

Jeanned'Hack CTF - Writeup

Seigneurs, Manoirs et Batailles

Catégorie	Difficulté	Points
Windows	Moyen	989

Description

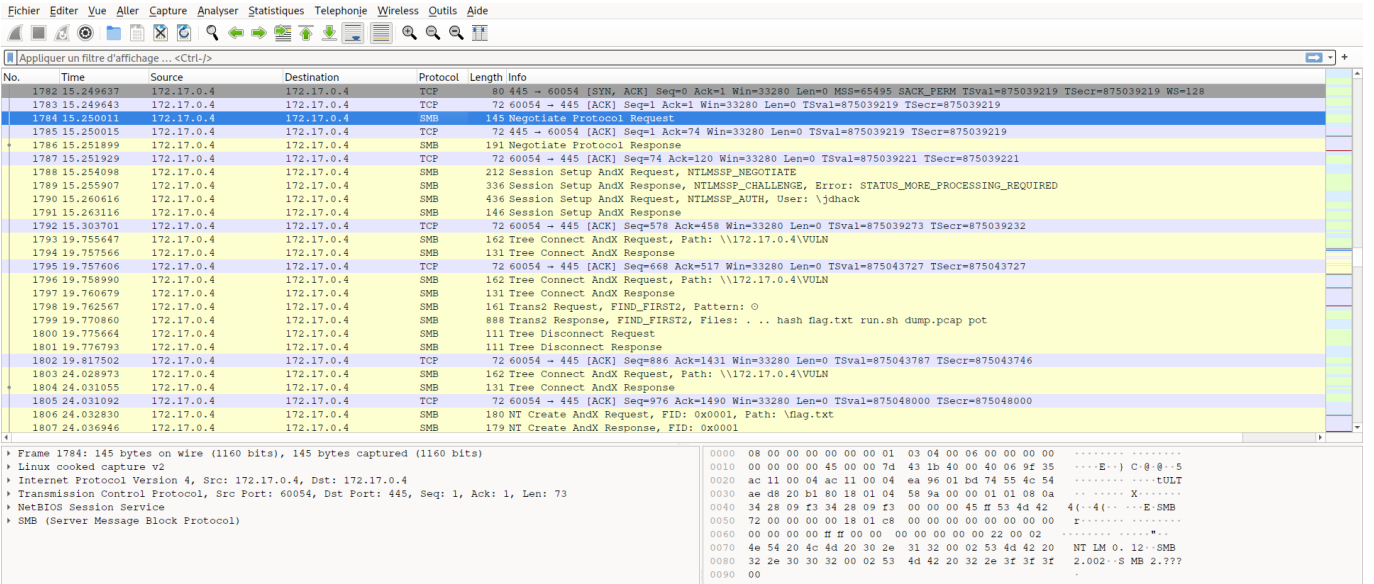
Vous avez intercepté des communications des pigeons voyageurs ennemis. Essayez de déchiffrer cette série de communications et d'y retrouver le mot de passe de l'utilisateur sur cette machine Windows.

