The Lay of the land

Help

Learn about and get hands-on with common technologies and security products used in corporate environments; both host and network-based security solutions are covered.

Task 1 Introduction

It is essential to be familiar with the environment where you have initial access to a compromised machine during a red team engagement. Therefore, performing reconnaissance and enumeration is a significant part, and the primary goal is to gather as much information as possible to be used in the next stage.

With an initial foothold established, the post-exploitation process begins!

This room introduces commonly-used concepts, technologies, and security products that we need to be aware of.

In this room, the assumption is that we have already gained access to the machine, and we are ready to expand our knowledge more about the environment by performing enumerating for the following:

* Network infrastructure
* Active Directory Environment
* Users and Groups
* Host-based security solutions
* Network-based security solutions
* Applications and services

Task 2 Deploy the VM

 Start Machine

In order to follow along with the task content and apply what is given in this room, you need to start the attached machine by using the green Start Machine button in this task, and wait a few minutes for it to boot up. To access the attached machine, you can either use the split in browser view or connect through the RDP.

If you prefer to connect via RDP, make sure you deploy the AttackBox or connect to the VPN.

Use the following credentials: kkidd:Pass123321@.

Terminal

user@machine$ xfreerdp /v:10.10.159.173 /u:kkidd

Task 3  Network Infrastructure

Once arriving onto an unknown network, our first goal is to identify where we are and what we can get to. During the red team engagement, we need to understand what target system we are dealing with, what service the machine provides, what kind of network we are in. Thus, the enumeration of the compromised machine after getting initial access is the key to answering these questions. This task will discuss the common types of networks we may face during the engagement.

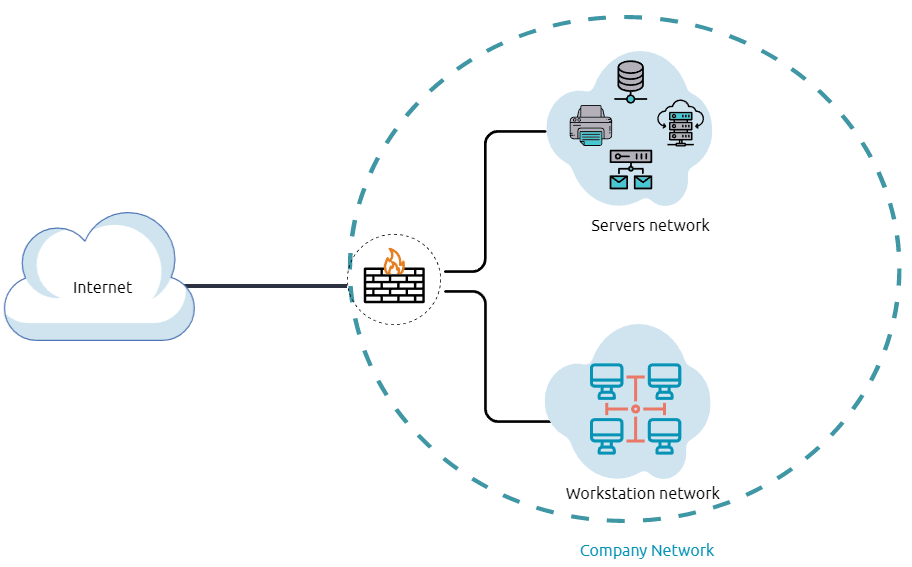
Network segmentation is an extra layer of network security divided into multiple subnets. It is used to improve the security and management of the network. For example, it is used for preventing unauthorized access to corporate most valuable assets such as customer data, financial records, etc.

The Virtual Local Area Networks (VLANs) is a network technique used in network segmentation to control networking issues, such as broadcasting issues in the local network, and improve security. Hosts within the VLAN can only communicate with other hosts in the same VLAN network.

If you want to learn more about network fundamentals, we suggest trying the following TryHackMe module: [Network Fundamentals](https://tryhackme.com/module/network-fundamentals).

Internal Networks

Internal Networks are subnetworks that are segmented and separated based on the importance of the internal device or the importance of the accessibility of its data. The main purpose of the internal network(s) is to share information, faster and easier communications, collaboration tools, operational systems, and network services within an organization. In a corporate network, the network administrators intend to use network segmentation for various reasons, including controlling network traffic, optimizing network performance, and improving security posture.

