

# Cracking NTLMv2 Authentication

Urity@SecurityFriday.com



# NTLM version 2

- in Microsoft Knowledge Base -

“Microsoft has developed an enhancement, called NTLM version 2, that significantly improves both the authentication and session security mechanisms.”

“For NTLMv2, the key space for password-derived keys is 128 bits. This makes a brute force search infeasible, even with hardware accelerators, if the password is strong enough.”

# Windows authentications for network logons

- LAN Manager (LM) challenge/response
- Windows NT challenge/response  
(also known as NTLM version 1)
- NTLM version 2 challenge/response
- Kerberos

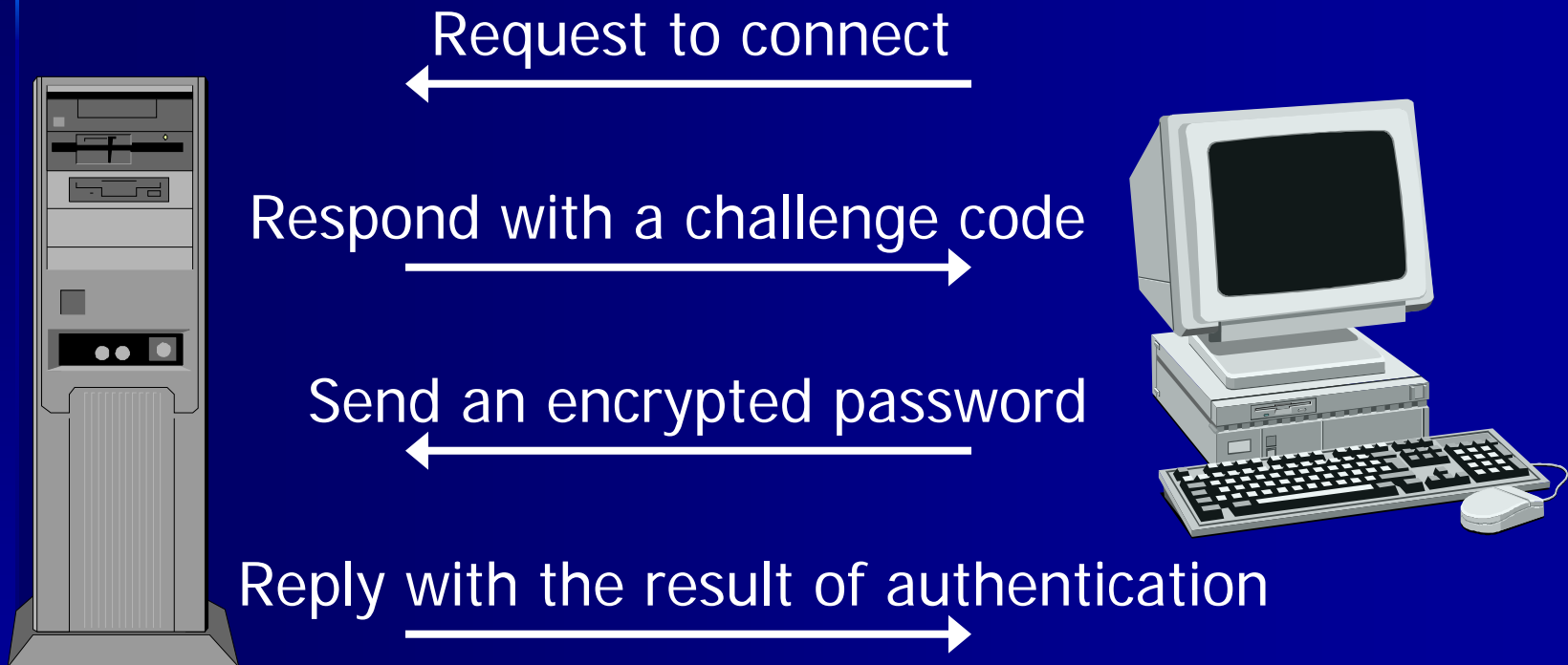
# Agenda

1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

# Agenda

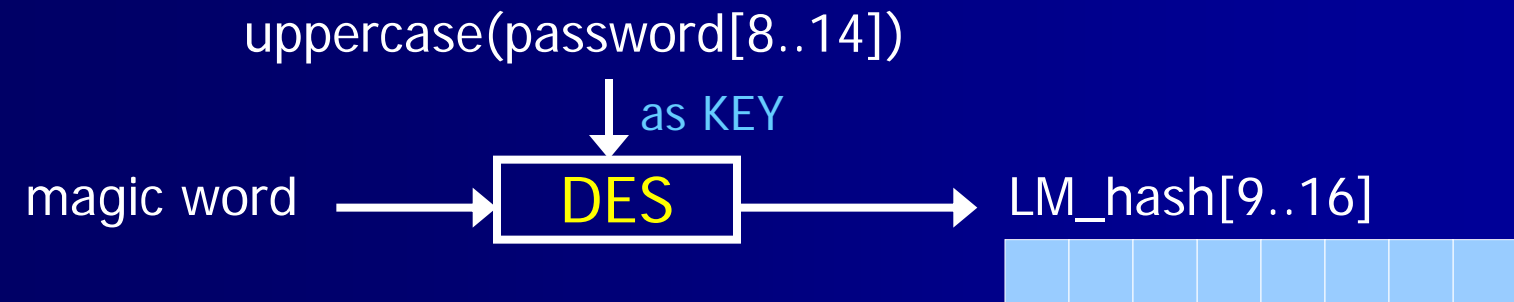
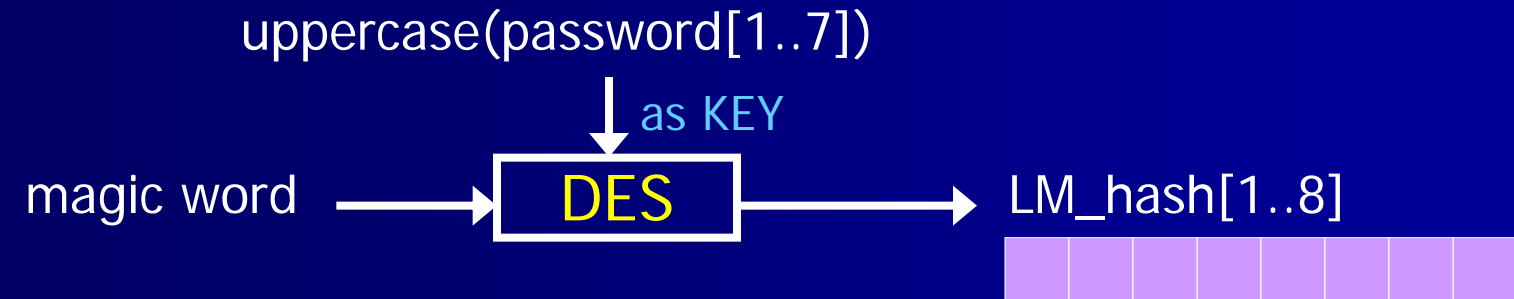
1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

