

CYBERSECURITY HOMELAB PROJECT

David Gutiérrez

davidf.io

Overview

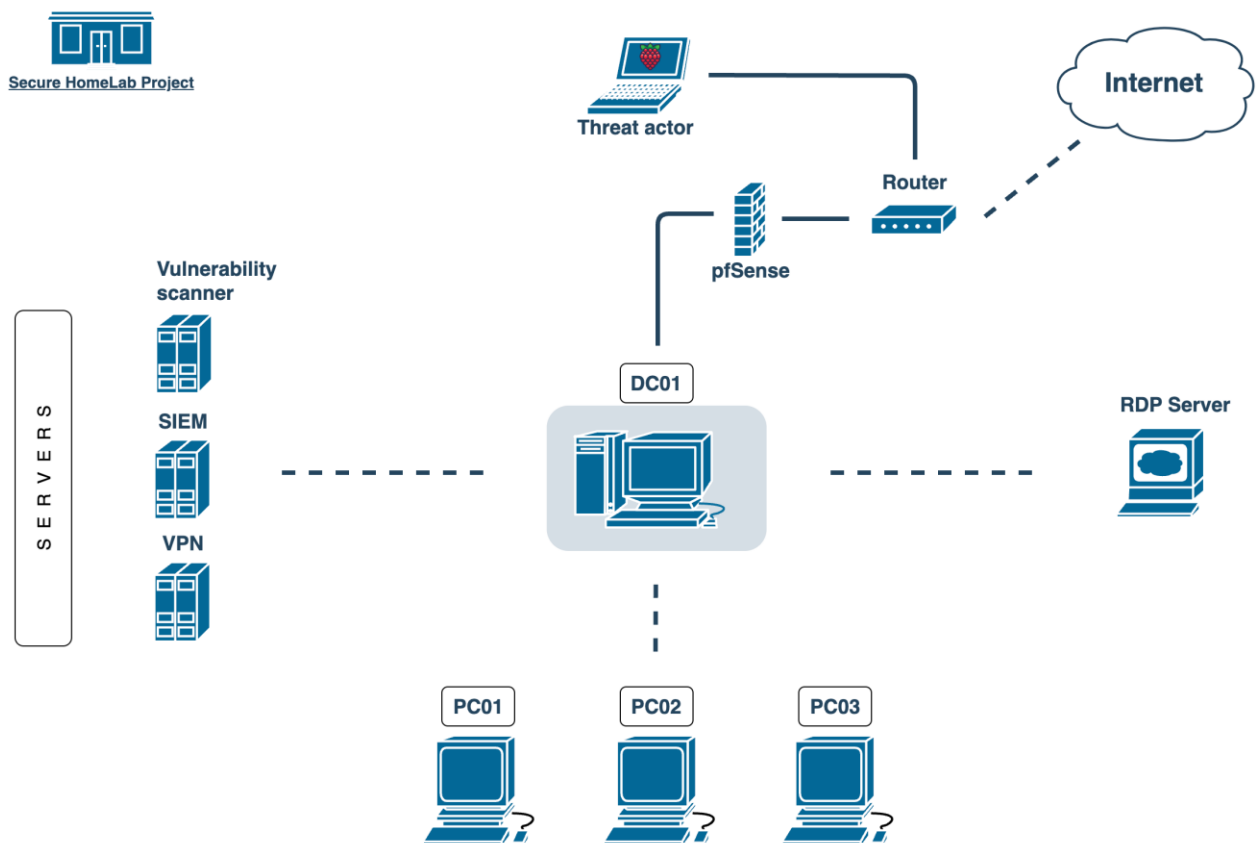
“Curiosity is insubordination in **its purest form.**”, Vladimir Nobokov

It is that act of insubordination that must prevail in the thinking being who wishes to dedicate their time to the study and understanding of science and information technologies. In the field of cybersecurity, it is essential to stay at the forefront of new trends, methodologies, and technologies in order to contribute positively to the security of individuals and organizations in a digitalized world. Under this premise, the idea of carrying out this project arises, allowing the strengthening and articulation of systems and security knowledge through the creation of a small-scale real-world scenario, a "cybersecurity homelab."

What's a “cybersecurity homelab”?

It is a small-scale environment designed to simulate real-world IT operations and their internal components. The primary goal is to deepen the understanding of security, systems, and networking concepts by integrating technologies, processes, and configurations in a controlled, experimental setting.

