Mandatory Assignment 2

Bendik Egenes Dyrli, Øystein Andreassen, Anne Grethe Heltne

13.10.2017

Table of Content

Introduction

The group was tasked with watching the documentary “The KGB, the Computer, and Me” in which a small discrepancy on a billing form turns into one of the earliest cases of cyber espionage.

Based on the documentary we should discuss what were the technical, formal, physical and/or informal security holes, which elements in the CIA triad, confidentiality, integrity or availability, had been compromised. And what could have been the consequences given that the hacking had been successful. The former is to be isolated to the network managed by Cliff, while the consequences are general.

Finally we were to write what our recommendations would be to avoid such a situation in 2017.

Discussion

Through the documentary we learn that the attacker gained access presumably by guessing Sventek’s username/password combination. As to how the attacker gained information about how to connect to the network or how their usernames were generated we are not given. One assumption is since this is part of a larger academic network, the attacker sourced information from already compromised networks. Other assumption is that they gained initial access through default credentials, as this is mentioned as an entry vector into other networks.

Once on the network the hacker elevated their privileges on the system by using an unknown attack vector, it is unclear whether this was an unknown zero-day. Effectively the attacker gained superuser privileges and could thus alter the system as they wanted.

The attacker could then use this network to jump onto other networks, for example MILNET is mentioned. From the section about the trace the attacker did use this a great deal to explore, and most likely to try and gain access to other networks using network trust.

Conclusion

Isolating to the network managed by Cliff; from an entry standpoint there was a technical loophole if default credentials were active on the machine, this is not confirmed, and the attacker uses the account of Sventek throughout, thusly it is more likely a formal loophole given easy to guess passwords.

The attacker then used a vulnerability in the mailing system to elevate his privileges to superuser, from the information we’re given we can conclude that was a zero-day, still this is a technical hole the attacker used to hide his tracks by modifying the accounting system. This also

affects the confidentiality in the CIA triad, as any restrictions on the system is now effectively bypassed by the attacker.
From the information given, the attacker couldn't gain much information. The MILNET was public information and air gapped. The attacker wasn't wasn't interested in doing damage either, as they were trying to gather information. In the absolute worst case though the attacker could obtain secret information that could change the outcome of the cold war.

Recommendations

We recommend having an automated deployment of networked systems. This automation should include removal, disabling or changing of default credentials, installation of software and updates both to the software and the underlying operating system. This will give a common basis for which the systems operate, having the deployment as automated as possible will also reduce the human factor in letting things slip.
Given a common platform and known good configurations of the systems, we can then have automated monitoring of the systems, that will alert when changes are made, for example altering of superuser privileges.
The systems should also be patched regularly, preferably once or twice every month in a scheduled window, a test system should be used to confirm the patches before deployment into production.

With respect to passwords; For new users the first password should be randomized such that a pattern shouldn't be determined for new accounts, the user should be forced to changing it on first login. Formally we also recommend user education on good password practice in alignment with the most recent NIST guidelines. This also flows onto the technical aspect, mainly longer delay between password changes and verification of passwords against so called known bad choices.
The usage of a second factor for authentication is also recommended, examples include YUBIKEY or a secure OTP solution like Google Authenticator.

Sources

none, take from own experience and knowledge.