Fichier attaché : `capture.pcap`

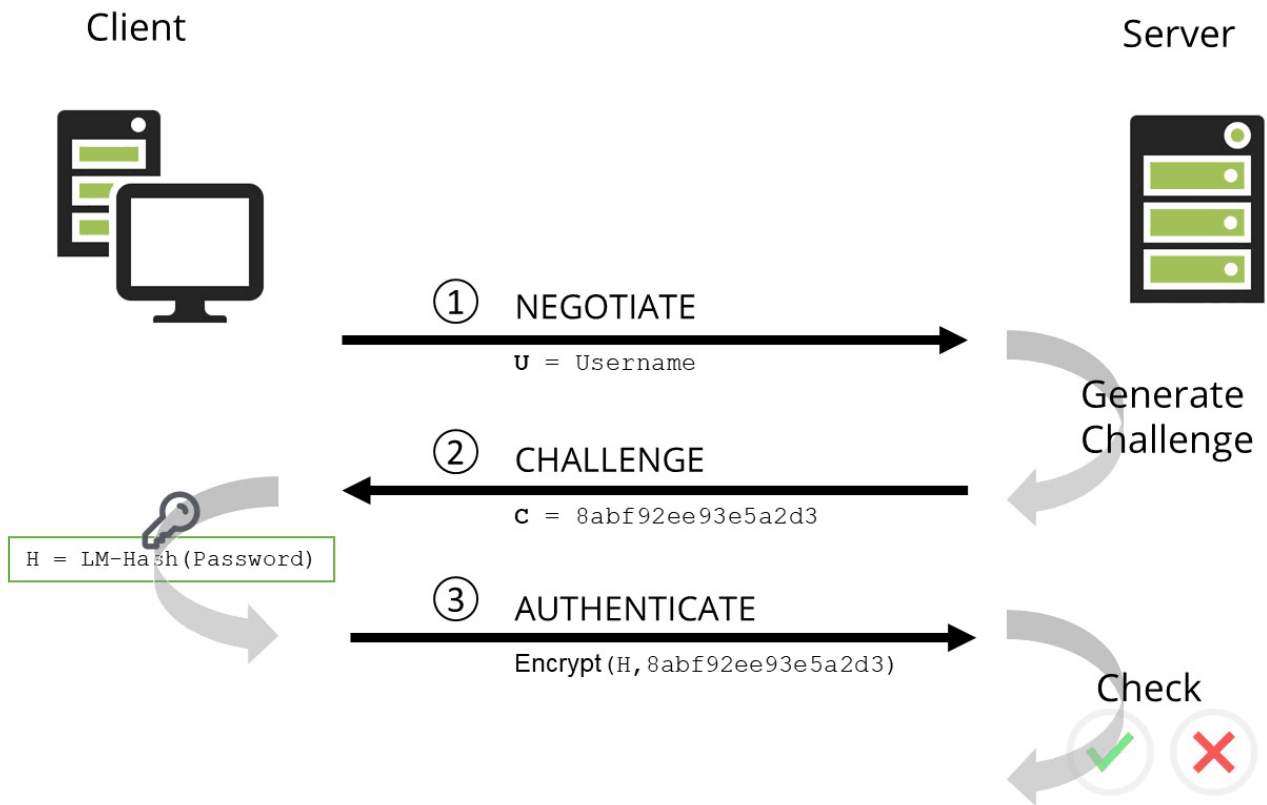
Writeup

Le fichier fourni est une capture réseau PCAP. On peut l'ouvrir avec un logiciel comme **Wireshark** pour l'analyser. Le but est de retrouver le mot de passe d'un utilisateur Windows à partir de ce fichier.

Pour commencer, il y a beaucoup de bruits et de fausses pistes dans ce fichier (spoiler: c'est fait exprès 😈). En fouillant le fichier on peut identifier des échanges utilisant le protocole **SMB**. C'est le seul protocole de cette capture qui est plus souvent utilisé par des machines Windows, c'est donc la piste la plus probable (ça et le nom du challenge).



L'authentification auprès du serveur SMB repose ici sur le protocole **NTLM**, utilisée sur Windows. Il est décrit rapidement dans le schéma ci-dessous :



On peut extraire uniquement les paquets en lien avec l'authentification en appliquant le filtre `ntlmssp` (NTLM Secure Service Provider) sur Wireshark. L'utilisateur tentant de se connecter s'appelle `jdhack` :

ntlmssp						
No.	Time	Source	Destination	Protocol	Length	Info
1788	15.254098	172.17.0.4	172.17.0.4	SMB	212	Session Setup AndX Request, NTLMSSP_NEGOTIATE
1789	15.255907	172.17.0.4	172.17.0.4	SMB	336	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
1790	15.260616	172.17.0.4	172.17.0.4	SMB	436	Session Setup AndX Request, NTLMSSP_AUTH, User: \jdhack

Maintenant, il faut retrouver dans ces paquets les informations suivantes pour reconstruire de quoi casser le mot de passe de l'utilisateur :

- Le nom d'utilisateur,
- Le challenge du serveur,
- La réponse de l'utilisateur au challenge, c'est-à-dire le HMAC-MD5 du challenge en utilisant le hash LM de son mot de passe comme secret,
- Et la réponse NTLMv2 complète.

Ici on peut retrouver le challenge du serveur :

✓ 1788 15.254098	172.17.0.4	172.17.0.4	SMB	212 Session Setup AndX Request, NTLMSSP_NEGOTIATE
✓ 1789 15.255907	172.17.0.4	172.17.0.4	SMB	336 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
✓ 1790 15.260616	172.17.0.4	172.17.0.4	SMB	436 Session Setup AndX Request, NTLMSSP_AUTH, User: \jdhack