Network topology



Software & hardware specifications

- MacBook M1 Pro 512GB/16GB (Running *Sonoma 14.5* as OS)
- Matebook D15 512GB/8GB (Running *Windows 11 Home* as OS)
- Raspberry Pi Zero 2 W (Running *Ubuntu Server 22.04* as OS)

Technologies & features

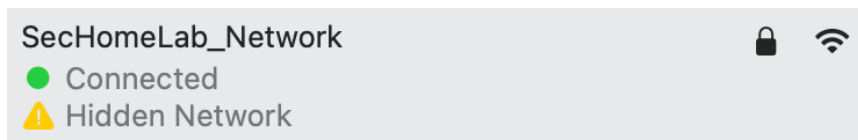
- Virtualization (VirtualBox & VMWare Fusion)
- Windows, Linux, Unix and macOS operating systems
- Active Directory Domain Services
- DNS, DHCP & RDP servers
- Group Policy Objects
- Folder redirection
- OpenVPN
- Nessus (Vulnerability scanner)
- SPLUNK (SIEM platform)
- pfSense (Firewall)

Guide

In the following guide I'm going to show a general chronologic view about all the procedures and configurations that I've performed to get a functional security home lab, including recommendations and practical experiments performed in the process.

1. Setup a dedicated router for laboratory (Optional)

- Link main router with dedicated router by connecting an ethernet cable from main router's LAN port to dedicated router's WAN port.
- Access to the dedicated router web panel and apply basic configurations (SSID, password and other parameters)
- Connect a device to the created network to check for internet connection.



2. Download virtualization software

- VMWare Fusion:
<https://www.mikeroyssoft.com/post/download-fusion-ws/>
- Virtualbox:
<https://www.virtualbox.org/wiki/Downloads>

In my case I downloaded VMWare from the Mac device and VirtualBox from the Windows machine.

Once you've download it, follow the steps for a basic installation.


3. Download and install Windows server

- Windows server 2022 download:
<https://www.microsoft.com/es-es/evalcenter/download-windows-server-2022>
- Install the .iso file on VirtualBox:
<https://softwarekeep.com/blogs/product-guides/windows-server-2022-installation-guide-step-by-step>

Do not forget to go to the VM settings and change the network adapter to “Bridged Adapter” (This will make the Win server reachable from other devices in the network)

4. Configure static IP address and Domain Controller

NOTE:

 **Karl Weng**
Microsoft Agent | Moderator

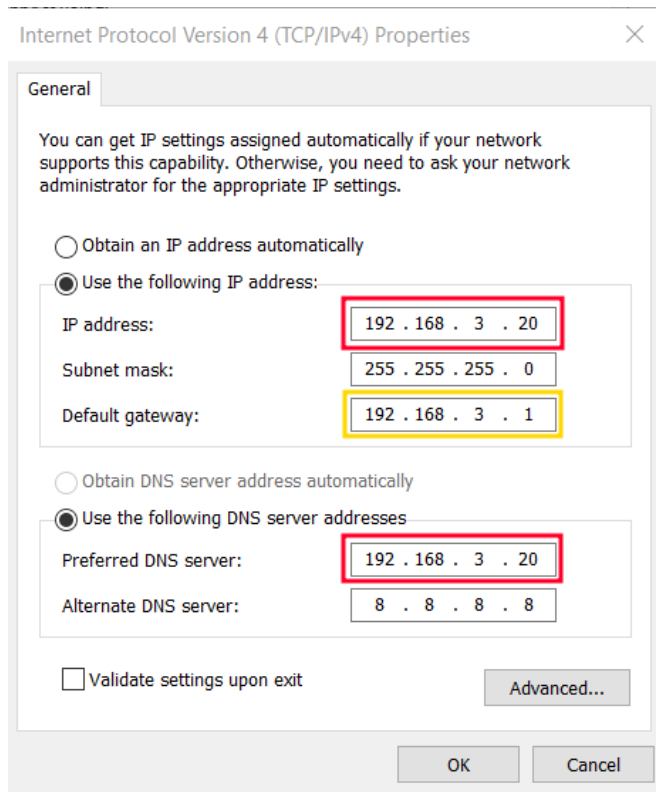
Replied on November 2, 2023
[Report abuse](#)

Hello!

While dynamic DNS registration can be convenient for end-user devices with dynamic IP addresses, for infrastructure components like DC which IP addresses are static and unlikely to change, static DNS entries may be appropriate. Static entries help maintain network reliability. Stability is crucial. We won't have to deal with unexpected changes in IP addresses.

Thanks,
Karl Weng

DC01 ethernet settings



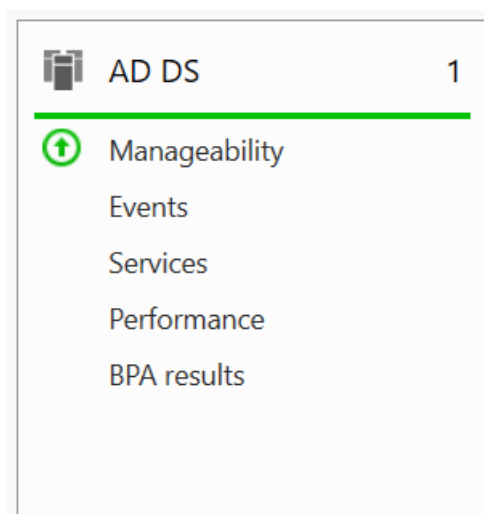
5. Add Active Directory Domain Services features

Active Directory is a centralized directory service developed by Microsoft for managing permissions and control access to network resources.