# Challenge/Response sequence



# LM challenge/response

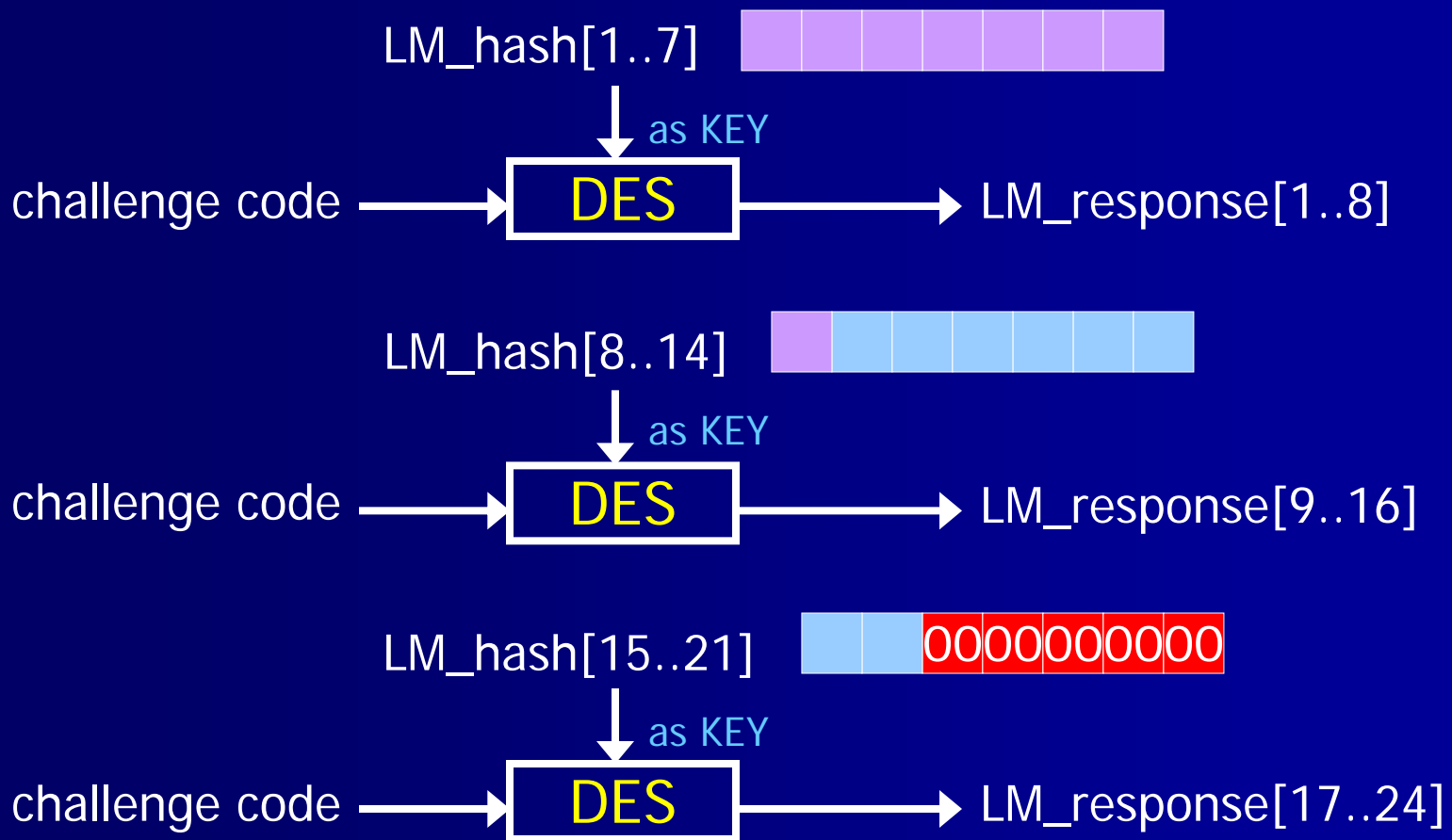
- 1 -



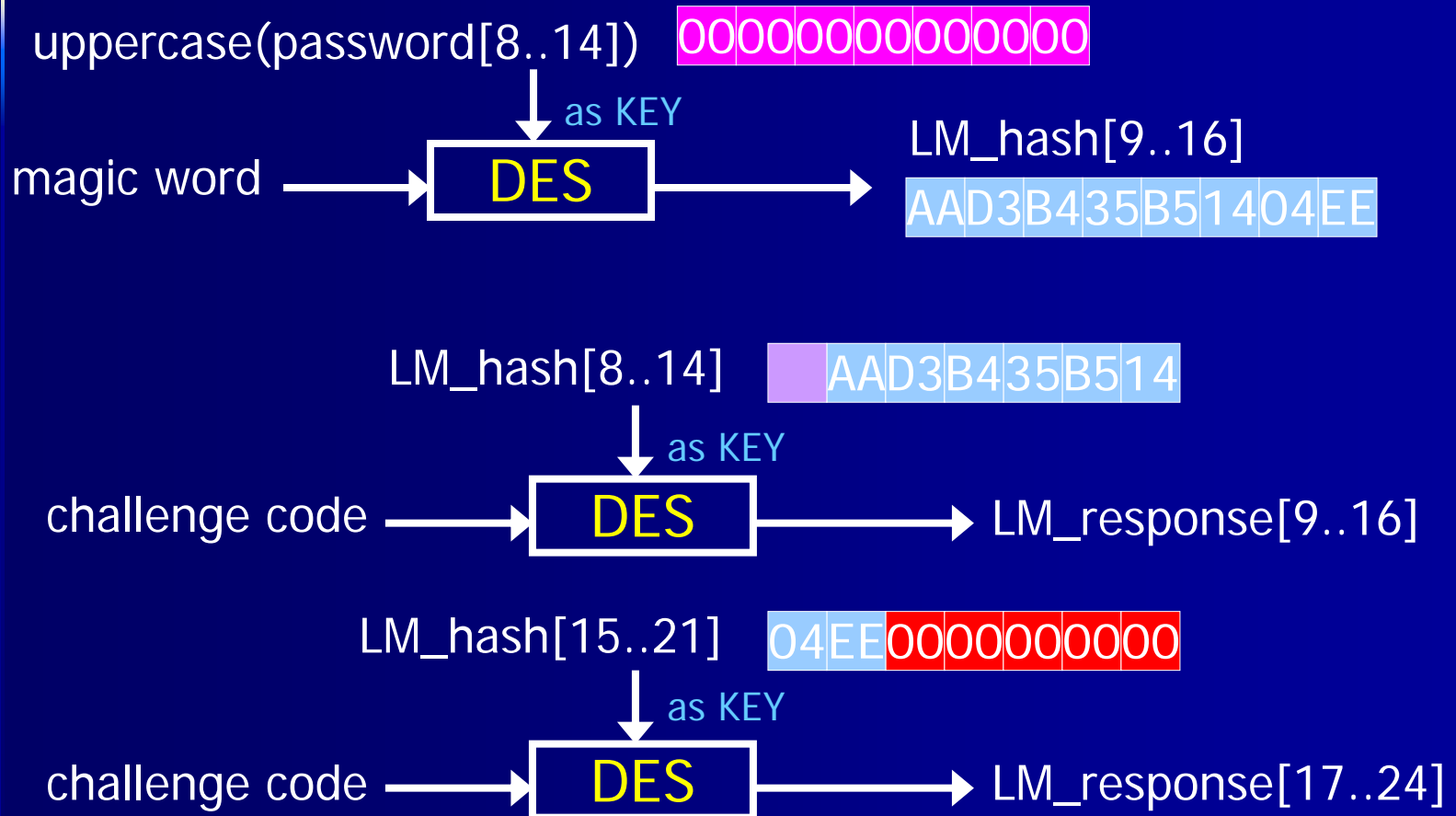
magic word is "KGS!@#\$%" ←

# LM challenge/response

- 2 -



# Password Less than 8 Characters



# BeatLM demonstration

- check the password less than 8
- 1000 authentication data in our office

# Weakness of LM & NTLMv1

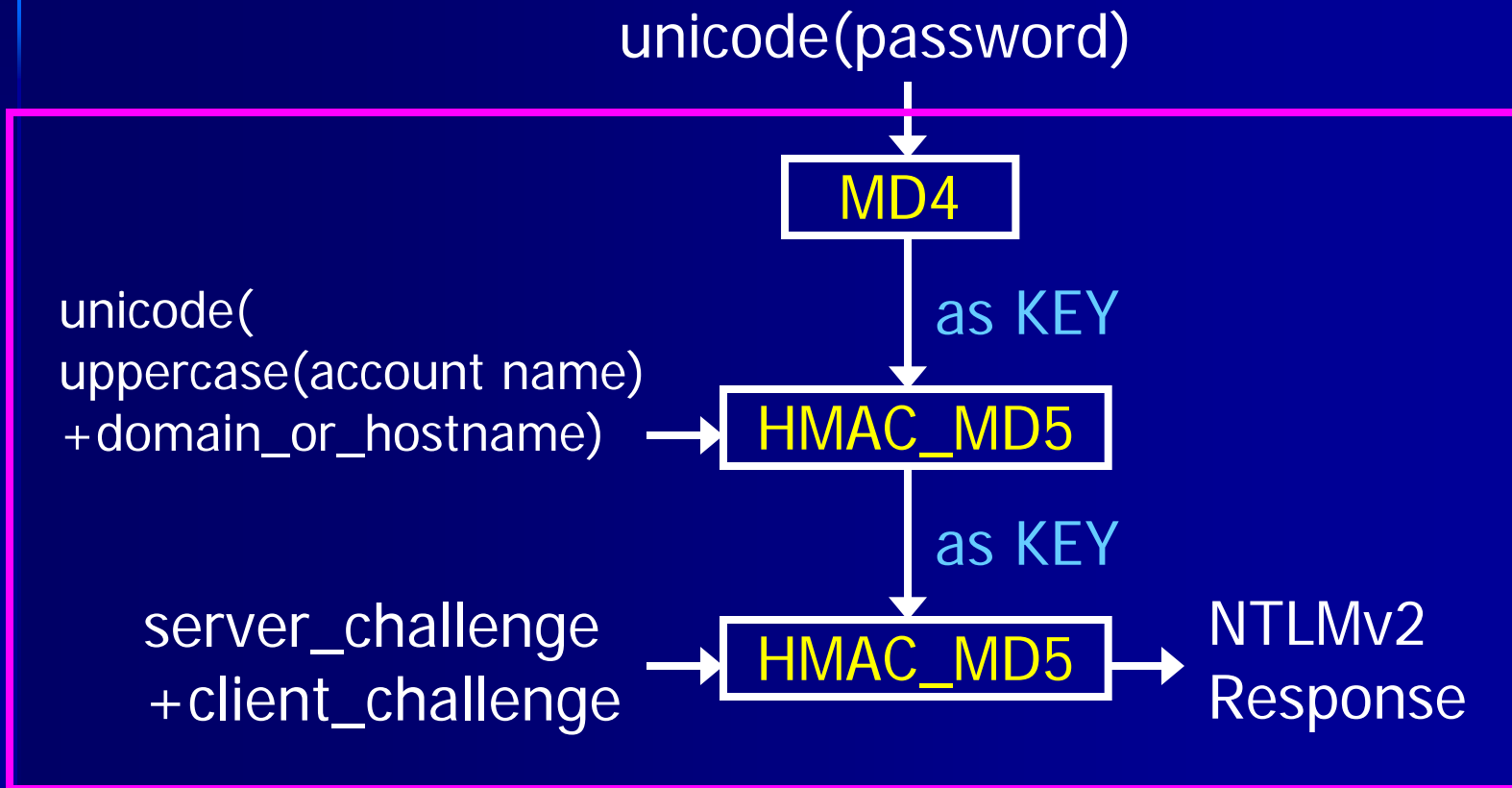
See:

- [Hacking Exposed Windows 2000](#)
- [Microsoft Knowledge Base: Q147706](#)
- [L0phtcrack documentation](#)

# Agenda

1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

# NTLM 2 Authentication



# NTLMv2 more info

- algorithm & how to enable -

- HMAC: RFC2104
- MD5: RFC1321
- MD4: RFC1320
- Microsoft Knowledge Base: Q239869

# LM, NTLMv1, NTLMv2

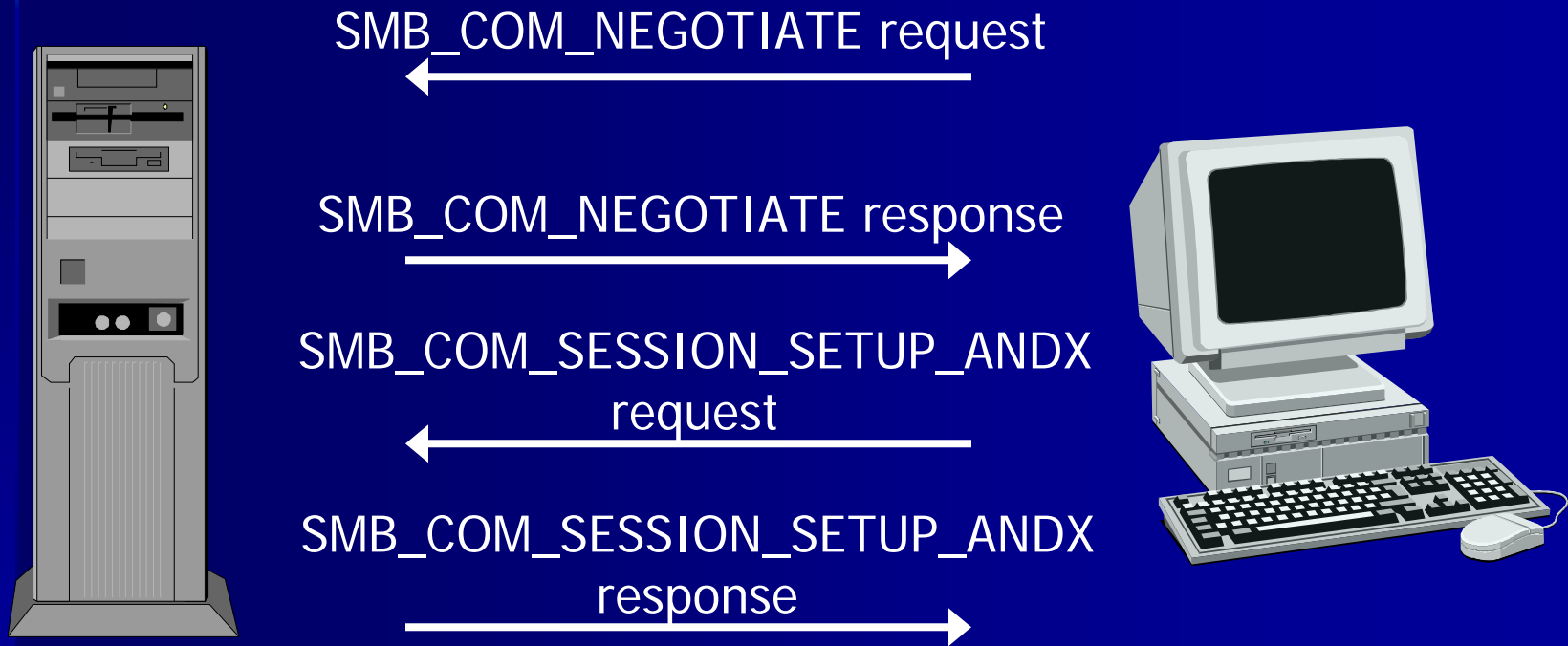
	LM	NTLMv1	NTLMv2
Password case sensitive	No	Yes	Yes
Hash key length	56bit + 56bit	-	-
Password hash algorithm	DES (ECB mode)	MD4	MD4
Hash value length	64bit + 64bit	128bit	128bit
C/R key length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit
C/R algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5
C/R value length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit

# Agenda

1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

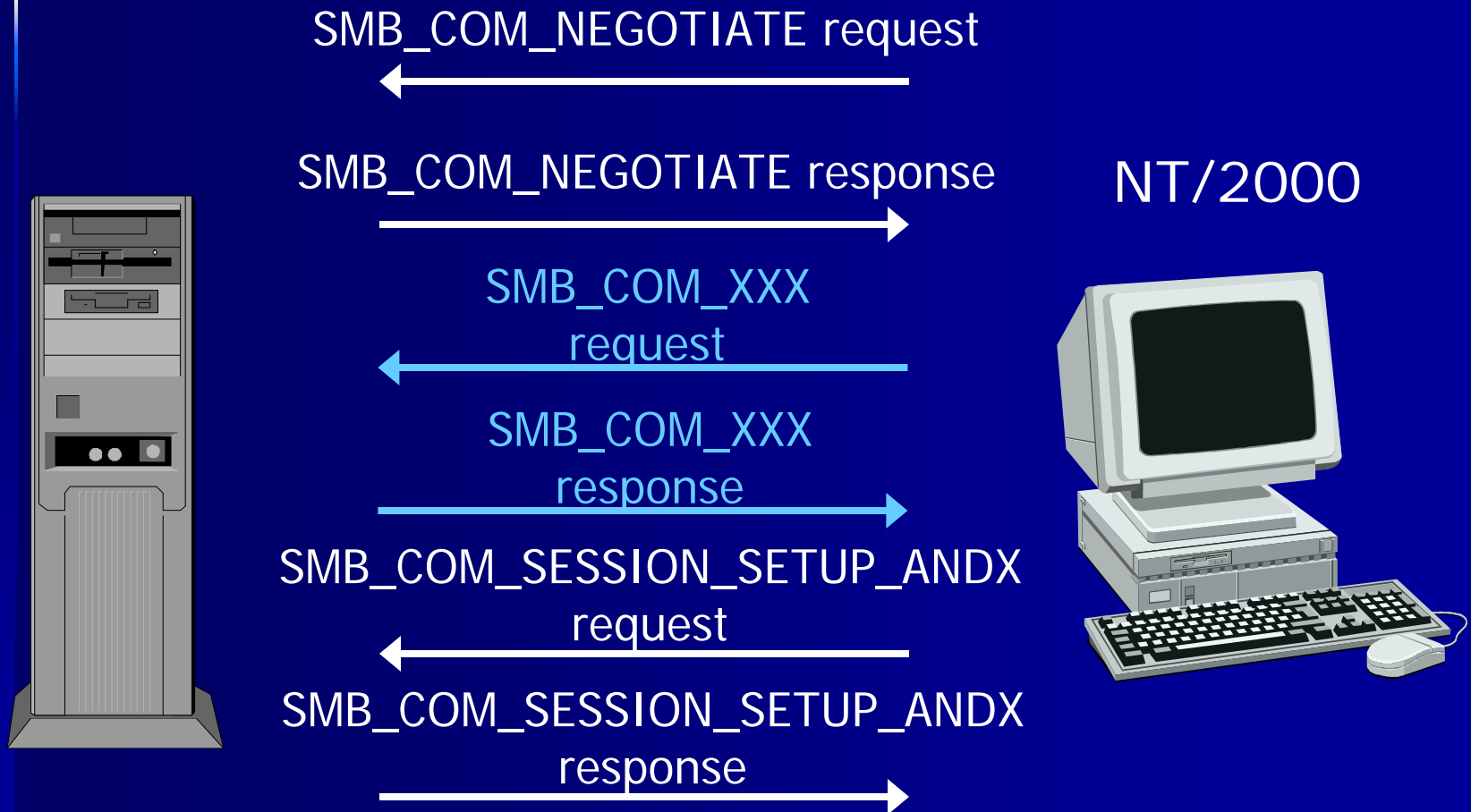
# Authentication sequence

- NetBT (NetBIOS over TCP/IP) -



# Extra SMB commands

- NetBT (NetBIOS over TCP/IP) -

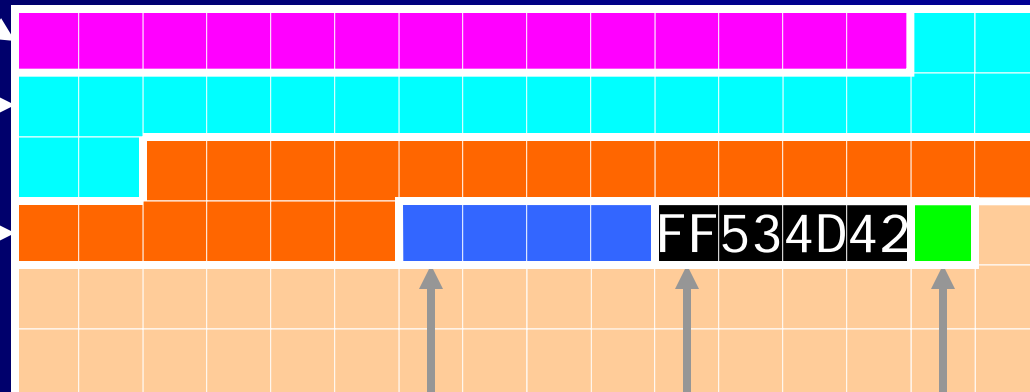


# Authentication packet header

Ethernet

IP

TCP



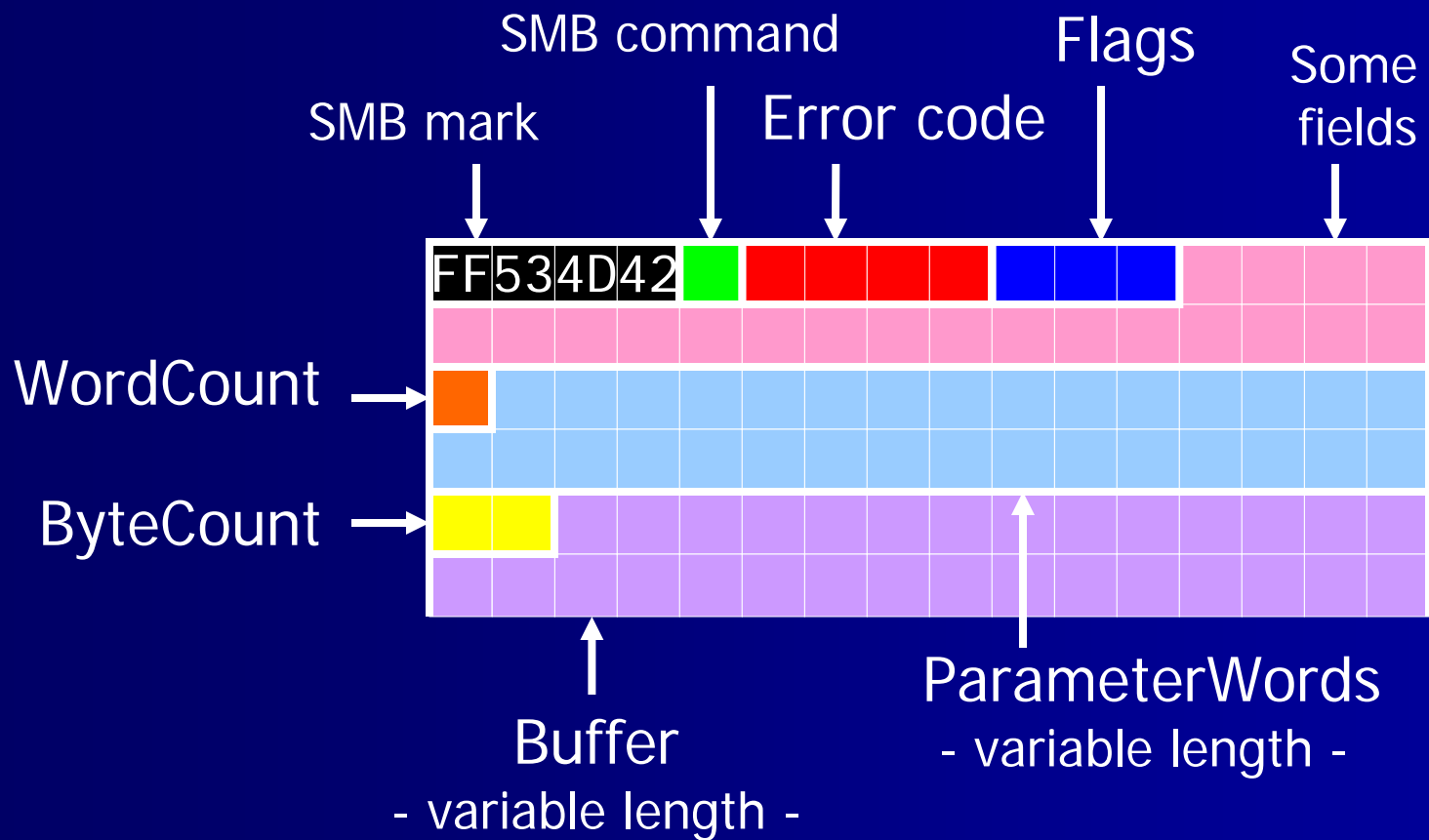
SMB block size

SMB command

SMB mark: 0xFF, 0x53, 0x4D, 0x42

'S' 'M' 'B'

# SMB general header structure



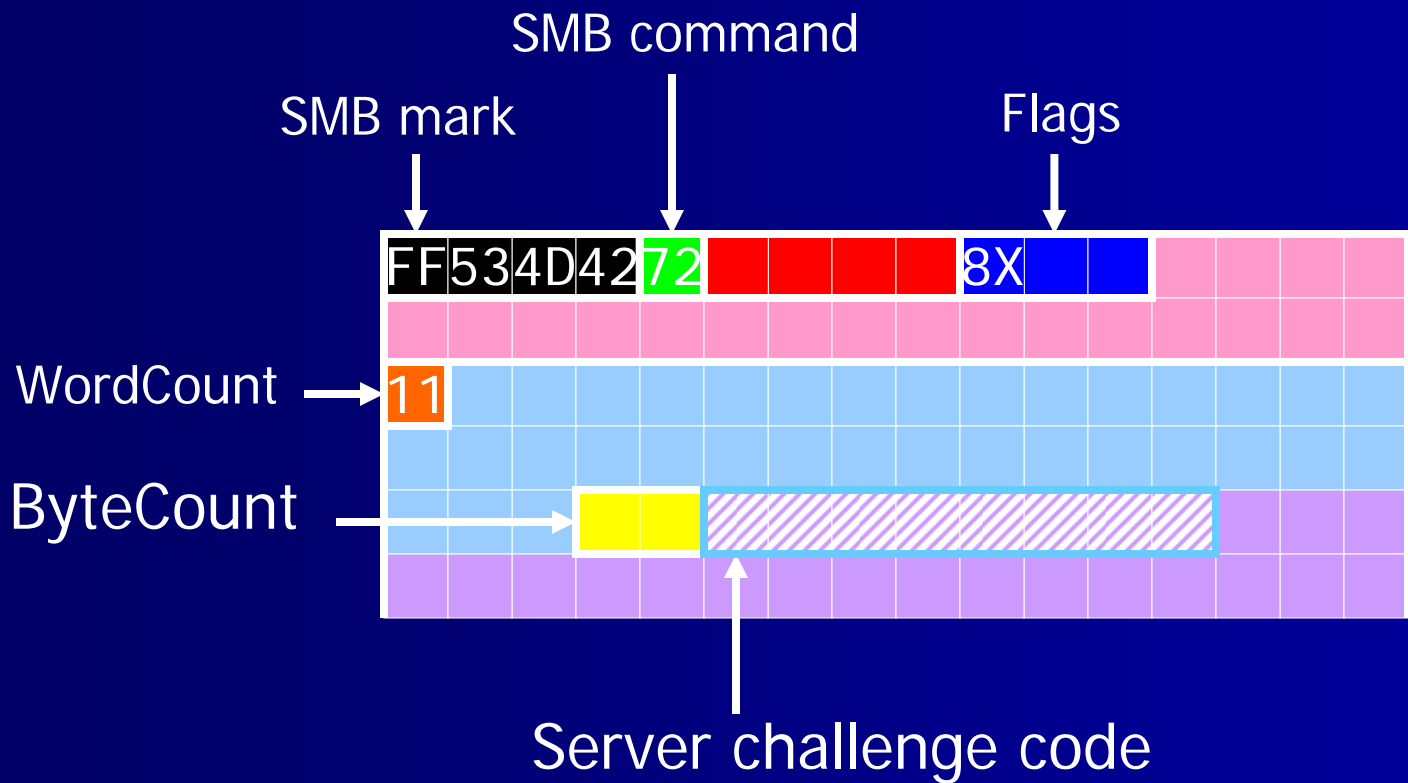
# SMB\_COM\_NEGOTIATE request over NetBT