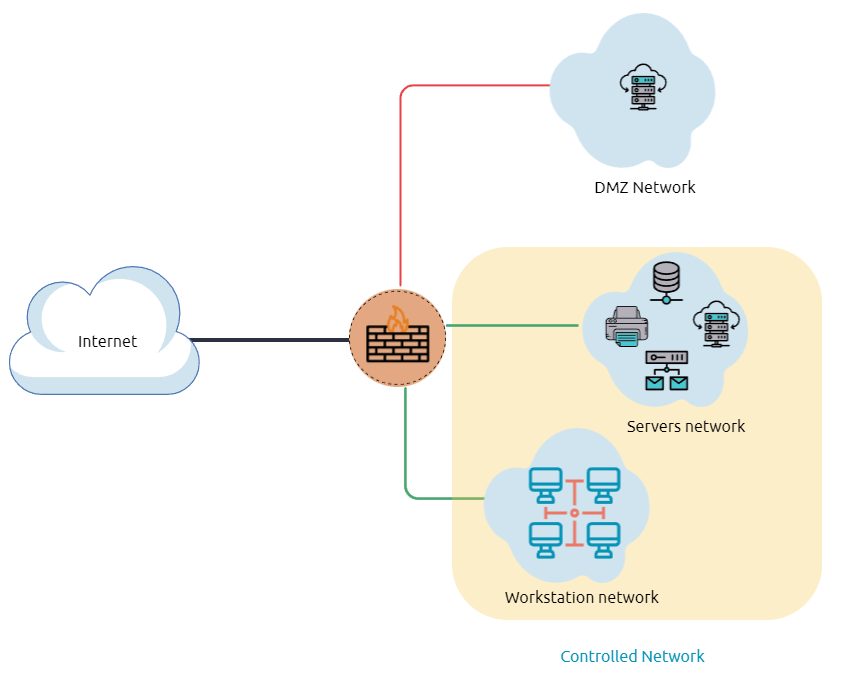


The previous diagram is an example of the simple concept of network segmentation as the network is divided into two networks. The first one is for employee workstations and personal devices. The second is for private and internal network devices that provide internal services such as DNS, internal web, email services, etc.

A Demilitarized Zone (DMZ)

A DMZ Network is an edge network that protects and adds an extra security layer to a corporation's internal local-area network from untrusted traffic. A common design for DMZ is a subnetwork that sits between the public internet and internal networks.

Designing a network within the company depends on its requirements and need. For example, suppose a company provides public services such as a website, DNS, FTP, Proxy, VPN, etc. In that case, they may design a DMZ network to isolate and enable access control on the public network traffic, untrusted traffic.



In the previous diagram, we represent the network traffic to the DMZ network in red color, which is untrusted ( comes directly from the internet). The green network traffic between the internal network is the controlled traffic that may go through one or more than one network security device(s).

Enumerating the system and the internal network is the discovering stage, which allows the attacker to learn about the system and the internal network. Based on the gained information, we use it to process lateral movement or privilege escalation to gain more privilege on the system or the AD environment.

Network Enumeration

There are various things to check related to networking aspects such as TCP and UDP ports and established connections, routing tables, ARP tables, etc.

Let's start checking the target machine's TCP and UDP open ports. This can be done using the netstat command as shown below.

Command Prompt

PS C:\Users\thm> netstat -na

Active Connections

Proto Local Address Foreign Address State

TCP 0.0.0.0:80 0.0.0.0:0 LISTENING

TCP 0.0.0.0:88 0.0.0.0:0 LISTENING

TCP 0.0.0.0:135 0.0.0.0:0 LISTENING

TCP 0.0.0.0:389 0.0.0.0:0 LISTENING

The output reveals the open ports as well as the established connections. Next, let's list the ARP table, which contains the IP address and the physical address of the computers that communicated with the target machines within the network. This could be helpful to see the communications within the network to scan the other machines for open ports and vulnerabilities.