- Setup tutorial

<https://www.youtube.com/watch?v=FDhndiAEyxs&t=16s>

Active Directory Domain Services feature dashboard view



6. Setup DNS and DHCP servers

- DNS server:

A DNS server will be the responsible of translate human readable domain names into IP addresses. In this AD environment the DNS server has been configured on DC and it's a crucial component that will get easier the communications between workstations, servers and the domain controller.

Pinging domain and dc from a network machine to check if DNS works

```
> ping securecorp.local
PING securecorp.local (192.168.3.20): 56 data bytes
64 bytes from 192.168.3.20: icmp_seq=0 ttl=128 time=96.996 ms
64 bytes from 192.168.3.20: icmp_seq=1 ttl=128 time=17.783 ms
64 bytes from 192.168.3.20: icmp_seq=2 ttl=128 time=35.880 ms
64 bytes from 192.168.3.20: icmp_seq=3 ttl=128 time=57.243 ms
^C
--- securecorp.local ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 17.783/51.975/96.996/29.508 ms
> ping DC01
PING dc01.securecorp.local (192.168.3.20): 56 data bytes
64 bytes from 192.168.3.20: icmp_seq=0 ttl=128 time=77.436 ms
64 bytes from 192.168.3.20: icmp_seq=1 ttl=128 time=97.417 ms
64 bytes from 192.168.3.20: icmp_seq=2 ttl=128 time=14.752 ms
64 bytes from 192.168.3.20: icmp_seq=3 ttl=128 time=34.193 ms
```

Setup guide:

<https://www.youtube.com/watch?v=OtdOEiTozUE>

– DHCP server:

It's the one in charge of assigning IP addresses automatically to the hosts that connect to a network based on a configured scope. In the present project DHCP server has been installed on DC, it's a powerful feature that allows you as administrator to segment network clients by creating different scopes, track domain clients and define reservations for servers or specific domain hosts.

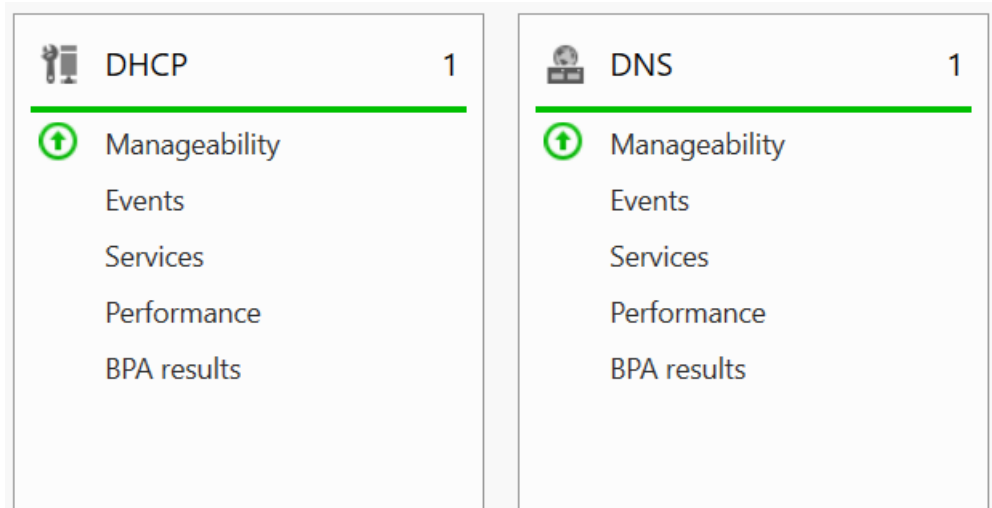
Setup guide:

<https://www.youtube.com/watch?v=OtdOEiTozUE>

DHCP leases view

Client IP Address	Name	Lease Expiration	Type
192.168.3.100	Davids-MBP.securec...	25/08/2024 3:34:15 p. m.	DHCP
192.168.3.101	VPN-SERVER.secure...	Reservation (active)	DHCP
192.168.3.102	SPLUNK-SERVER.sec...	24/08/2024 9:28:57 p. m.	DHCP
192.168.3.103	PC02.securecorp.local	19/08/2024 7:30:21 p. m.	DHCP

DHCP & DNS servers running on DC



Troubleshooting

To verify if a machine is actually getting the IP address from AD DHCP server go to DHCP panel on DC and look for *IPv4 > Scope > Address Leases*. There you should be able to see the current DHCP hosts.

