Page 10 / Skills Assessment - Snort



Skills Assessment - Snort

Snort Rule Development Exercise: Detecting Overpass-the-Hash

PCAP source: https://github.com/elcabezzonn/Pcaps

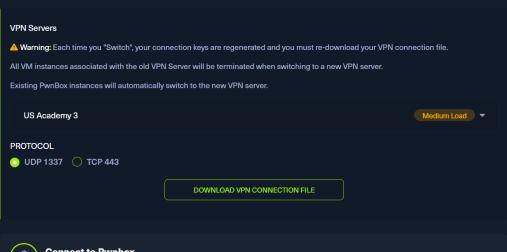
Attack description and possible detection points: http://www.labofapenetrationtester.com/2017/08/week-of-evading-microsoft-ata-day2 html

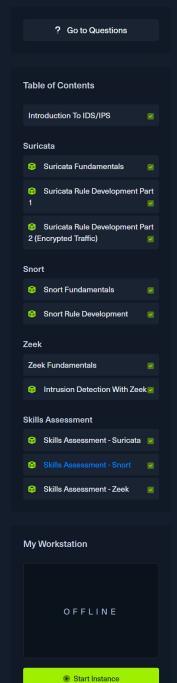
Overpass-the-Hash (Pass-the-Key) is a type of attack where an adversary gains unauthorized access to resources by using a stolen NTLM (NT LAN Manager) hash or Kerberos key, without needing to crack the password from which the hash was derived. The attack involves using the hash to create a Kerberos TGT (Ticket-Granting Ticket) to authenticate to Active Directory (AD).

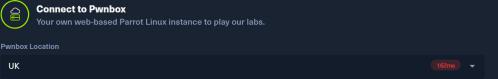
When the adversary utilizes Overpass-the-Hash, they have the NTLM hash of the user's password, which is used to craft an AS-REQ (Authentication Service Request) to the Key Distribution Center (KDC). To appear authentic, the AS-REQ contains a PRE-AUTH field, which contains an encrypted timestamp (Enc-Timestamp). This is normally used by a legitimate client to prove knowledge of the user's password, as it is encrypted using the user's password hash. In this attack scenario, the hash used to encrypt the timestamp is not derived from the actual password but rather it is the stolen NTLM hash. More specifically, in an Overpass-the-Hash attack the attacker doesn't use this hash to encrypt the Enc-Timestamp. Instead, the attacker directly uses the stolen NTLM hash to compute the Kerberos AS-REQ, bypassing the usual Kerberos process that would involve the user's password and the Enc-Timestamp. The attacker essentially "overpasses" the normal password-based authentication process, hence the name Overpass-the-Hash.

One key aspect of this type of attack that we can leverage for detection is the encryption type used for the Enc-Timestamp. A standard AS-REQ from a modern Windows client will usually use the AES256-CTS-HMAC-SHA1-96 encryption type for the Enc-Timestamp, but an Overpass-the-Hash attack using the older NTLM hash will use the RC4-HMAC encryption type. This discrepancy can be used as an indicator of a potential attack.

Review the previously referenced resource that discusses the network traces resulting from executing an Overpassthe-Hash attack, and then proceed to address the following question.







Waiting to start...