<p>Frame 1789: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)</p> <ul style="list-style-type: none"> Linux cooked capture v2 Internet Protocol Version 4, Src: 172.17.0.4, Dst: 172.17.0.4 Transmission Control Protocol, Src Port: 445, Dst Port: 60054, Seq: 120, Ack: 214, Len: 264 NetBIOS Session Service SMB (Server Message Block Protocol) <ul style="list-style-type: none"> SMB Header <ul style="list-style-type: none"> Session Setup AndX Response (0x73) <ul style="list-style-type: none"> Word Count (WCT): 4 AndXCommand: No further commands (0xff) Reserved: 00 AndXOffset: 0 Action: 0x0000 Security Blob Length: 199 Byte Count (BCC): 217 Security Blob [truncated]: a181c43081cia0030a0101a10c060a2b06010401823702020aa281ab0481a84e544c4d5353 	<pre> 0000 08 00 00 00 00 00 00 01 03 04 00 06 00 00 00 00E...C@... 0010 00 00 00 00 45 00 01 3c 83 8e 40 00 40 06 5e 03E...C@... 0020 ac 11 00 04 ac 11 00 04 01 bd ea 96 ae d8 21 28tUM... 0030 74 55 4d 29 80 18 01 04 59 59 00 00 01 01 08 0aYY... 0040 34 28 09 f9 34 28 09 f7 00 00 01 04 ff 53 4d 42 4((...H...SMB 0050 73 16 00 00 c0 80 01 48 00 00 00 00 00 00 00 00s...H... 0060 00 00 00 00 ff ff bc 33 0a 00 00 00 04 ff 00 003... 0070 00 00 00 c7 00 d9 00 a1 81 c4 30 81 c1 a0 03 0a0... 0080 01 01 a1 0c 06 0a 2b 06 01 04 01 82 37 02 02 0a+...7... 0090 a2 81 ab 04 81 a8 4e 54 4c 4d 53 53 50 00 02 00NT LMSSP... 00a0 00 00 10 00 10 00 38 00 00 00 05 02 8a a2 aa aa8... 00b0 aa aa aa aa aa aa 00 00 00 00 00 00 00 00 60 00M... 00c0 60 00 48 00 00 00 ff ff ff ff ff ff ff 4d 00H... 00d0 71 00 6d 00 58 00 42 00 6e 00 4c 00 6c 00 01 00q-m-X-B-n-L... 00e0 10 00 55 00 72 00 78 00 44 00 54 00 45 00 4c 00U-r-x-D-T-E-L... 00f0 42 00 03 00 10 00 55 00 72 00 78 00 44 00 54 00B...U-r-x-D-T... 0100 45 00 4c 00 42 00 02 00 10 00 4d 00 71 00 6d 00E-L-B...-M-q-m... 0110 58 00 42 00 6e 00 4c 00 6c 00 04 00 10 00 4d 00X-B-n-L-1...-M... 0120 71 00 6d 00 58 00 42 00 6e 00 4c 00 6c 00 07 00q-m-X-B-n-L-1... 0130 08 00 00 28 ce 49 64 6b da 01 00 00 00 00 44 6f(-Idk...-Do... 0140 4c 73 6d 4a 4e 6a 00 44 6f 4c 73 6d 4a 4e 6a 00LsmJNj-D oLsmJNj- </pre>
--	---

Et ici le HMAC-MD5 (NTProofStr) et la réponse NTLM (NTLMv2 Response) :

✓ 1788 15.254098	172.17.0.4	172.17.0.4	SMB	212 Session Setup AndX Request, NTLMSSP_NEGOTIATE
✓ 1789 15.255907	172.17.0.4	172.17.0.4	SMB	336 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
✓ 1790 15.260616	172.17.0.4	172.17.0.4	SMB	436 Session Setup AndX Request, NTLMSSP_AUTH, User: \jdhack