Sometimes you'll need to request a new IP to the DHCP server, to achieve that run this command from CMD:

```
/Users/davidf> ipconfig /release  
  
/Users/davidf> ipconfig /renew
```

7. Join Windows machine to the Active Directory environment to check if previous configurations are correctly applied

- Windows 11 iso file download:

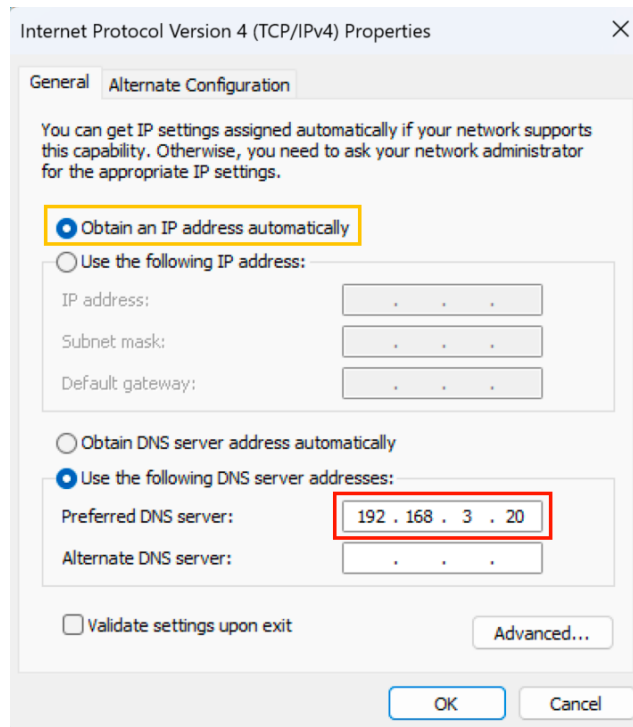
<https://www.microsoft.com/es-es/software-download/windows11>

Once you've downloaded the *iso* file go to the virtualization software of your preference and install it.

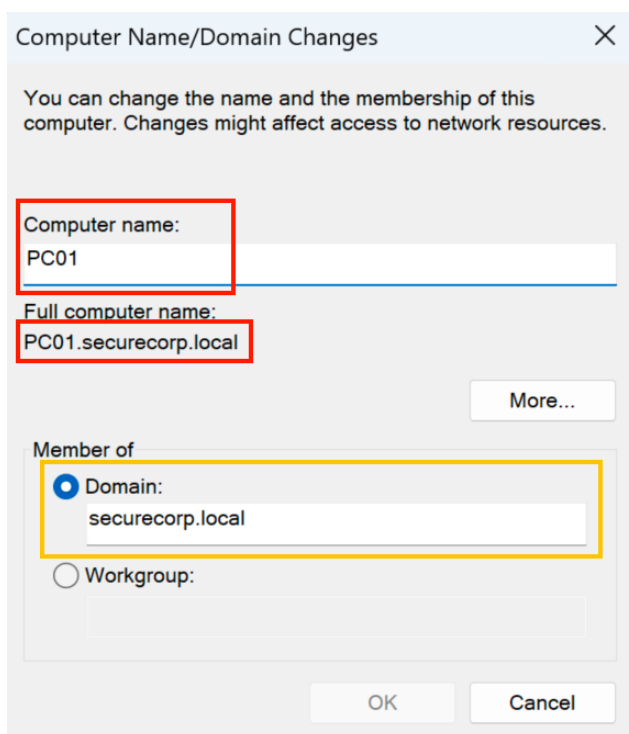
Now, follow this short guide to join the new VM to the AD domain services:

<https://rdr-it.io/en/windows-server-join-an-active-directory-domain/>

Ethernet client configuration



Domain and computer name configuration



IMPORTANT

It's crucial to implement “**Bridged Networking**” as network adapter for all the virtual machines of the environment, by doing that we guarantee that all

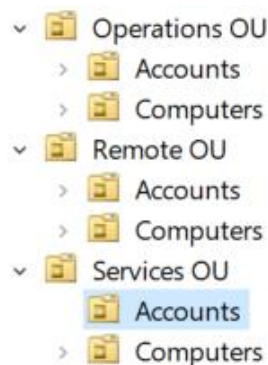
hosts are reachable inside the laboratory network (*SecHomeLab_Network*) for this particular case.

8. Create main OU(s) and user accounts

An Organizational Unity, also known as OU is a container that allows you to organize your AD objects, such as computers, users, groups and even other OUs. It's commonly used in real-world business to segment the company in departements (Sales, Marketing, IT, Finances).

Implementing OUs in this project has been the best way to organize and track network resources based on the role they play in the AD environment.

Organizational units structure



- **Services OU:** Contains AD services, including Remote Desktop services, vulnerability and security scanners.
- **Operations OU:** Includes non-privileged users, workstations, and employee-related groups in a business context.
- **Remote OU:** Remote users and VPN resources.