Command Prompt

PS C:\Users\thm> arp -a

Interface: 10.10.141.51 --- 0xa

Internet Address Physical Address Type

10.10.0.1 02-c8-85-b5-5a-aa dynamic

10.10.255.255 ff-ff-ff-ff-ff-ff static

Internal Network Services

It provides private and internal network communication access for internal network devices. An example of network services is an internal DNS, web servers, custom applications, etc. It is important to note that the internal network services are not accessible outside the network. However, once we have initial access to one of the networks that access these network services, they will be reachable and available for communications.

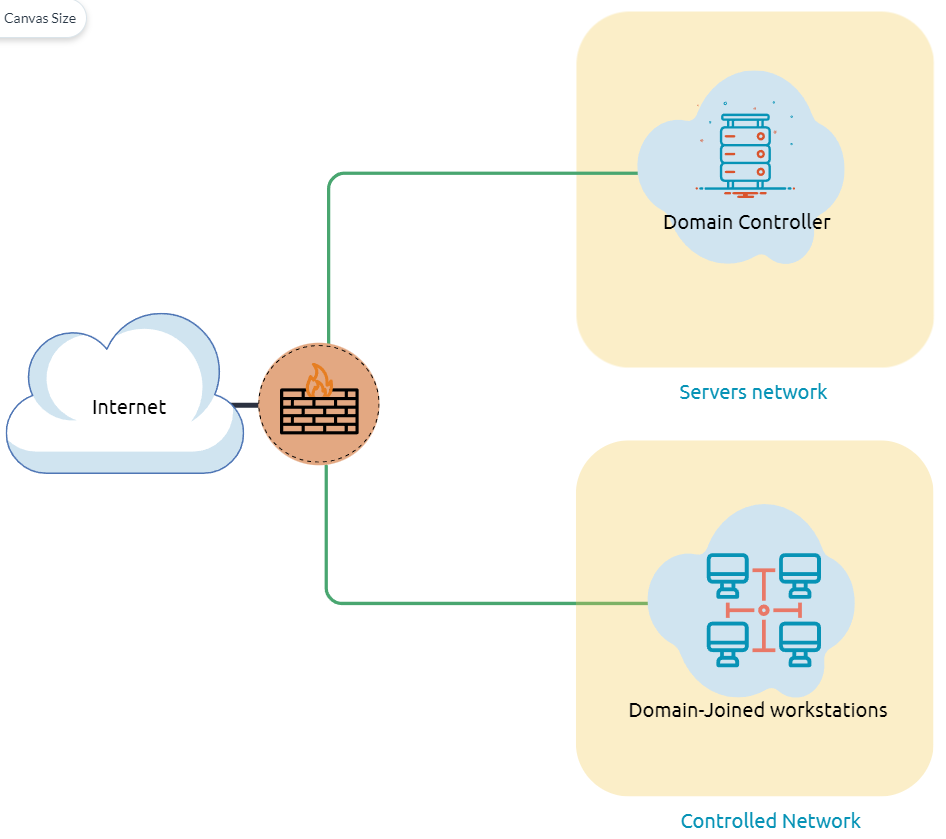
We will discuss more Windows applications and services in Task 9, including DNS and custom web applications.

Task 4  Active Directory (AD) environment

What is the Active Directory (AD) environment?



It is a Windows-based directory service that store and provide data objects to the internal network environment. It allows for centralized management of authentication and authorization. The AD contains essential information about the network and the environment, including users, computers, printers, etc. For example, AD might have users' details such as job title, phone number, address, passwords, groups, permission, etc.