- SMB command: 0x72
- WordCount: 0x00

# SMB\_COM\_NEGOTIATE response over NetBT

- SMB command: 0x72
- Flags
  - Server response bit: on
- WordCount: 0x11
- Buffer contains
  - Server challenge code: 8 bytes

# Server challenge code

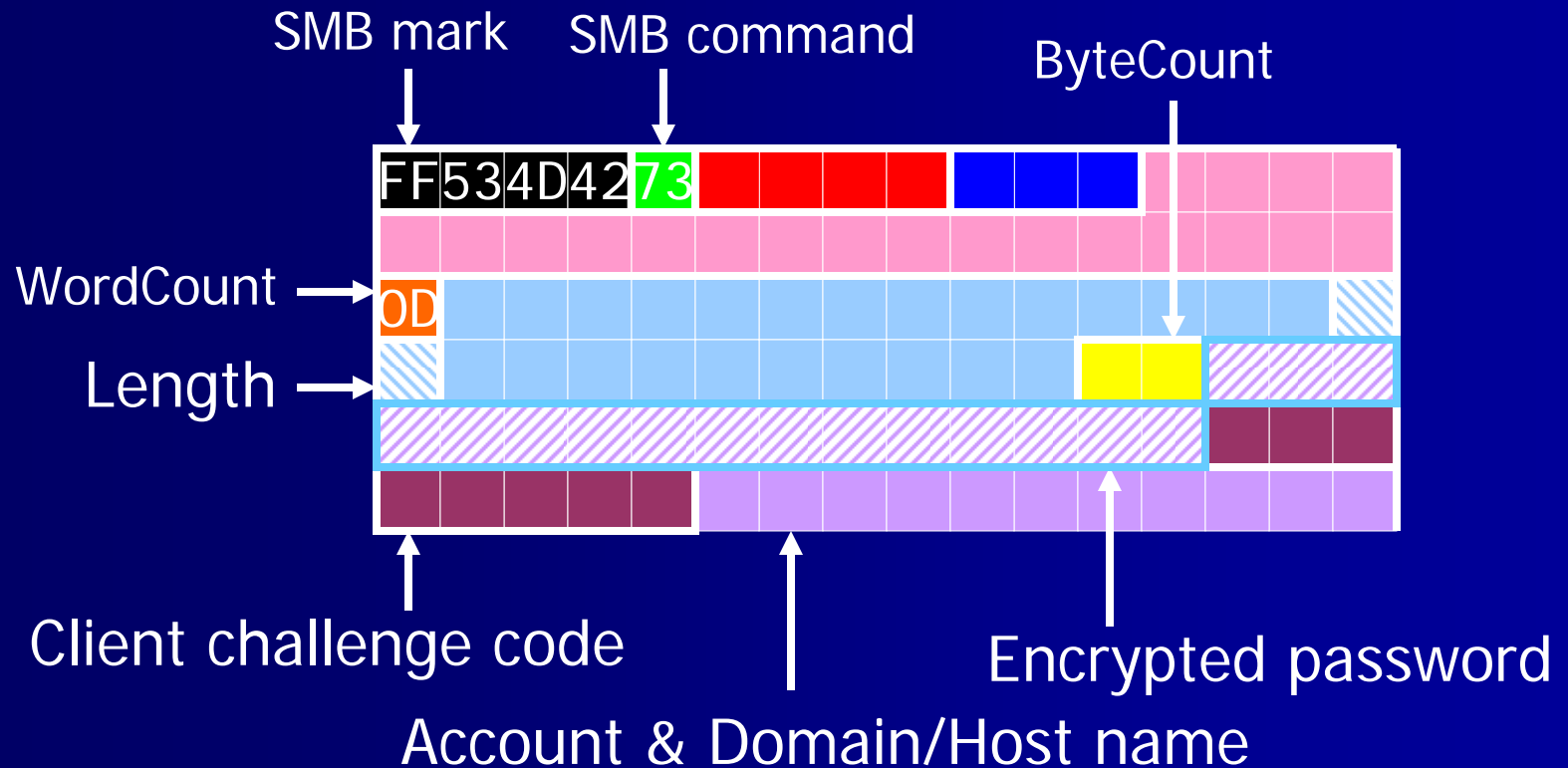


# SMB\_COM\_SESSION\_SETUP\_ANDX

request over NetBT

- SMB command: 0x73
- WordCount: 0x0D
- Buffer contains
  - Encrypted password: 16 bytes
  - Client challenge code: 8 bytes
  - Account name
  - Domain/Workgroup/Host name

# Encrypted password



If client challenge code = 0x0000000000000000 then DS client

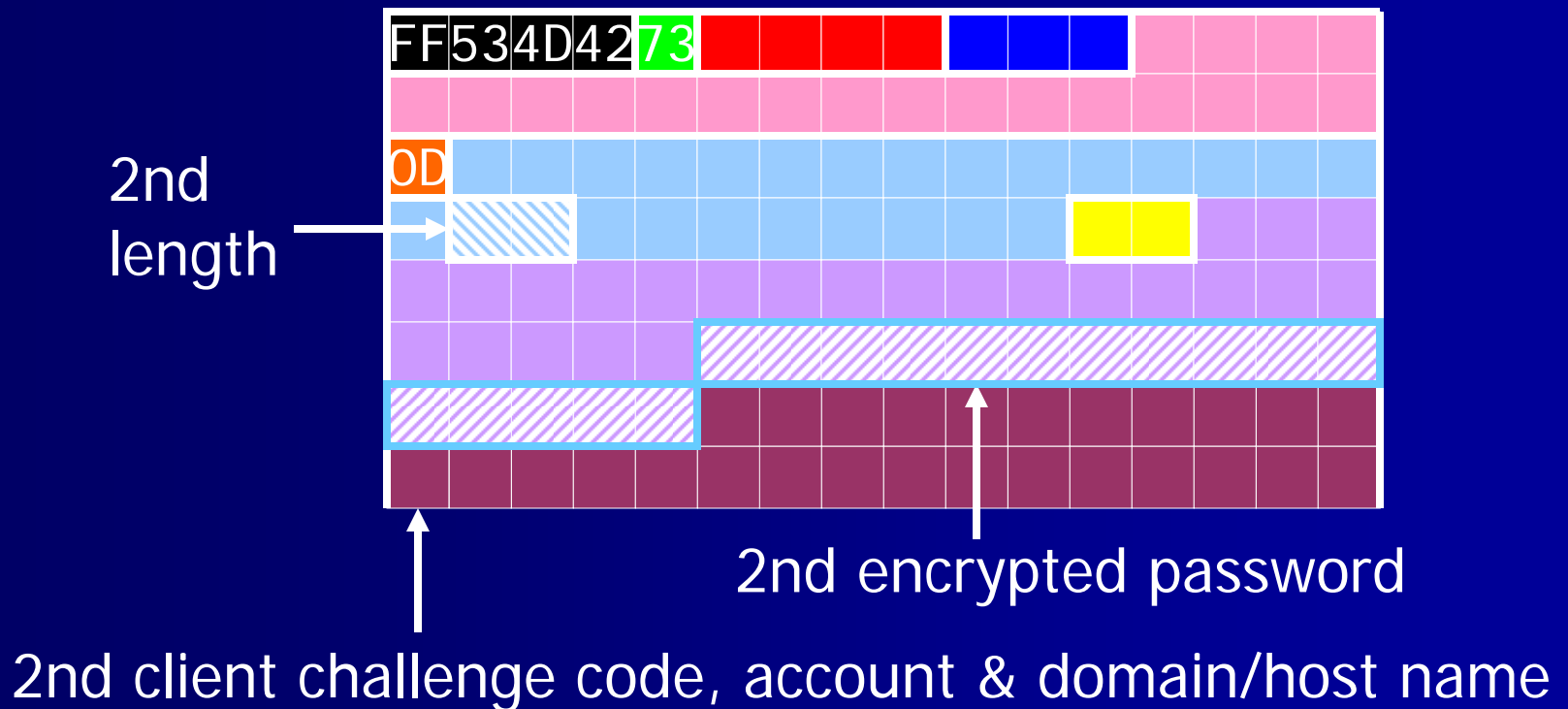
# 2nd encrypted password

- 1 -

- NT/2000 transmits two types encrypted password
- 2nd client challenge code has variable length

# 2nd encrypted password

- 2 -



# SMB\_COM\_SESSION\_SETUP\_ANDX response over NetBT

- SMB command: 0x73
- Error code
- WordCount: 0x03

# Error code

- correct password -

- 0xC000006F
  - The user is not allowed to log on at this time.
- 0xC0000070
  - The user is not allowed to log on from this workstation.
- 0xC0000071
  - The password of this user has expired.
- 0xC0000072
  - Account currently disabled.
- 0xC0000193
  - This user account has expired.
- 0xC0000224
  - The user's password must be changed before logging on the first time.