NOTE:

You can always add, delete or modify OUs as well as the network resources contained in them on the fly according to your needs. Just remember to refresh changes from “*Server Manager*” and log back in to make sure the changes are applied.

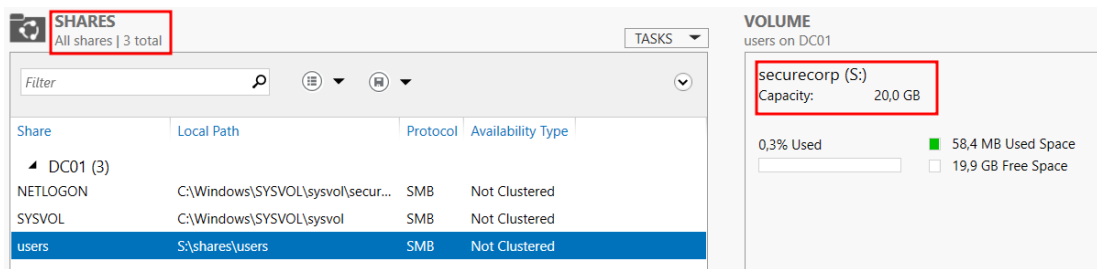
9. Configure “Folder redirection” through GPO (Optional)

Folder redirection enables users and administrators to redirect specific path(s) to a new location. It's useful to store data in a centralized location within the network.

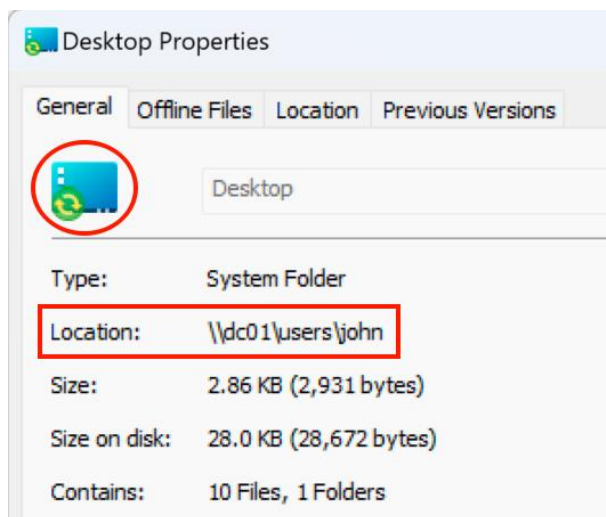
- Video tutorial:

https://www.youtube.com/watch?v=sys_QWLQRC0

Shares panel view



Redirected folder properties from client machine



By doing this:

- Only administrators and the folder's owner have access to the contents of the redirected folders.
- Redirected folders are stored on a dedicated disk.
- Administrators can track and monitor the information that users are working with on their workstations, ensuring security and enabling collaboration/sharing files or resources.

10. Create, configure and link Group Policy Object

A GPO is a collection of policy settings, security permissions and scope of management that are applied to users and computers within the AD environment.

- Video tutorial:

https://www.youtube.com/watch?v=VzogobjGag&list=PLLDjngo_4bmPWS4lMBEQdBMrQ1EH_mnhh&index=4

- Important Group Policy settings to prevent security breaches

<https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/>

NOTE:

The creation and application of GPOs are an indispensable practice for risk reduction, prevention of security breaches and protection of sensitive information in its infrastructures.

Troubleshooting

If you notice that GPO settings aren't being applied to user accounts or workstations, run the following command on the involved Windows workstations to ensure the new GPO settings are adopted:

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

11. Configure and secure Remote Desktop Protocol server

What's RDP and why use it?

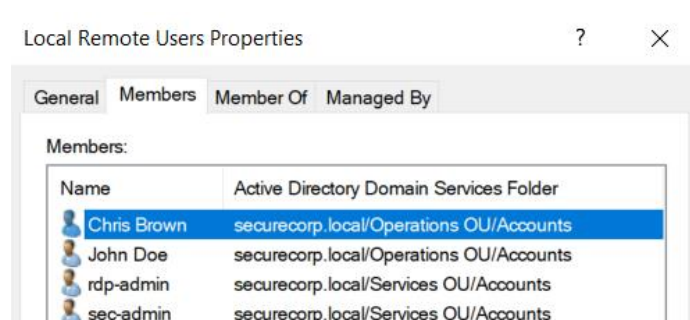
RDP or Remote Desktop Protocol is a secure network communication protocol that allows users and administrators to connect remotely to their physical workstations.

