The Legend of Windows : A Link to the Hash

Authors : six / m4kx

$ id -un

- IT Sec enthusiasts, pentesters
- Sometimes researchers
- Work @ big streaming company in Lux.

$ history

How we got there ?

- Received zip file from untrusted source (customer)
- Intel: might be dangerous h4ck3rZ exploit
- Fires up a XP VM w/o network (no malware found...)
- Sniff traffic, unzip… NTLM goes remote…
- Magic trixx ?

124 100.469204	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49742	139
125 100.495945	10.0.2.15	1.2.3.4	TCP	66 [TCP Retransmission] 49742→139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49742	139
2202 105.511691	10.0.2.15	1.2.3.4	TCP	62 [TCP Retransmission] 49741→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	49741	445
4208 106.511340	10.0.2.15	1.2.3.4	TCP	62 [TCP Retransmission] 49742→139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	49742	139
7328 115.525124	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49742	139
8746 136.564697	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49741	445
8748 163.602350	10.0.2.15	1.2.3.4	TCP	66 49758→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49758	445
8749 164.601822	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49758	445
8750 164.702726	10.0.2.15	1.2.3.4	TCP	66 49759→139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49759	139
8751 165.701043	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49759	139
8752 166.605554	10.0.2.15	1.2.3.4	TCP	66 [TCP Retransmission] 49758→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49758	445
8753 167.714769	10.0.2.15	1.2.3.4	TCP	66 [TCP Retransmission] 49759→139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49759	139
8754 170.716855	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49759	139
8757 172.605948	10.0.2.15	1.2.3.4	TCP	62 [TCP Retransmission] 49758→445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	49758	445
8758 173.716237	10.0.2.15	1.2.3.4	TCP	62 [TCP Retransmission] 49759→139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	49759	139
8759 174.718452	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49759	139
8765 181.637570	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49758	445
8766 185.752038	10.0.2.15	1.2.3.4	TCP	66 49763→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49763	80
8767 185.753992	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49763	80
8768 188.761496	10.0.2.15	1.2.3.4	TCP	66 [TCP Retransmission] 49763→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	49763	80
8769 188.768632	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49763	80
8774 194.762293	10.0.2.15	1.2.3.4	TCP	62 [TCP Retransmission] 49763→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1	49763	80
8779 197.765297	10.0.2.2	10.0.2.15	ICMP	70 Destination unreachable (Network unreachable)	49763	80

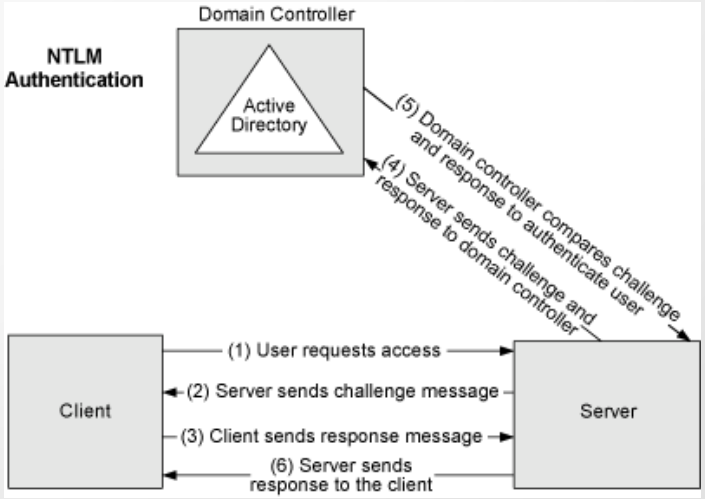
$ history

So what is happening automagically©?

- WindOS tcp p/445 SMB NTLM auth try
- If fails, tcp p/80 webDAV HTTP auth try (on LAN)

How can we abuse it?

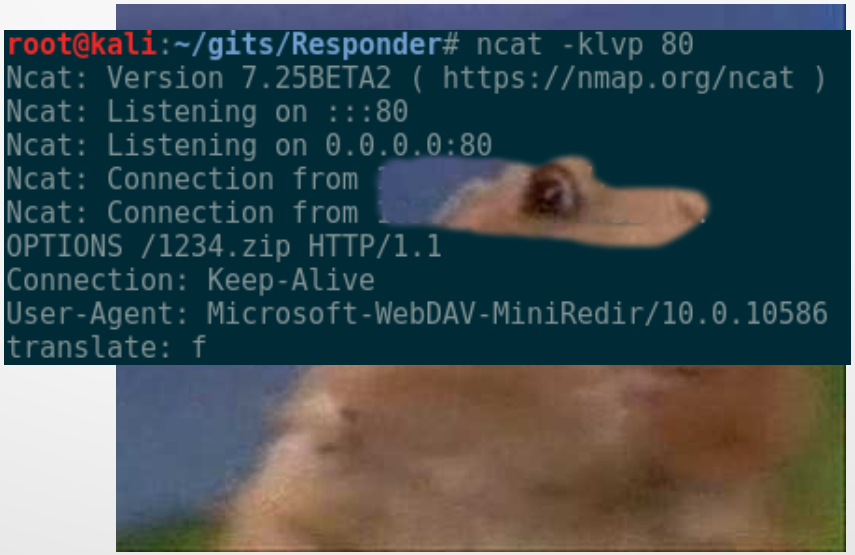
- Too easy if **445** is not blocked.
- Respond to SMB to get NetNTLM hash **on 445**
- Respond to HTTP to get NetNTLM hash **on 80**
- Respond to HTTP and prompt Basic auth **on 80** for phishing



msf > exploit -g

OK, have some fun !!