# Requisite information

- Account name
- Domain/Workgroup/Host name
- Server challenge code
- Client challenge code
- Encrypted password
- The result of authentication

# SMB protocol

- specifications -

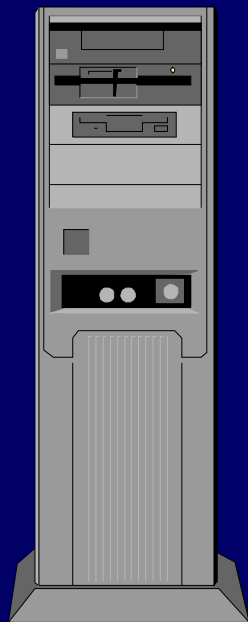
Please check out:

- <ftp.microsoft.com/developr/drg/cifs>
- DCE/RPC over SMB (ISBN 1-57870-150-3)
- [www.samba.org/cifs/docs/what-is-smb.html](http://www.samba.org/cifs/docs/what-is-smb.html)

# Win 98/ME file sharing

- encrypted password -

98/ME file sharing



SMB\_COM\_NEGOTIATE request



SMB\_COM\_NEGOTIATE response



SMB\_COM\_SESSION\_SETUP\_ANDX request



**not NTLMv2**

SMB\_COM\_SESSION\_SETUP\_ANDX response



98/ME with DS Client

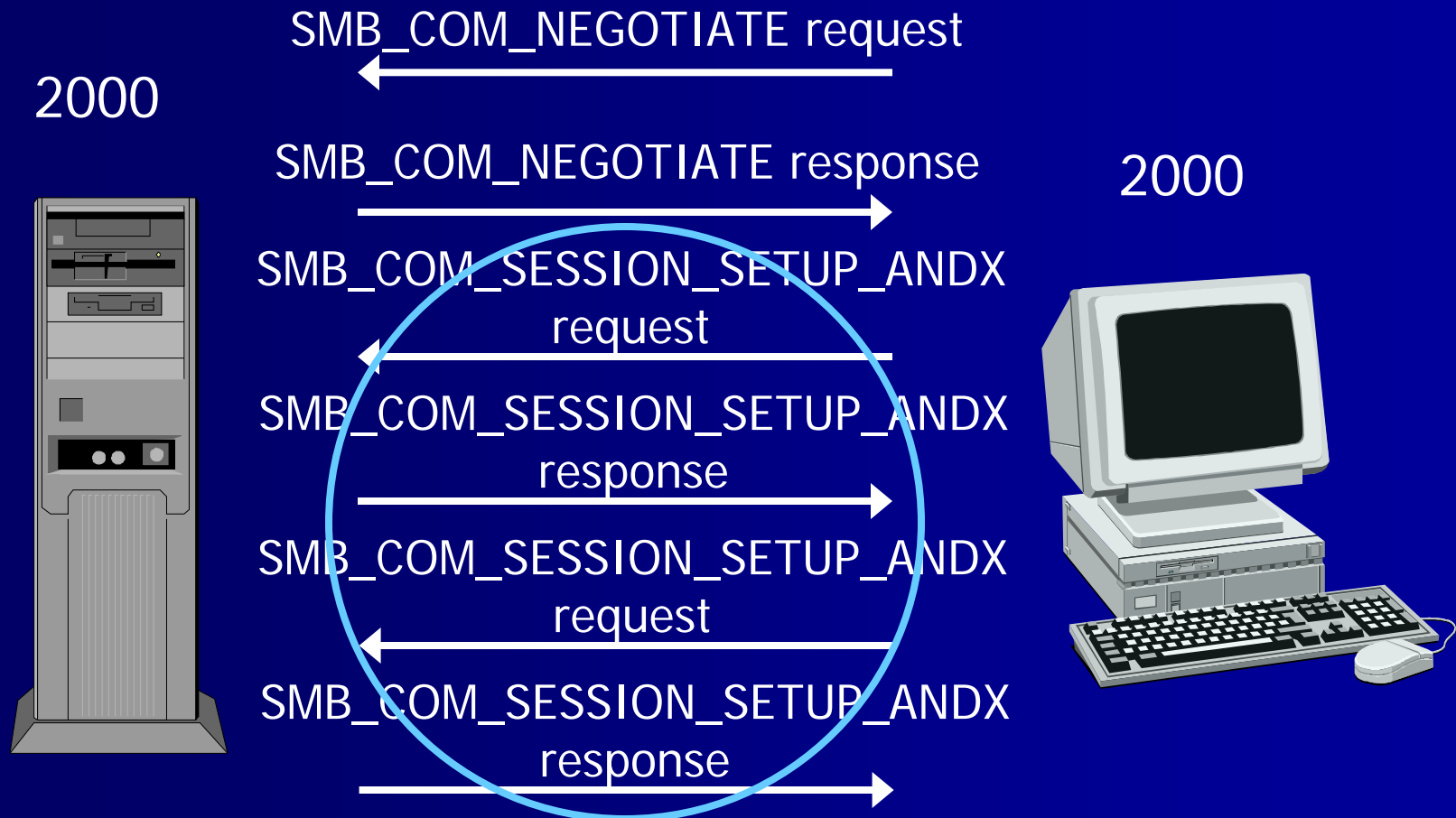


# Agenda

1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