Among its most common use cases are:

- Remote troubleshooting
 - Remote desktop access
 - Remote administration
- Setup video tutorial:

<https://www.youtube.com/watch?v=Ba25sxbEHNs>

Local Remote Users group



RDP session into Ubuntu machine

```
chris@securecorp.local@PC03: ~/Desktop$ whoami
chris@securecorp.local
chris@securecorp.local@PC03: ~/Desktop$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.3.104 netmask 255.255.255.0 broadcast 192.168.3.255
    inet6 fe80::9b2:2d:2dc:c8f prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:58:5e:bd txqueuelen 1000 (Ethernet)
    RX packets 31062 bytes 2147564 (2.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 265143 bytes 370765166 (370.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 44 memory 0x3fe00000-3fe20000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 582 bytes 52910 (52.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 582 bytes 52910 (52.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

For the current lab a RDP server has been configured on a “*Windows 11 Enterprise*” VM to have a better organization and isolation of roles within the AD environment. By doing this:

- Only “*rdp-admin*” can RDP into specific users’s workstations that are members of “Local Remote Desktop Users” group.
- The “*rdp-admin*” can also use RDP to access an Ubuntu workstation, where security operations like vulnerability and host scanning are performed.

12. Setup VPN server with AD server via LDAP

The incorporation of a dedicated VPN server in this project broadens its scope and aligns it more closely with labor market demands. It enables remote users to access network resources and interact with network objects from anywhere, offering a practical solution in a world where teleworking is increasingly prevalent.

NOTE:

I've written a comprehensive article on how to install and configure OpenVPN on a dedicated server to manage remote user connections to the AD network:

- <https://davidf.io/2024/07/16/setup-ubuntu-server-as-vpn-server-on-active-directory-via-ldap/>

STRONG SECURITY FEATURES

13. Configure and perform vulnerability scans with “Nessus” (Security server)

- Setup video tutorial:

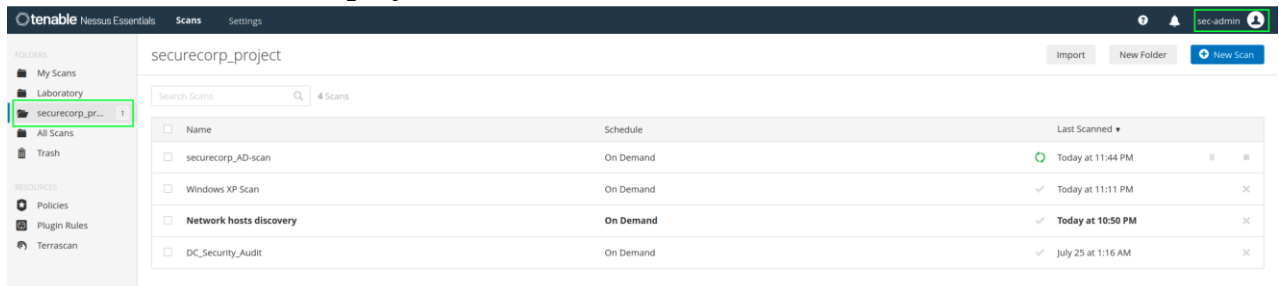
<https://www.youtube.com/watch?v=x87gbgQD4eg>

Nessus is a powerful security tool that enables a wide range of scans, including those on individual devices, web applications, network segments, and entire enterprise environments, covering both software and hardware.

The installation and configuration were carried out as follows:

- Set up Ubuntu Server on a VM.
- Install Nessus.
- Complete initial configuration.
- Execute scans on the Domain Controller (*DC01*), network segments, and specific workstations, utilizing “Host Discovery”, “Basic Network Scan”, and “Active Directory Starter Scan”.

Nessus dashboard with performed scans



The screenshot shows the Nessus dashboard interface. On the left, there is a sidebar with 'FOLDERS' (My Scans, Laboratory, securecorp_pr..., All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area displays the 'securecorp_project' with a search bar and a table of scans. The table has columns for Name, Schedule, and Last Scanned. The scans listed are: securecorp_AD-scan, Windows XP Scan, Network hosts discovery, and DC_Security_Audit.

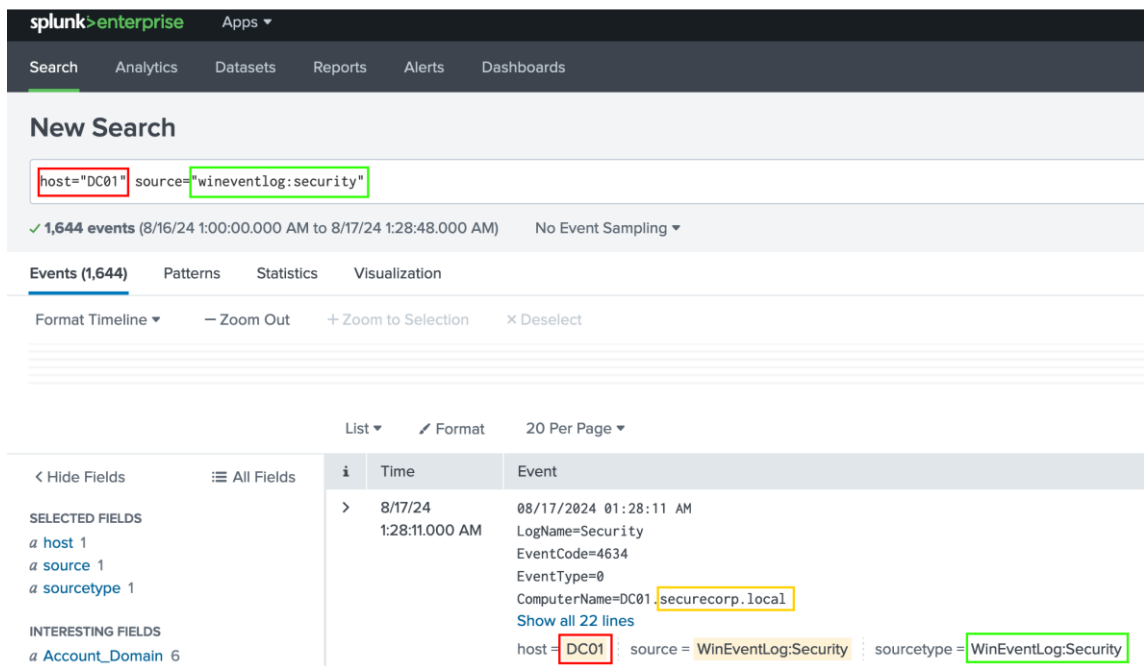
Name	Schedule	Last Scanned
securecorp_AD-scan	On Demand	Today at 11:44 PM
Windows XP Scan	On Demand	Today at 11:11 PM
Network hosts discovery	On Demand	Today at 10:50 PM
DC_Security_Audit	On Demand	July 25 at 1:16 AM

infhost binary output from Nessus server