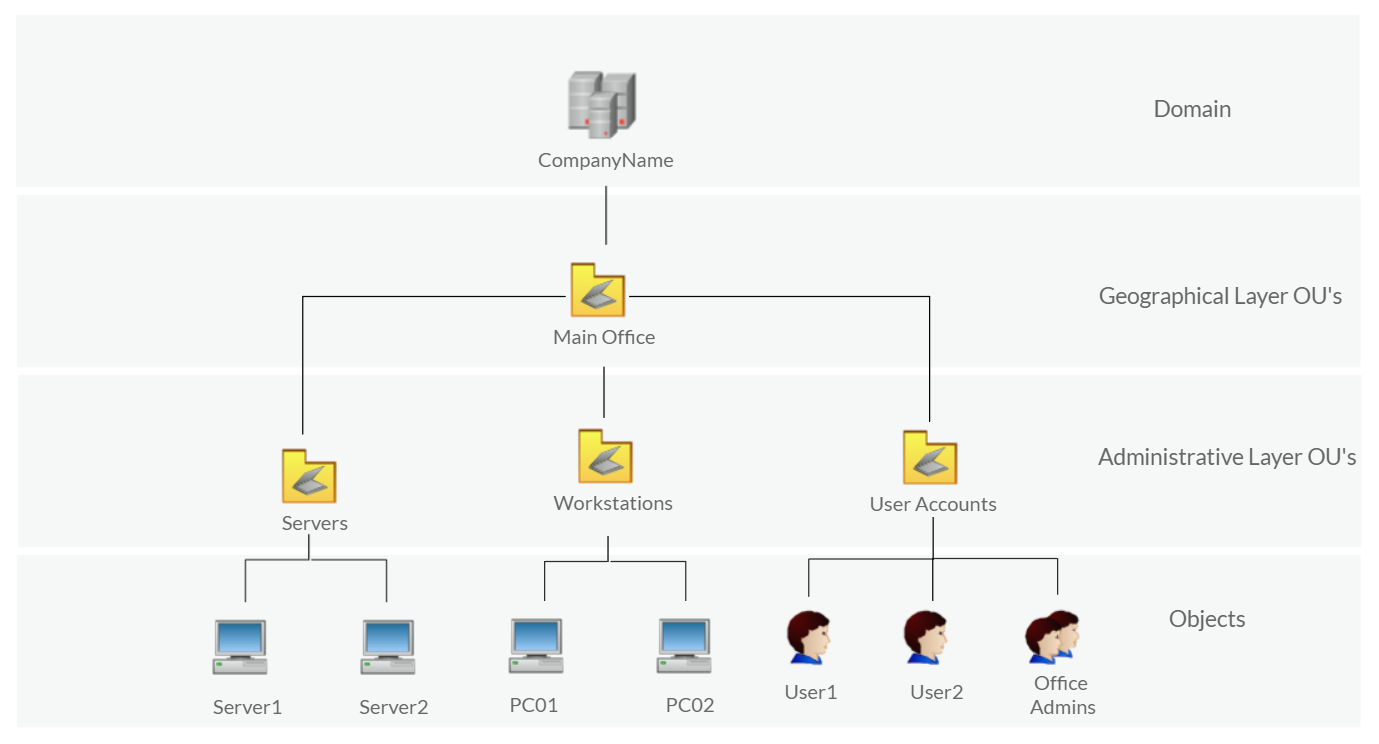


The diagram is one possible example of how Active Directory can be designed. The AD controller is placed in a subnet for servers (shown above as server network), and then the AD clients are on a separate network where they can join the domain and use the AD services via the firewall.

The following is a list of Active Directory components that we need to be familiar with:

* Domain Controllers
* Organizational Units
* AD objects
* AD Domains
* Forest
* AD Service Accounts: Built-in local users, Domain users, Managed service accounts
* Domain Administrators

A Domain Controller is a Windows server that provides Active Directory services and controls the entire domain. It is a form of centralized user management that provides encryption of user data as well as controlling access to a network, including users, groups, policies, and computers. It also enables resource access and sharing. These are all reasons why attackers target a domain controller in a domain because it contains a lot of high-value information.