<p>VC Number: 1</p> <p>Session Key: 0x00000000</p> <p>Security Blob Length: 290</p> <p>Reserved: 00000000</p> <p>Capabilities: 0x8000c044, Unicode, NT Status Codes, Large ReadX, Large WriteX, Extended Security</p> <p>Byte Count (BCC): 301</p> <p>Security Blob [truncated]: a182011e3082011aa2820116048201124e544c4d535300003000000180018004c000000a0ae</p> <p>GSS-API Generic Security Service Application Program Interface</p> <ul style="list-style-type: none"> Simple Protected Negotiation <ul style="list-style-type: none"> negTokenTarg <ul style="list-style-type: none"> responseToken [truncated]: 4e544c4d535300003000000180018004c000000a0ae0ae064000000000000004 NTLM Secure Service Provider <ul style="list-style-type: none"> NTLMSSP identifier: NTLMSSP NTLM Message Type: NTLMSSP_AUTH (0x00000003) Lan Manager Response: 39d91598ae2356d4e131ec9d8bb95e0e6345497734776f74 <ul style="list-style-type: none"> Length: 24 Maxlen: 24 Offset: 76 NTLM Response [truncated]: 00c233abdbea555fc3618f329d8ff7770101000000000000028ce49646bda01 <ul style="list-style-type: none"> Length: 174 Maxlen: 174 Offset: 100 NTLMv2 Response [truncated]: 00c233abdbea555fc3618f329d8ff7770101000000000000028ce49646bda01 <ul style="list-style-type: none"> NTProofStr: 00c233abdbea555fc3618f329d8ff777 Response Version: 1 Hi Response Version: 1 Z: 000000000000 Time: Feb 29, 2024 23:09:04.000000000 UTC 	<pre> 0000 08 00 00 00 00 00 00 01 03 04 00 06 00 00 00 00E...C@... 0010 00 00 00 00 45 00 01 a0 43 1e 40 00 40 06 9e 0fE...C@... 0020 ac 11 00 04 ac 11 00 04 ea 96 01 bd 74 55 4d 29tUM... 0030 ae 48 22 30 80 18 01 04 59 bd 00 00 01 01 08 0ag...Y... 0040 34 28 09 fe 34 28 09 f9 00 00 01 68 ff 53 4d 42 4((...H...SMB 0050 73 00 00 00 00 18 01 48 00 00 00 00 00 00 00 00s...H... 0060 00 00 00 00 ff ff bc 33 0a 00 00 00 0c ff 00 003... 0070 00 00 f0 02 00 01 00 00 00 00 00 22 01 00 00 00D... 0080 00 44 c0 00 80 2d 01 a1 82 01 1e 30 82 01 1a a2D... 0090 82 01 16 04 82 01 12 4e 54 4c 4d 53 53 50 00 03N TLMSSP... 00a0 00 00 00 18 00 18 00 4c 00 00 00 ae 00 ae 00 64d... 00b0 00 00 00 00 00 00 4c 00 00 00 0c 00 0c 00 40@... 00c0 00 00 00 00 00 00 4c 00 00 00 00 00 00 00 12L... 00d0 01 00 00 05 02 88 a0 6a 00 64 00 68 00 61 00 63j...d-h-a-c... 00e0 00 6b 00 39 d9 15 98 ae 23 56 d4 e1 31 ec 9d bbk-9...#V...1... 00f0 b9 5e 0e 63 45 49 77 34 77 6f 74 00 c2 33 ab dbcEIw4 wot...3... 0100 ea 55 5f c3 61 8f 32 9d 8f f7 77 01 01 00 00 00U_a-2...w... 0110 00 00 00 28 ce 49 64 6b da 01 63 45 49 77 34(-Idk...cEIw4... 0120 77 6f 74 00 00 00 00 01 00 10 00 55 00 72 00 78wot...U-r-x... 0130 00 44 00 54 00 45 00 4c 00 42 00 03 00 10 00 55D-T-E-L-B...U... 0140 00 72 00 78 00 44 00 54 00 45 00 4c 00 42 00 02r-x-D-T-E-L-B... 0150 00 10 00 4d 00 71 00 6d 00 58 00 42 00 6e 00 4cM-q-m-X-B-n-L... 0160 00 6c 00 04 00 10 00 4d 00 71 00 6d 00 58 00 42l...M-q-m-X-B... 0170 00 6e 00 4c 00 6c 00 07 00 08 00 00 28 ce 49 64n-L-1...(-Id... 0180 6b da 01 09 00 1a 00 63 00 69 00 66 00 73 00 2fk...-l-f-s-/... 0190 00 55 00 72 00 78 00 44 00 54 00 45 00 4c 00 42U-r-x-D-T-E-L-B... 01a0 00 00 00 00 00 00 00 00 00 55 6e 69 78 00 53 61Unix-Sa... 01b0 6d 62 61 00mba... </pre>
---	---

On peut ensuite construire le hash de la manière suivante :

```
User:::Server-Challenge:HMAC-MD5:NTLMv2Response
```

Ce qui donne :

```
jdhack:::aaaaaaaaaaaaaaaa:00c233abdbea555fc3618f329d8ff777:010100000000000000
028ce49646bda016345497734776f7400000000010010005500720078004400540045004c00
4200030010005500720078004400540045004c004200020010004d0071006d00580042006e0
04c006c00040010004d0071006d00580042006e004c006c00070008000028ce49646bda0109
001a0063006900660073002f005500720078004400540045004c0042000000000000000000
```

Enfin on peut stocker ce hash dans un fichier et tenter de le cracker avec john ou hashcat et notre meilleur wordlist (rockyou.txt) et récupérer le mot de passe :

```
louka > ~/CTF/JeanneD-Hack-CTF/windows/SeigneursManoirsBatailles > main !1 ?2
john ntlm.txt --wordlist=/usr/share/john/rockyou.txt
Warning: detected hash type "netntlmv2", but the string is also recognized as "ntlmv2-opencl"
Use the "--format=ntlmv2-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Windowshater      (jdhack)
1g 0:00:00:03 DONE (2024-03-04 23:24) 0.2577g/s 2704Kp/s 2704Kc/s 2704KC/s Woodywood..Welcome456
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
```

Et c'est gagné : `FLAG{Windowshater}`.

Liens utiles

Vidéo explicative [ici](#).