```
+-----+
Machine Information
+-----+
[+] Local_IP_Address - 192.168.3.107
[+] Hostname - SEC-SCANNER.securecorp.local
[+] Username - sec-admin
[+] OS - Ubuntu 22.04.4 LTS
[+] Domain_Name - securecorp.local
[+] Domain_Software - active-directory
[+] Uptime - 1 hour,
[+] Host - VMware20,1
+-----+
```

14. Install and setup “Splunk Enterprise” as SIEM (Security Information and Event Management) platform

Splunk search panel



To effectively monitor and detect security and internal system events, I have implemented the following setup:

- Install Splunk Enterprise on an Ubuntu server.
- Configure the Splunk Universal Forwarder on the domain controller (DC01).

This configuration allows for the seamless redirection of security and system activity logs from the domain controller to the Splunk server. As a result, I can analyze and filter data through the Splunk dashboard, enabling timely detection of anomalous behaviors that could impact the performance and security of the root server.

– Splunk setup:

<https://hurricanelabs.com/splunk-tutorials/from-zero-to-splunk-how-to-install-splunk-on-a-linux-vm-in-minutes/>

– Event codes for threat hunting on Splunk

https://www.splunk.com/en_us/blog/security/threat-hunting-sysmon-event-codes.html

MALWARE SIMULATION & SPLUNK DETECTION

To align the implementation of Splunk with real-world scenarios, I undertook the following steps:

- Create a PowerShell Script:** On the “DC01” server, I developed a PowerShell script designed to simulate malware by pinging the

Raspberry Pi, which serves in the homelab project as the threat actor machine.

```
# threat actor ip
$ipAddress = "192.168.3.5"


# Set ping requests with time delay
while ($true) {
    ping $ipAddress -n 1

    Start-Sleep -Seconds 2
}
```

- b. **Compile the Script:** The PowerShell script (.ps1) was then compiled into an executable file (.exe).

```
ps2exe -inputFile file.ps1 -outputFile spotify.exe
```

- c. **Execute the File:** I ran the compiled executable file (.exe) on the server.

 C:\Users\Administrator\Music\spotify.exe

```
Ping statistics for 192.168.3.5:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms

Pinging 192.168.3.5 with 32 bytes of data:
Reply from 192.168.3.5: bytes=32 time=82ms TTL=64

Ping statistics for 192.168.3.5:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 82ms, Maximum = 82ms, Average = 82ms

Pinging 192.168.3.5 with 32 bytes of data:
Reply from 192.168.3.5: bytes=32 time=199ms TTL=64
```

- d. **Monitor ICMP Traffic:** On the Raspberry Pi (attacker machine), I configured it to listen for ICMP traces coming from the DC server by running the command:

