Cover Memo

To: James (@james), Aaron (@aaron)
From: Akhilesh Anand Undralla, UBNetDef SysSec F21
Date: 12/20/2021
Re: Summary of Catflix

Overview:

UBNetDef SysSec F21 successfully deployed ‘Catflix’, a website that streams thousands of 8k155fps quality cat videos. While adhering to the current UBNetDef Wiki network model, personnel training, documentation, and administrative tasks are implemented and maintained with secure Information technology (IT) systems practices. We at UBNetDef SysSec F21 are confident that adequate resources and time are given for additional testing that will serve the website to stand up the core of the network.

CIS Top 20 Framework Application

AKHILESH ANAND UNDRALLA

UBNETDEF SYSSEC F21

12/20/2021

TABLE OF CONTENTS

Executive Summary

UBNetDef SysSec F21 finds that the implementation of the greater Catflix Wiki network has been ensured with utmost security controls. Using ‘CIS Controls v7’ as reference, various technical controls implemented are Inventory and control of hardware assets, Inventory And Control Of Software Assets and Controlled Use of Administrative Privileges. Along this, firewall configurations are altered to ensure network hardening. This can potentially help towards system hardening by minimising attack vectors such as outdated packages with known security vulnerabilities, unnecessary network access. Publicly accessible resources such as database server, web servers are placed in a buffer network called demilitarized zone (DMZ) creating a layered security approach. This ensures organization to isolate all applications that are riskier than others through segmentation and offer smooth business operations.

The buffer network can help to mitigate the likelihood of a data breach and consequences from a potential attack can be addressed through enabling strict access control, network segmentation. This will prevent organisation’s sensitive data, systems and resources that could be attacked by adversarie by activating as an advanced security layer in the internal network.

As part of software restriction policies and strict system hardening group policies to protect systems new sub controls such as Multi-Factor Authentication, limited access to scripting tools, authorized whitelisting libraries & scripts, authentication of hardware asset certificates. Implementation of these sub controls also fulfill the organisation's security posture with streamlined Identity and Access Management policies.

Technical Findings

UBNetDef SysSec F21, using CIS Controls as reference implemented technical control namely Inventory and control of hardware assets, Inventory And Control Of Software Assets and Controlled Use of Administrative Privileges.

From 'CIS Top 20 Controls v7' CIS Control 1, CIS Control 2 and CIS Control are enforced and consdiered top priority for implementation to protect catflix wiki netwok.

CIS Control 1 - Inventory and Control of Hardware Assets:

A detailed asset inventory has been provided to the entrepreneurs that ensures maintenance of an accurate inventory of all the technology assets in the network model build that includes WindowsClient, Windows Active Directory, Linux Client, Linux Web Server, Rocky DataBase Server, PfSense Router and an Outside Windows Device. This adheres to the sub-control 1.4 which establishes inventory control of all hardware assets in the organization's network. Another sub-control 1.5 is addressed by documenting detailed asset inventory information in the form of recorded network topology that include network address details, machine name and department name for each authorized asset connected to the network. Network details include the device name, IP address, DNS and Gateway. CIS subcontrol 1.7 is deployed with port level access control using firewall rules (both network and host-based firewall) as well as hardware asset inventory control using active directory and domain controller to authorize the devices connected to the network.

Moving forward, new sub-control that is necessary for the organisation is 'CIS 1.8: Utilize Client Certificates to Authenticate Hardware Assets' which enusres client certificates should be maintained to control authorised devices within the network by validating hardware assets of the organization's trusted network.

CIS Control 2 - Inventory And Control Of Software Assets:

The control, Inventory and control of software assets ensures all of installed softwares on endpoint devices are minimised and maintained to reduce the potential for vulnerabilities to be exposed. Sub-control 2.1 is partially addressed by maintaining up-to-date software packages required in the network model to run streaming business-as-usual. This mitigated unnecessary security threats due to unpatched softwares.

Sub-control 2.10 is implemented by segregating high-risk devices and web servers that run services and placing them in demilitarized zone (DMZ) which is protected by the pfSense Security Gateway Appliance (pfSense). This ensures administering a layered security approach that isolates a private network (here LAN) and the untrusted network (here internet).

Moving forward, approved software packages should be mandated within the organisational business and operational purpose. This would completely fulfill subcontrol 2.1. New Sub-controls 2.8 and 2.9 i.e., 'Implement Application Whitelisting of Libraries and Scripts' will help prevent editing unauthorized scripts, registry edits, libraries and malicious softwares in to the system processes.

CIS Control 4 - Controlled Use of Administrative Privileges:

Separation of duties by having normal accounts and privilege accounts in order to have escalation access for sysadmin, security groups for Windows clients while maintaining active directory and administrator account for mediawiki.

