Overpass-the-Hash Attack: Principles and Detection

blog.netwrix.com/2022/10/04/overpass-the-hash-attacks

The overpass-the-hash attack is a combination of two other attacks: pass-the-hash and pass-the-ticket. All three techniques fall under the Mitre category “Exploitation of remote services.”

In an overpass-the-hash attack, an adversary leverages the NTLM hash of a user account to obtain a Kerberos ticket that can be used to access network resources. This technique is handy if you are not able to obtain the cleartext password for an account but require Kerberos authentication to reach your destination. This attack can be used to perform actions on local or remote servers. The most common tools used to perform this kind of attack are Mimikatz and Rubeus.

Download eBook:

CISA Simulated Attack: How to Improve Detection and Response

How Overpass-the-Hash Works

Step 1. Obtain the password hash of a user account.

The first step is the same as for a pass-the-hash attack: Obtain the NTLM password hash (NT hash) for a user account we want to compromise. For that we will use Mimikatz:

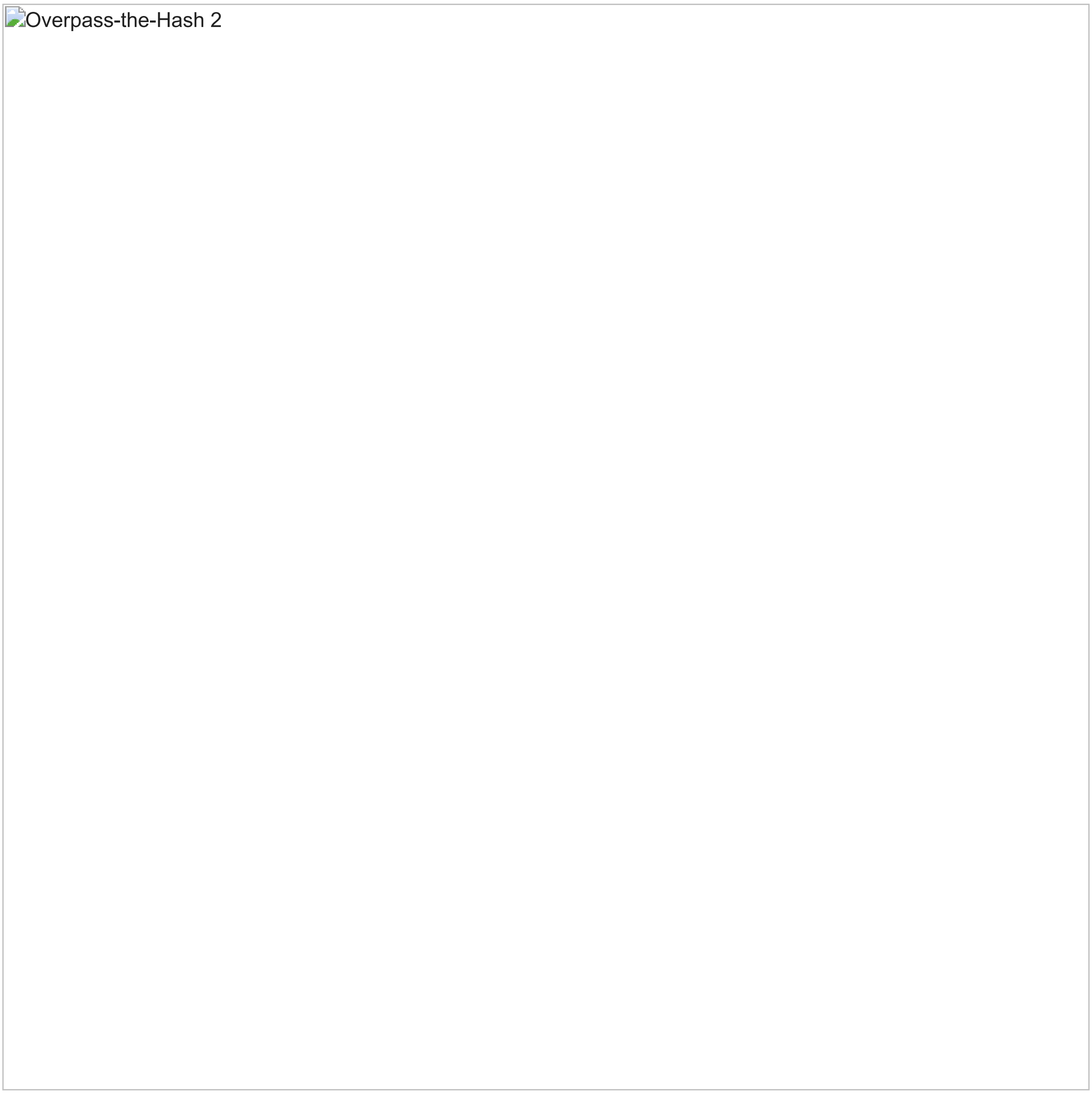
```
Privilege::debug
Sekurlsa::logonpasswords
```

Overpass-the-Hash 1

Step 2. Perform a overpass-the-hash attack.

Using the NTLM hash, we can perform a overpass-the-hash attack:

```
Sekurlsa::pth /user:[USER] /domain:[DOMAIN] /ntlm:[NTLM HASH]
```



Overpass-the-Hash 2

Not only did we just pass the hash, we overpassed it: The NTLM hash was passed into the Kerberos authentication provider using RC4 encryption. This is possible because Microsoft provides the ability to create RC4-HMAC-MD5-encrypted Kerberos tokens based on NTLM hashes. This is supported primarily for backwards compatibility, but it can also be exploited — all you need is a user’s NTLM hash to create a Kerberos ticket with the lowest level of security. For more details, read Benjamin Delpy’s blog post.