```
sudo tcpdump -i wlan0 icmp
```

ICMP requests and responses

```
01:58:12.417504 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 661, length 40
01:58:14.670138 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 662, length 40
01:58:14.670290 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 662, length 40
01:58:16.748866 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 663, length 40
01:58:16.749017 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 663, length 40
01:58:18.971091 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 664, length 40
01:58:18.971244 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 664, length 40
01:58:21.224070 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 665, length 40
01:58:21.224225 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 665, length 40
01:58:23.388122 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 666, length 40
01:58:23.388280 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 666, length 40
01:58:25.526464 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 667, length 40
01:58:25.526636 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 667, length 40
01:58:27.675233 IP 192.168.3.20 > RASPBERRY: ICMP echo request, id 1, seq 668, length 40
01:58:27.675391 IP RASPBERRY > 192.168.3.20: ICMP echo reply, id 1, seq 668, length 40
```


- e. **Detect with Splunk:** Using Splunk's Search Processing Language (SPL), I analyzed the data to detect the simulated malware and trace its origins.

New Search Save A

```
sourcetype=wineventlog:security EventCode=4688
| stats count, values(Creator_Process_Name) as Creator_Process_Name by New_Process_Name
| table New_Process_Name, count, Creator_Process_Name
| sort count
```

43 of 43 events matched No Event Sampling ▾

Events Patterns **Statistics (5)** Visualization

20 Per Page ▾ Format

New_Process_Name ▾	count ▾	Creator_Process_Name ▾
C:\Program Files\SplunkUniversalForwarder\bin\splunk-MonitorNoHandle.exe	2	C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-netmon.exe	2	C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe	2	C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
C:\Program Files\SplunkUniversalForwarder\bin\splunk-powershell.exe	4	C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe
C:\Windows\System32\PING.EXE	33	C:\Users\Administrator\Music\spotify.exe

DETECTION & ANALYSIS:

As observed, Splunk has identified a new process (PING.EXE) originating from another process (spotify.exe), which corresponds to our malicious binary. This confirms the successful identification of a security threat. Next, we need to stop the execution of the binary and analyze the structure of the executable file using tools such as “*PEStudio*” to identify potential extensions of the binary.

In this case study, the malware performed minimal actions. However, in a real-world scenario, such malware could engage in various malicious activities, including insider trading, user credential theft, or establishing a persistent backdoor for ongoing access to the corporate network.

Troubleshooting

If you cannot access or find results related to Event Code 4688 (which pertains to process creation), on your forwarder machine, navigate to: *Local Security Policy > Advanced Audit Policy Configuration > System Audit Policies > Detailed Tracking*. Click on **Audit Process Creation** and set it to “**Success**”. This configuration will allow you to audit events generated when a process is created or started.

15. Securing network with pfSense firewall

Integrating a firewall into an enterprise network is crucial as it safeguards the private corporate network from unauthorized access, both on local area networks (LANs) and wide area networks (WANs).

- PfSense ISO Download:

<https://archive.org/details/pfSense-CE-2.6.0-RELEASE-amd64>

- PfSense Installation and configuration guide:

<https://blog.davidvarghese.dev/posts/building-home-lab-part-4/>

The previous configuration is ideal when all your components and workstations are hosted on the same virtualization software and host. This setup allows you to connect all your machines to the internal network of the firewall and interact among them without complications. Nevertheless, I have decided to implement a custom configuration for the following reasons:

- The project involves both physical and virtual machines.
- It includes machines hosted on two different virtualization platforms across various devices, making the task of connecting network adapters to internal VM networks complex.
- Seamless communication among all devices in the project is crucial.

pfSense management CLI view

```
FreeBSD/amd64 (pfSense.securecorp.lab) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 36d10f1350110cd1f4d2
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
SECURECORP (lan) -> em1      -> v4: 192.168.3.10/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Conclusions

Developing a “cybersecurity home lab” is a detailed and time-consuming project that involves the integration of various technologies, procedures, and configurations to achieve effective results. Through this project, a range of key skills and competencies have been acquired, including:

- Knowledge and troubleshooting of operations across various operating systems (Windows, Linux, Unix, and macOS)
- Understanding of network and protocols (TCP, IP, DHCP, ICMP, DNS)
- Proficiency with security tools (vulnerability scanners, SIEM solutions & firewalls)
- Proficiency with virtualization management tools (VMWare & VirtualBox)

- Problem-solving
- Understanding of Active Directory

SOURCES

Full documentation: <https://github.com/birdm4nw/Cybersecurity-HomeLab>

HomeLab reference:

https://www.youtube.com/watch?v=P85L2vwmBKA&list=PLLDjngo_4bmPWS4lMBEQdBMrQ1EH_mnhh

Join Ubuntu to AD: <https://mattglass-it.com/ubuntu-domain-join/>

RDP into Ubuntu machine on AD: <https://phoenixnap.com/kb/ubuntu-remote-desktop-from-windows>

Windows XP + Active Directory Troubleshooting:

<https://community.spiceworks.com/t/unable-to-join-xp-machine-to-domain/703165/11>

Nessus basics:

https://www.youtube.com/watch?v=x87gbgQD4eg&list=PLErQ2qAXz3rrvP91TPJfWrTd3niM_7AAx