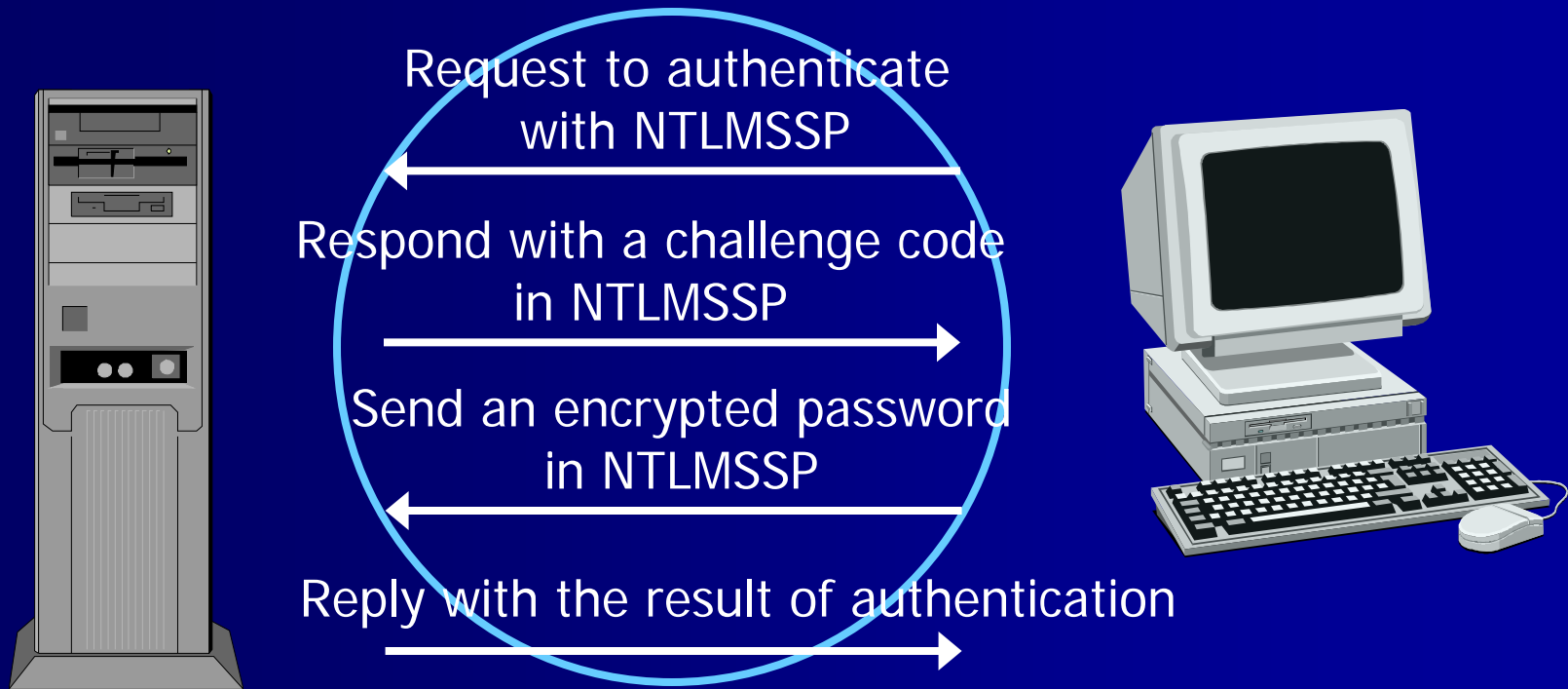
# Authentication sequence

- MS-DS (Direct SMB Hosting Service) -



# Challenge/Response

- MS-DS (Direct SMB Hosting Service) -



# 1st SMB\_COM\_SESSION\_SETUP\_ANDX request over MS-DS

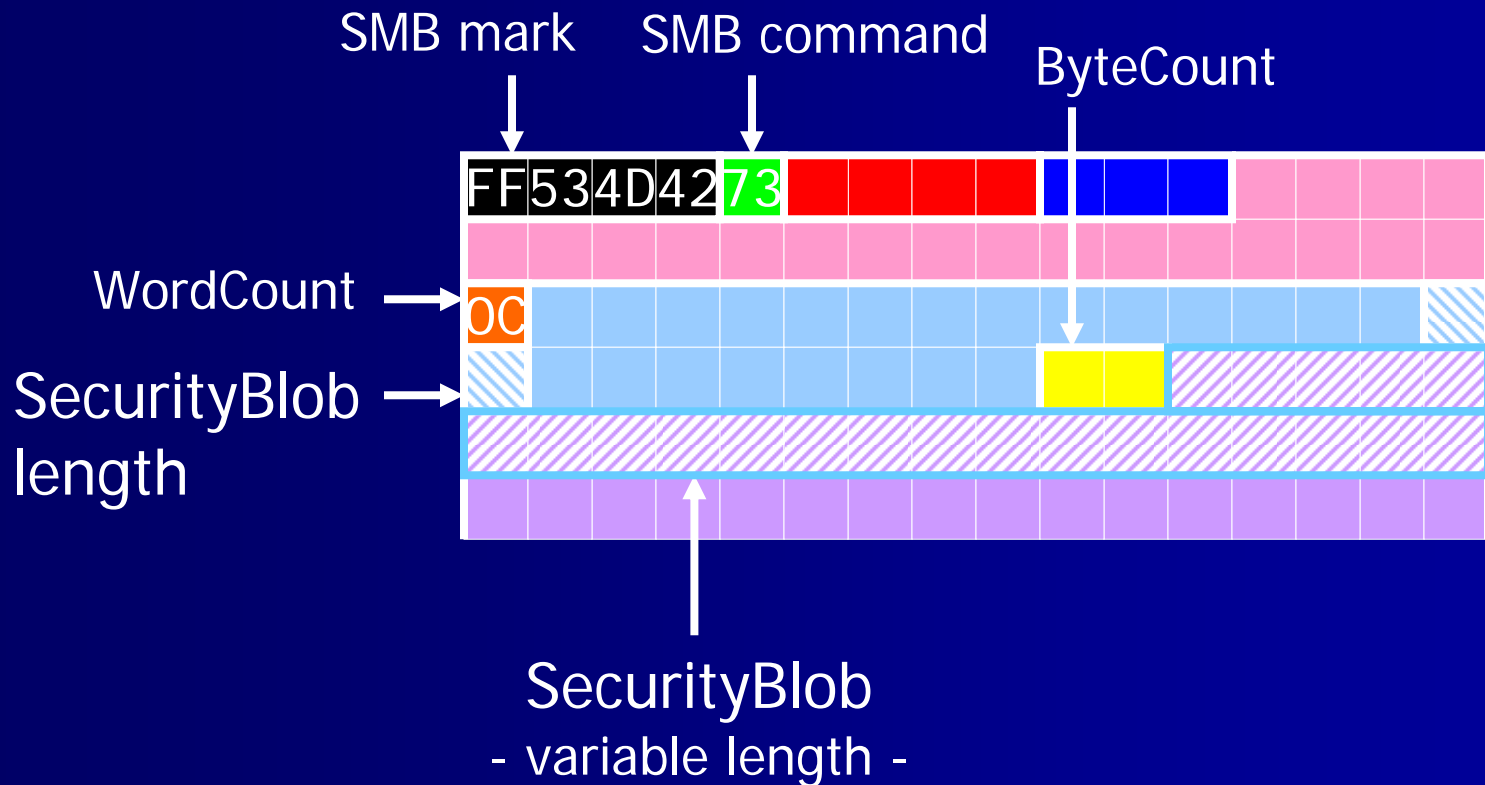
- WordCount: 0x0C
- Buffer contains
  - SecurityBlob

# SMB\_COM\_SESSION\_SETUP\_ANDX

- WordCount -

- Type 3 has
  - OS name, LM type, Domain name
- Type 4 has
  - SecurityBlob, OS name, LM type, Domain name
- Type 12 has
  - SecurityBlob, OS name, LM type
- Type 13 has
  - Password, Account name, Domain name, OS name, LM type

# SMB\_COM\_SESSION\_SETUP\_ANDX command - Type 12 (0x0C)



# NTLMSSP 1 in SecurityBlob

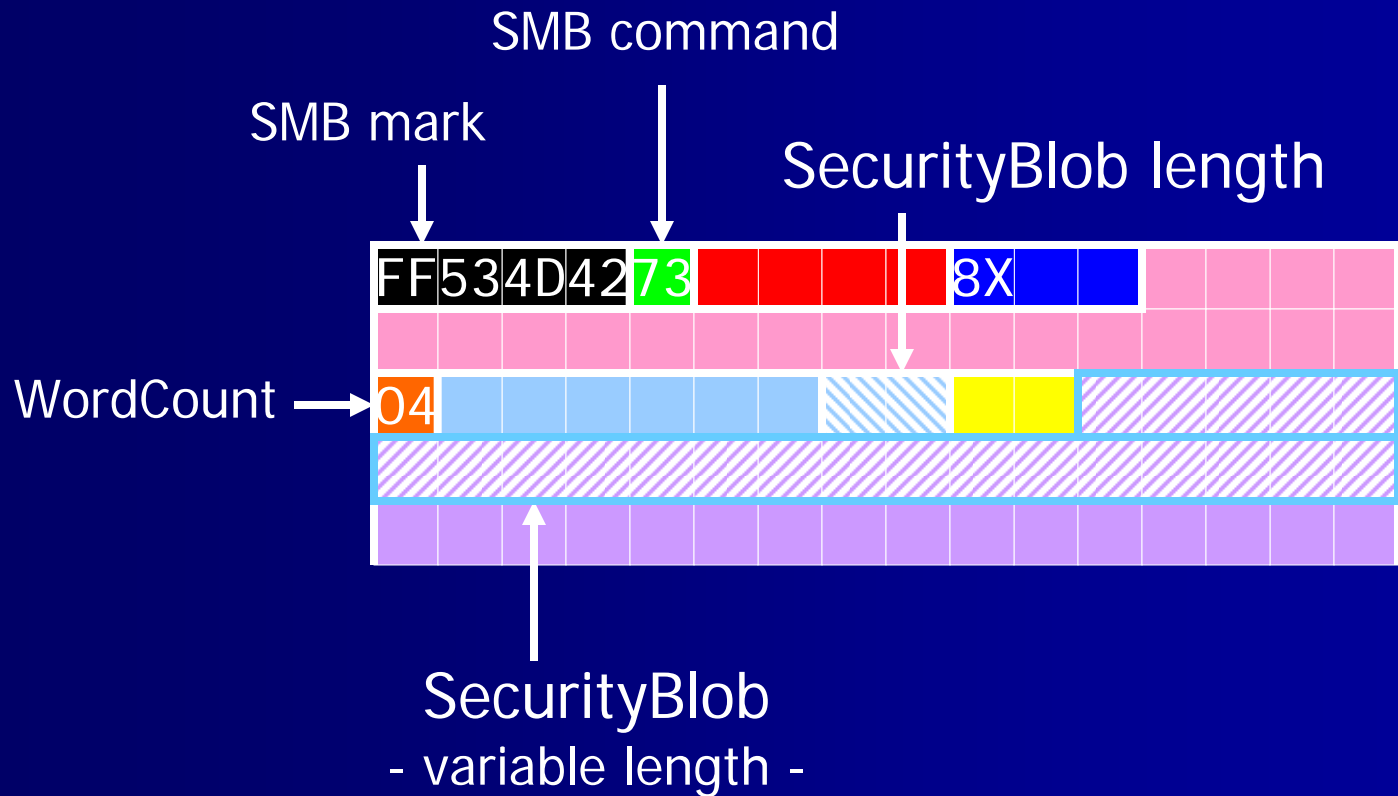
4E	54	4C	4D	53	53	50	00
01	00	00	00				
00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00

