Vulnerability Assessment and Pentesting Report 15/03/2024

horizontal line

# Name: Jon Doe (jondoe@protonmail.com)

# EXECUTIVE SUMMARY

The machines in our company are protected from most kinds of threats by using firewalls, and security assessment is done quarterly to find several vulnerabilities and to find patches to fix the system, new machines have been introduced recently and web servers set up. Due to this, a chance of finding multiple vulnerabilities in the system is possible.

# METHODOLOGY & GOALS

We are doing a security assessment to find any vulnerabilities in the existing infrastructure. One machine has been identified as the target. The goal is to identify any vulnerabilities which pose a risk to the company and its business.

# SCOPE

A Windows Machine was tested.

IP 10.10.11.174

Windows Server 2022

# NARRATIVE & FINDINGS

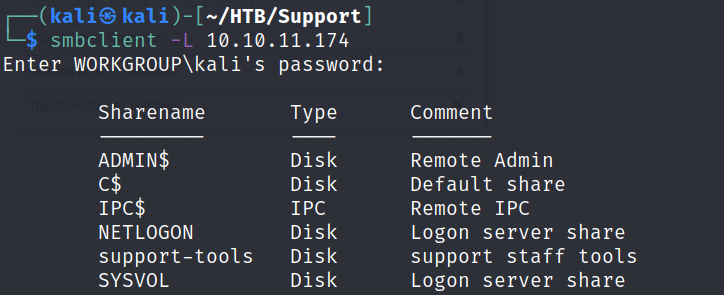
**August 31st:**

**Initial Enumeration**

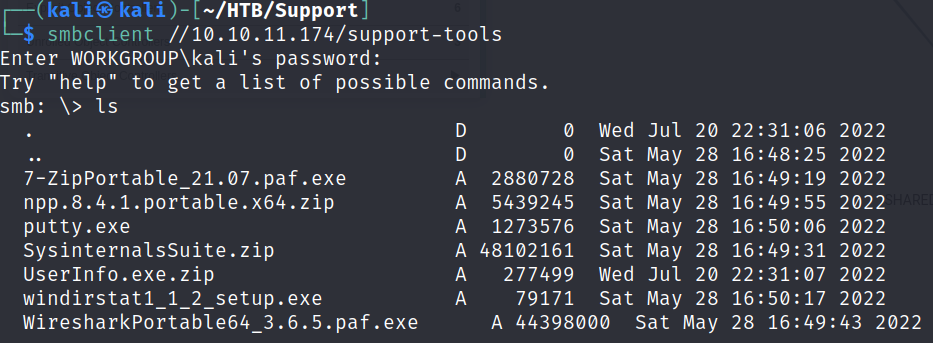
A system running Windows Server 2022 fully patched was found during the initial enumeration.

The Domain name is **“box.com”.**

Smb shares of the system were accessible via anonymous login, which revealed multiple shares.



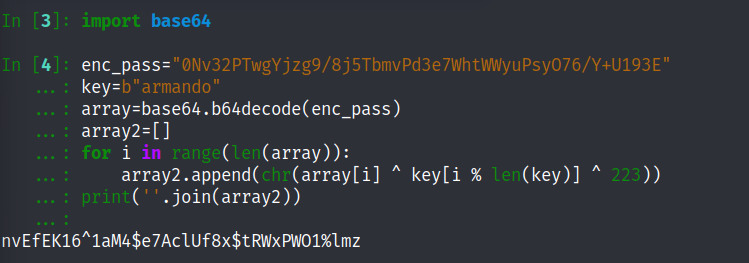
On further enumeration, the share support-tools is accessible. The share contained some interesting files.



The UserInfo.exe.zip file was downloaded and extracted, it contained a Userinfo.exe file. The file was analyzed using dotpeak. The binary contained an authentication system wherein an enc\_password was used, and some operations were performed on it to create a password.



On recreating this in python, we got the password- “**nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz**”



The above password was used to perform an LDAP search.

| └─$ ldapsearch -x -H ldap://10.10.11.174 -D 'support\ldap' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "CN=Users,DC=support,DC=htb" |
| --- |

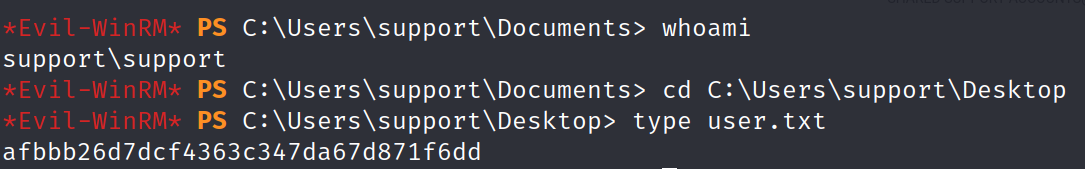
There was a password present in the retrieved information.