Other options for performing overpass-the-hash attacks

You can also create Kerberos tickets using other information about a user, such as their AES keys. Mimikatz enables you to extract AES keys in a couple different ways. The DCSync command returns this information for any user in the domain if you have the proper Active Directory permissions. Or you can use the *sekurlsa::ekeys* command on your local system.

```
Lsadump::dcsync /user:[USER] /domain:[DOMAIN]
```

Once we have access to the user’s AES keys, we can abuse them without actual privilege escalation.

Overpass-the-Hash 3

From there we can issue a pass-the-hash command to inject the AES key into a Kerberos ticket. This will be more difficult to detect as it will use more secure and commonly used encryption keys.

```
Sekurlsa::pth /user:[USER] /domain:[DOMAIN] /aes256:[AES256 KEY]
```

Overpass-the-Hash 4

Now we can authenticate as this user. If we use the klist command, we should see AES256-encrypted Kerberos tickets being used for our authentication:

Overpass-the-Hash 5

Detecting Overpass-the-Hash Attacks

Using pass-the-hash detection techniques

The best way to spot overpass-the-hash hacking attacks is to use the same strategy as for detecting pass-the-hash: Look for the following event log signature in each endpoint's authentication process:

- Event ID 4624 with Logon Type = 9, Authentication Package = Negotiate, and Logon Process = seclogo
- Sysmon Event ID 10 LSASS process access

When you see both of those events at the same time, you've got either pass-the-hash or overpass-the-hash, since the process of injecting the NTLM authentication and Kerberos tickets into a new session is the same in both attacks. However, there is no way on the endpoints to distinguish what options were passed into the pass-the-hash command from the event logs.

So how can administrators distinguish between pass-the-hash and overpass-the-hash? The main difference is that in overpass-the-hash, the event log will show Kerberos, rather than NTLM, authentication activity on the domain controller. Let's compare the event logs during the two types of attacks (the differences are bolded):

Pass-the-hash logs

Source Host	Target Host	Domain Controller
4648 – A logon was attempted using explicit credentials.	4624 – An account was successfully logged on. Logon Type 3, NTLM	4776 – The computer attempted to validate the credentials for an account.
4624 – An account was successfully logged on. (Logon type = 9 Logon Process = Seclogo)	4672 – Special privileges assigned to new logon.	
4672 – Special privileges assigned to new logon. (Logged on user, not impersonated user)		

Overpass-the-hash logs

Source Host	Source Host Target Host	Domain Controller
4648 – A logon was attempted using explicit credentials.	4624 – An account was successfully logged on. (Logon Type = 3, Logon Process = Kerberos, Authentication Package = Kerberos)	4768 – A Kerberos authentication ticket (TGT) was requested. (Encryption Type for RC4/AES128/AES256)
4624 – An account was successfully logged on. (Logon type = 9 Logon Process = Seclogo)	4672 – Special privileges assigned to new logon.	4769 – A Kerberos service ticket was requested. (Encryption Type for RC4/AES128/AES256)
4672 – Special privileges assigned to new logon. (Logged on user, not impersonated user)		

It is worth noting that on the domain controller, you can see the encryption level for the tickets (0x17 for RC4, 0x11 for AES128, and 0x12 for AES256). However, as we've demonstrated, this is not a reliable detection technique as an attacker can specify any or all of these when creating a ticket.

To recap, the best method of detection is to check the endpoints for event ID 4624 with Logon Type = 9 and Sysmon event ID 10. Then, we can inspect our domain controller logs for event ID 4776 for that user (pass-the-hash) or 4768/4769 (overpass-the-hash).

Using pass-the-ticket detection techniques

The detection strategy covered in our pass-the-ticket tutorial is useful here as well. That involves inspecting user sessions for their associated Kerberos tickets. If a ticket exists that doesn't match the user associated with the session, then there has been a ticket injection.

One useful thing with overpass-the-hash is that we get the 4624 event on the endpoint with logon type 9, and this contains the session ID for the new session:

We can see we have a new logon for the user Michael. If we use the klist –li command on that logon ID, we can see any associated Kerberos tickets. In this case, it will show the tickets from the compromised user:

Overpass-the-Hash 7

Conclusion

The strategies detailed above are one way to detect overpass-the-hash and other lateral movement techniques in your network, but they generally require the collection and inspection of event logs and running diagnostic scripts on each endpoint and domain controller. For a comprehensive approach to detecting, preventing and responding to these and other Active Directory attacks, check out the Netwrix Active Directory Security Solution.

FAQ

What is overpass-the-hash?

Overpass-the-hash is an attack that enables an adversary to pass a user account’s NTLM hash into the Kerberos authentication provider. It combines pass-the-hash and pass-the-ticket techniques.

How can overpass-the-hash attacks be detected?

The best way to detect this attack is to check endpoint logs for event ID 4624 with Logon Type = 9. Also checking for Sysmon event ID 10 will reduce false positives.

What is an NTLM password hash?

The NTLM authentication protocol relies on password hashing, which is a one-way function that transforms a plaintext password into another string of text — the NTLM password hash

Jeff Warren