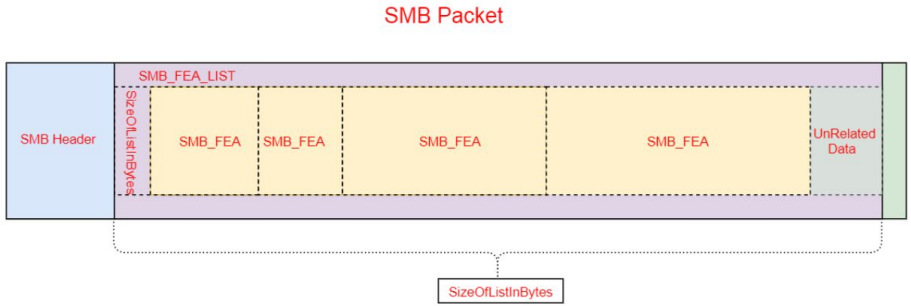
Before Shrinking:



After Shrinking: if the size of `SizeOfListInBytes` is below 2^{16}:



After Shrinking (bug): if the size of `SizeOfListInBytes` is above 2^{16}:



WRONG PARSING FUNCTION BUG

SMB Transactions

- Transaction messages of Interest:
  - SMB_COM_TRANSACTION2 or Trans2 (*WORD Size)*
  - SMB_COM_TRANSACT or NT Trans (*DWORD Size)*
- Each sub-command has a corresponding sub-command *_SECONDARY*.
- *_SECONDARY* is used when data is too big for single packet

Exploitation

- Difference in amount of maximum data between Trans2 and NT Trans.
- Parsing is according to last transaction type. No validation which for which function started the transaction.
- Possible to send NT Trans followed by Trans2_SECONDARY
- Leads to previous bug by treating DWORD as WORD since both different transaction data are parsed incorrectly.

NON PAGED POOL ALLOCATION BUG

Session Setup Allocation Error

- Two ways to login in SMB
  - NT Security & Extended Security
- Certain flag values can confuse it
  - Can reserve large memory
- Free on Demand
  - Close Client socket

Exploitation

- Begin User Authentication on an SMB Connection and establish the SMB Session by sending request: *SMB_COM_SESSION_SETUP_ANDX*
- The request is split in 2 section- *SMB_Parameters* & *SMB_Data*
- The server accepts and does an integrity check.
- Bug is in the extraction of SMB_Data performed by the function- *BlockingSessionSetupAndX*
- The bug allows to send a small packet and leads to a big allocation in the non-paged pool.

Variations & Impacts

- *Eternal Romance*
- *Eternal Champion*
- *Eternal Rocks*
- *Eternal Synergy*

- *WannaCry*
- *Petya (2016)*
- *Non Petya*
- *Bad Rabbit*
- *Olympic Destroyer*
- *Baltimore Ransomware*

DOUBLE CHECK YOUR 445 😉

Bibliography

- https://research.checkpoint.com/2017/eternalblue-everything-know/amp/
- https://www.thewindowsclub.com/smb-port-what-is-port-445-port-139-used-for
- https://www.slideshare.net/kandelrc/eternal-blue-vulnerability
- https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/81e15dee-8fb6-4102-8644-7eaa7ded63f7?redirectedfrom=MSDN
- https://en.wikipedia.org/wiki/Server_Message_Block