Operation Keanu After-Report

Completed by:

Team Texas

Members:

Thomas Larkin

Colin Mullican

Graeme Dickerson-Southworth

Ikechukwu Igboemaka

Completed on:

05/18/2024

Overview

On May 6th, we initiated an attack on our target, Team Illinois's Steel domain. The attack was successful, as we exfiltrated their own flags and replaced their current flags with dummy flags of our own.

Procedure

Initial Access

Initial access was granted by logging in via SSH to Team Illinois's Waukegan system on the Steel domain, using credentials for admin accounts obtained from our ally, Team New York. It was later confirmed that these credentials were obtained from a PAM module on Team Illinois's system, logging log-in credentials and posting them in plaintext to a linked text file. While connection was established only to 1 of 7 systems, the victim system contained the flags, our main objective of this attack.

Hostname	IPv4	Operating System
peoria.steel.illinois.tu	172.21.140.118	Windows Server 2019
waukegan.steel.illinois.tu	172.21.140.240	Windows 2019
elgin.steel.illinois.tu	172.21.140.58	Windows Server 2019
schaumburg.steel.illinois.tu	172.21.140.17	Windows Server 2019
springfield.steel.illinois.tu	172.21.140.238	Linux
cicero.steel.illinois.tu	172.21.140.32	Windows 11|10|2022
champaign.steel.illinois.tu	172.21.140.252	Windows

(Targeted system = Green)

Persistence

Due to time constraints, persistence from previous operations was used, with no further persistence being established.

Exfiltration

Access to the File Share was established using the **net use** command, assigning a drive letter to the syntax for the File Share, assigned to all teams. Once access to the File Share was established, the flags were sent over SFTP to our remote Kali system. Additionally, we as a team replaced Team Illinois's flags with dummy flags, assigning the same names to each. This means that unless Team Illinois inspects their flags visually, the chances of detecting modification is slim.

Conclusion

Overall, while small in scope, we believe the attack to be a major success. While again relying on mechanisms left by our adversaries, such as the PAM module, the mechanisms were used to our advantage against Team Illinois. Additionally, the exfiltrated flags helped advance our goal of collecting all 15 flags, a goal Illinois was leading in amongst the other teams.