- NTLMSSP mark: 8-byte ASCII string
- 1: 4-byte little-endian
- Unknown flags: 4bytes
- (If any) Domain/Workgroup name length: 2-byte little-endian \* 2
- (If any) Domain/Workgroup name offset: 4-byte little-endian
- (If any) Host name length: 2-byte little-endian \* 2
- (If any) Host name offset: 4-byte little-endian
- (If any) Host name & Domain/Workgroup name

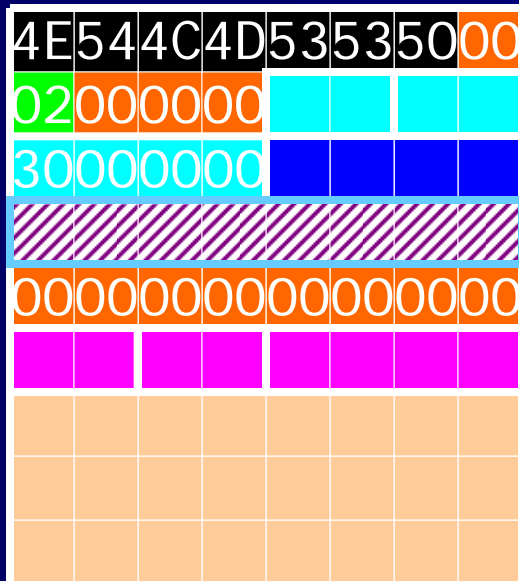
# 1st SMB\_COM\_SESSION\_SETUP\_ANDX response over MS-DS

- WordCount: 0x04
- Buffer contains
  - SecurityBlob

# SMB\_COM\_SESSION\_SETUP\_ANDX command - Type 4 (0x04)



# NTLMSSP 2 in SecurityBlob

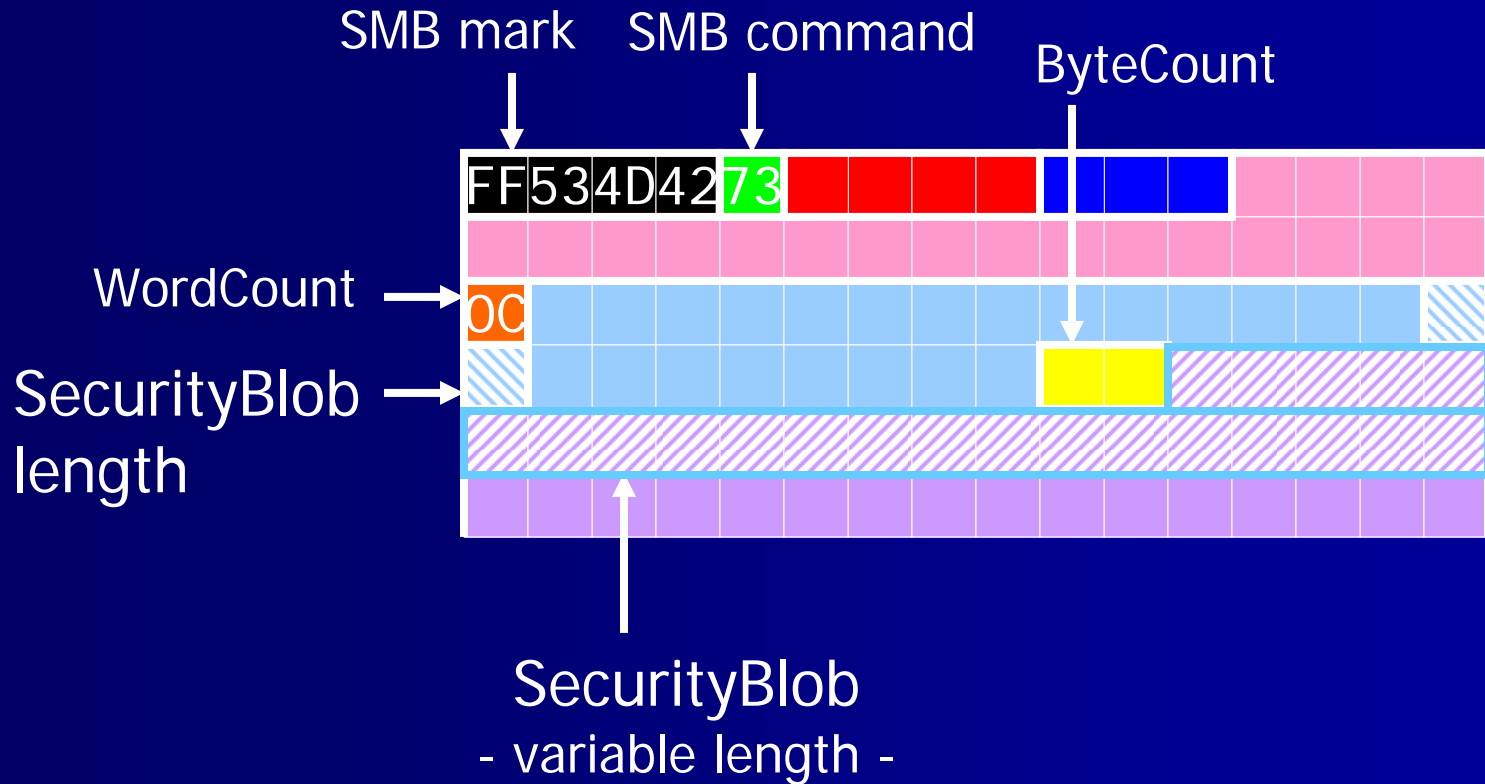


- NTLMSSP mark: 8-byte ASCII string
- 2: 4-byte little-endian
- Host name length: 2-byte little-endian \* 2
- Host name offset: 4-byte little-endian
- Unknown flags: 4bytes
- Server challenge code: 8bytes
- 8-byte zero
- Host & Domain name length: 2-byte little-endian
- Host & Domain name offset: 4-byte little-endian
- Host name & Domain name

# 2nd SMB\_COM\_SESSION\_SETUP\_ANDX request over MS-DS

- WordCount: 0x0C
- Buffer contains
  - SecurityBlob

# SMB\_COM\_SESSION\_SETUP\_ANDX command - Type 12 (0x0C)





# NTLMv2 LM/NT response

- LM response is constructed with
  - 1st encrypted password: 16 bytes
  - 1st client challenge code: 8 bytes
- NT response is constructed with
  - 2nd encrypted password: 16 bytes
  - 2nd client challenge code: variable length

# 2nd SMB\_COM\_SESSION\_SETUP\_ANDX response over MS-DS

- Error code
- WordCount: 0x04

# Requisite information

- Account name
- Domain/Workgroup/Host name
- Server challenge code
- Client challenge code
- Encrypted password
- The result of authentication

# NTLMSSP structure

also used in NTLM authentication of

- IIS
- DCOM
- NT Terminal Server
- 2000 Terminal Service
- NNTP Service

# Agenda

1. LM authentication mechanism
2. Demonstration (1)
3. NTLM v2 authentication algorithm
4. Sniffing SMB traffic on port 139
5. Sniffing SMB traffic on port 445
6. Demonstration (2)

# Demonstration

- Cracking NTLMv2 challenge/response
  - send a password using NTLMv2 authentication
  - capture the encrypted password using ScoopLM
  - send the encrypted password to our system in Japan using pscp
  - recover the password from the encrypted string using Sixteen-Beat



# Sixteen-Beat



- 16 nodes Beowulf type cluster
  - 1 server & 15 diskless clients
  - CPU: Athlon 1.4GHz
  - RAM: SD-RAM 512MB
  - NIC: 100Base-TX
  - HD: 80GB (server only)
  - Linux kernel 2.4.2.2
  - mpich-1.2.2
  - 100Base-TX Switch

# NTLMv2 challenge/response cracking performance

- 16CPU - about 4 million trials/sec
  - 4 numeric & alphabet characters: < 5 seconds
  - 5 numeric & alphabet characters: < 4 minutes
  - 6 numeric & alphabet characters: < 4 hours
  - 7 numeric & alphabet characters: about 10 days
  - 8 numeric & alphabet characters: about 21 months
- 1CPU - about 0.25 million trials/sec
  - 4 numeric & alphabet characters: < 1 minute
  - 5 numeric & alphabet characters: < 1 hour
  - 6 numeric & alphabet characters: about 63 hours
- gcc version 3.0.1 with -O2 option
  - MD4 & MD5: OpenSSL toolkit libcrypto.a
  - HMAC: RFC 2104 sample code

# Conclusion

“For NTLMv2, the key space for password-derived keys is 128 bits. This makes a brute force search infeasible, even with hardware accelerators, **if the password is strong enough.**”

from Microsoft Knowledge Base