**Ironside47pleasure40Watchful**

This was used for logging in as the support user.

| ┌──(kali㉿kali)-[~/HTB/Support] └─$ evil-winrm -i 10.10.11.174 -u support -p Ironside47pleasure40Watchful |
| --- |

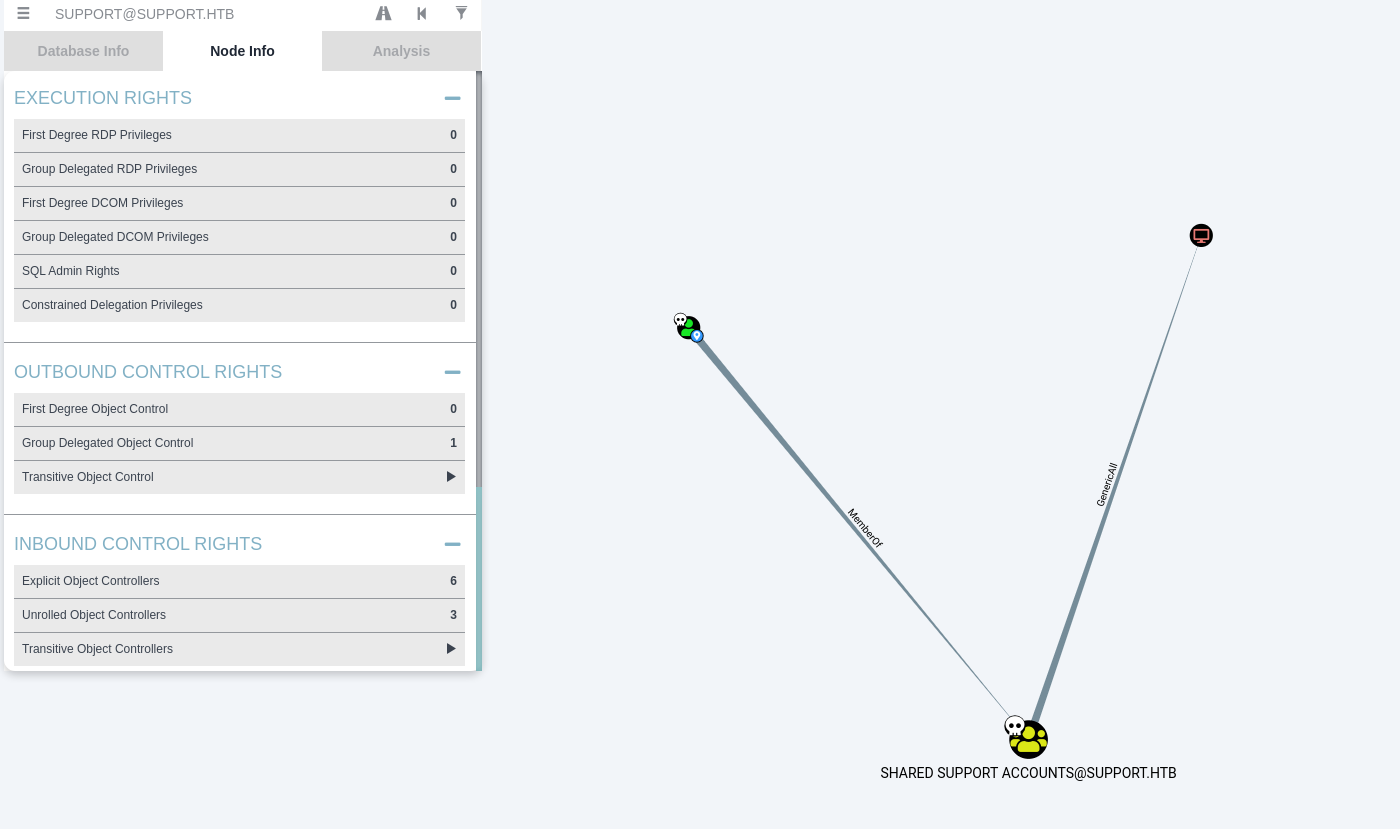
This allowed access to the user hash.



**Privilege Escalation**

Bloodhound was run on the system and we found a pathway to gain Domain Admin privileges.

The user support is a member of the Shared Support Accounts. The Shared support accounts has Delegated object control to the Domain Controller.



This can be leveraged to perform the Privilege escalation.

The Domain Admin Flag:- **bb26d7dcf4363c347da67d8dadd**

# RESULT

The pentest of the company revealed that their system can be exploited in the following way. The outcome revealed that an attacker can become the domain controller, leading to full system compromise.