Sub control 4.2 is covered by changing default passwords and removing blank/empty password entries (blank DB password). This ensures authentication and access control for the already present passwordless MariaDB database server that would act as a safeguard against wrongful access to the database.

New Sub control 4.5 should be implemented. This requires multi factor authentication centralizing access control for all enterprise assets through a directory service or SSO provider that would act as a safeguard against wrongful access to the databases. Another new sub-control 4.7 which limits access to scripting tools such as powershell, python, limiting sudoers list will ensure that only administrative privilege users to reduce the attack vectors in the organisation and hardens group policies.

Appendix

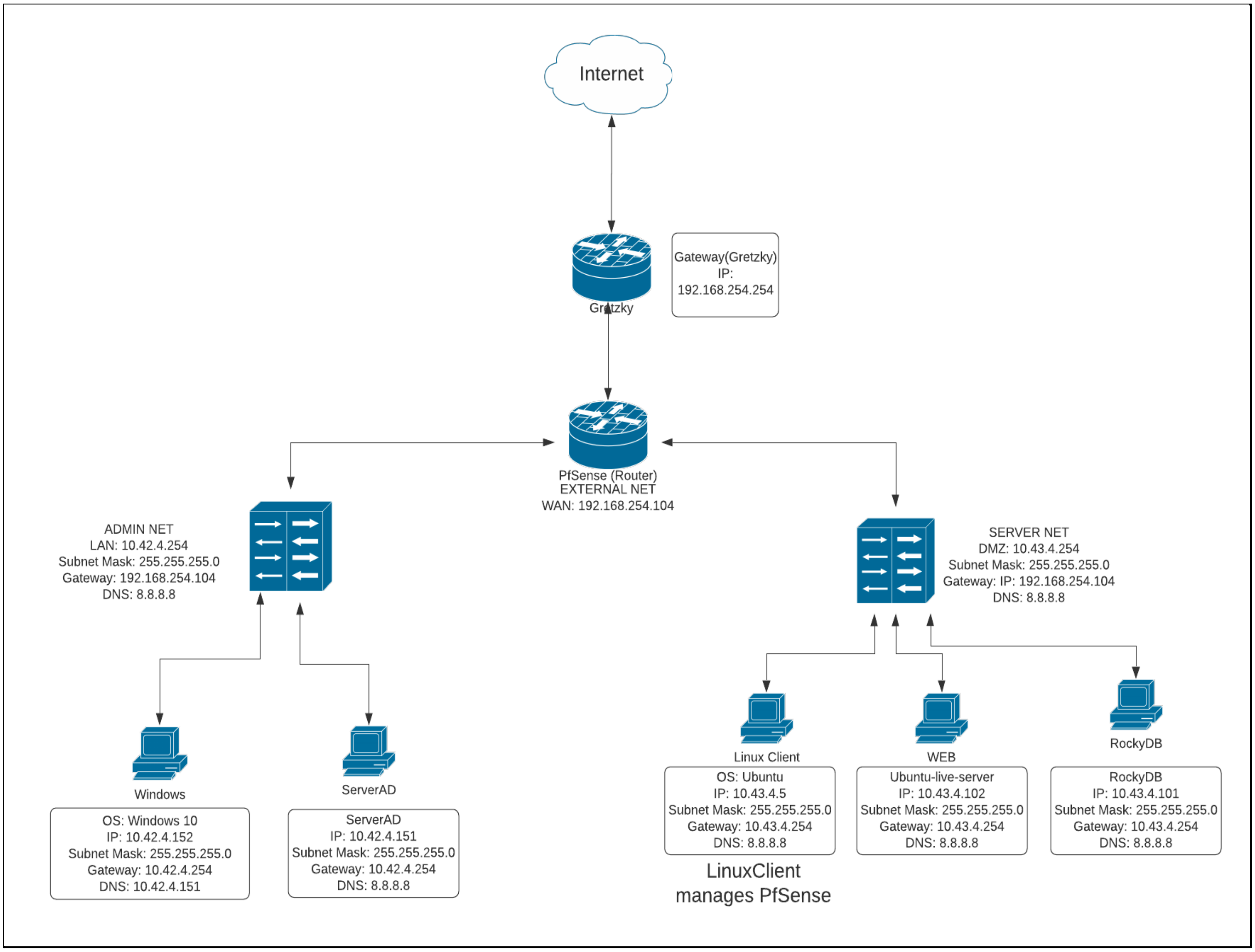

Figure 1.0: Topology of Catflix Network

References

Center for Internet Security – CIS Controls Version 7. (n.d.). Retrieved from https://jstor.uniri.hr/nph-proxy.cgi/en/60/https/itsecurity.cuyahogacounty.us/en-US/home.aspx