- Almost no user interaction :)
- Just have to drop the file anywhere :))
- Folder opened or browsed (background also) :)))
- Automatic fetching of .lnk / .url with NTLM :))))



msf > exploit -g

Exploit scenario 1: SMB sign disabled, no crack, hash relaying

REMINDER: NetNTLM is not pass-the-hashable

- Drop .lnk / .url on all writable shared

  Smbmap --upload [github]
- Use MSF exploit/windows/smb/smb_relay or Impacket smbrelayx
- Use the relayed credentials
- Profit ?

msf > exploit -g

Exploit scenario 2: SMB sign, hash crack and pass use

- **Drop** .lnk / .url on all writable shared folders

  Smbmap --upload [github]
- Responder.py collect everything

  Responder, .sqlite dump Responder.db [github]
- Crack and repeat

  Hashcat / John
- Likely get users / admin / domain admin

Practical usage feedback: found a log shared folder written by all, drop the .lnk, collected ***all hashes in 1 hour***

```
[SMB] NTLMv2-SSP Client   : 192.168.56.1
[SMB] NTLMv2-SSP Username : DESKTOP-UD60LL7\spodi
[SMB] NTLMv2-SSP Hash     : spodi::DESKTOP-UD60LL7:1122334455667788:822706816DC425044541256B5EEFAD37:0101000000000006AA85E09C71FD20180F4C92FF349A65E000000002000A0053004D0042003100320001000A0053004D00420031003
0004000A0053004D0042003100320003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000001000000002000006E45BA610714426E66543EC63288C240F3C93A8DC87D61010AFE313799D1D8880A0010000000000000000
000000000000000000000090022006300690066007300 2F00310039003200 2E00310036003800 2E00350036002E0031000000000000000000
[SMB] Requested Share     : \\192.168.56.1\TEST.TXT
```

msf > exploit -g

Exploit scenario 2 (cont'd): SMB or HTTP

- Where 445 is **blocked** you get HTTP NetNTLM on LAN
- NetNTLMv1 cracks fast, v2 is a *****
- You can **force HTTP NTLM** by blocking 445 (plain text)
- Our crack using GPU (GTX980): 27/107 in 3 days :-))))

For instance, cudaHashcat with one GPU card (GeForce GTX 980, 4095MB, 1278Mhz, 16MCU) delivers:

LM hash	12261.3 MH/s
NTLMv1 hash	22896.5 MH/s
NetNTLMv1 response	5275.9 MH/s
NetNTLMv2 response	742.9 MH/s

This means that NTLMv1 hash of a 7-byte length password will be cracked in 2.4 hours.

msf > exploit -g

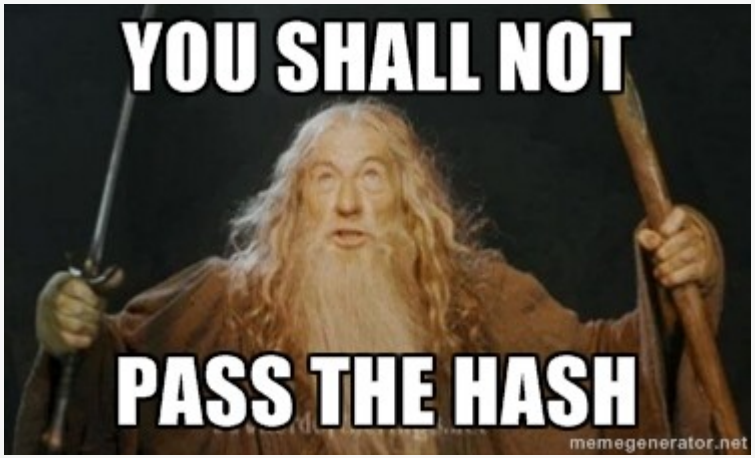
Exploit scenario 3: From .lnk to domain admin.

- Send hidden .lnk / .url in zip files (to HR? :)
- Probably gets unzipped and dropped to open or used folders.
- Get tcp p/445 NTLM if **net sec is weak**
    - In that case: start cracking.
    - Successful crack: if there is RDP, login
    - Escalate to other users through share drive if any
    - If lucky: domain admin cracked (remember 27/107? :))
    - Target pwnt.
- If blocked: WindOS still connects you over tcp/80 and at least it's still possible to phish - but no NTLM.

msf > exploit -g

Exploit scenario 2 (cont'd): How to use cracked passwords ?

REMINDER: NetNTLM is not pass-the-hashable



- Features simple: RDP, VPN, OWA
- Classic pentest: Smbshell / psExec & co
- More exotic : Rpclient / Remote registry
- Underground swag : Win SCCM remote controller (agent based)

$ printf stfu

DEMO TIME !

$ # tl;dr

What we find cool about this exploit:

- It's a **feature!** Since XP to 10 (MS won't fix)
- Similar to msf > use post/windows/escalate/droplnk but simpler
- No WPAD, mitm or any active attack is needed. Silent.
- Fix is an obscure reg change (we won't tell:))))
- If you disable NTLM as MS recommends your services stop working (eg. exchange, vpn, macOS… etc)

What's not cool?

- Remote exploitation over Internet **does not always** work, if 445 blocked, on 80 no NTML

$ find / -name *credits

- Thanks for listening!

- Questions?

- Website: https://itsec.lu/
- E-mail: itsecpublic@doclerholding.com
- PGP ~ 14BB E380 464D E0E9 E183 F02B D0F8 36D4 C7C1 1908