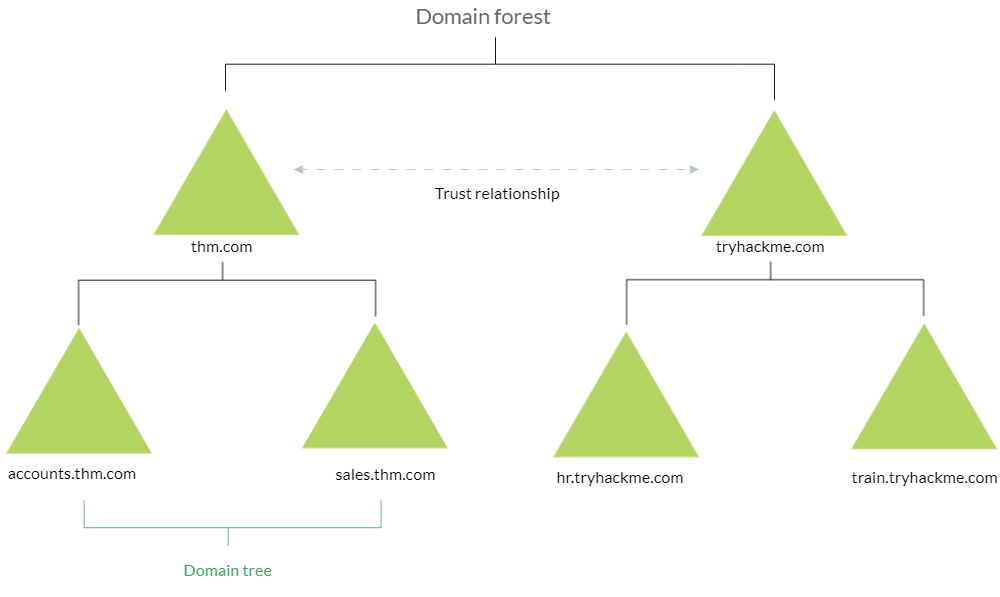
Organizational Units (OU's) are containers within the AD domain with a hierarchical structure.

Active Directory Objects can be a single user or a group, or a hardware component, such as a computer or printer. Each domain holds a database that contains object identity information that creates an AD environment, including:

* Users - A security principal that is allowed to authenticate to machines in the domain
* Computers - A special type of user accounts
* GPOs - Collections of policies that are applied to other AD objects

AD domains are a collection of Microsoft components within an AD network.

AD Forest is a collection of domains that trust each other.



For more information about the basics of Active Directory, we suggest trying the following TryHackMe room: [Active Directory Basics](https://tryhackme.com/room/activedirectorybasics).

Once Initial Access has been achieved, finding an AD environment in a corporate network is significant as the Active Directory environment provides a lot of information to joined users about the environment. As a red teamer, we take advantage of this by enumerating the AD environment and gaining access to various details, which can then be used in the lateral movement stage.

Answer the questions below

In order to check whether the Windows machine is part of the AD environment or not, one way, we can use the command prompt systeminfo command. The output of the systeminfo provides information about the machine, including the operating system name and version, hostname, and other hardware information as well as the AD domain.

Powershell

PS C:\Users\thm> systeminfo | findstr Domain

OS Configuration: Primary Domain Controller

Domain: thmdomain.com

From the above output, we can see that the computer name is an AD with thmdomain.com as a domain name which confirms that it is a part of the AD environment.

Note that if we get WORKGROUP in the domain section, then it means that this machine is part of a local workgroup.

Before going any further, ensure the attached machine is deployed and try what we discussed. Is the attached machine part of the AD environment? (Y|N)



 Submit

If it is part of an AD environment, what is the domain name of the AD?

Task 5  Users and Groups Management

In this task, we will learn more about users and groups, especially within the Active Directory. Gathering information about the compromised machine is essential that could be used in the next stage. Account discovery is the first step once we have gained initial access to the compromised machine to understand what we have and what other accounts are in the system.



An Active Directory environment contains various accounts with the necessary permissions, access, and roles for different purposes. Common Active Directory service accounts include built-in local user accounts, domain user accounts, managed service accounts, and virtual accounts.

* The built-in local users' accounts are used to manage the system locally, which is not part of the AD environment.
* Domain user accounts with access to an active directory environment can use the AD services (managed by AD).
* AD managed service accounts are limited domain user account with higher privileges to manage AD services.
* Domain Administrators are user accounts that can manage information in an Active Directory environment, including AD configurations, users, groups, permissions, roles, services, etc. One of the red team goals in engagement is to hunt for information that leads to a domain administrator having complete control over the AD environment.

The following are Active Directory Administrators accounts:

|  |  |
| --- | --- |
| BUILTIN\Administrator | Local admin access on a domain controller |
| Domain Admins | Administrative access to all resources in the domain |
| Enterprise Admins | Available only in the forest root |
| Schema Admins | Capable of modifying domain/forest; useful for red teamers |
| Server Operators | Can manage domain servers |
| Account Operators | Can manage users that are not in privileged groups |

Now that we learn about various account types within the AD environment. Let's enumerate the Windows machine that we have access to during the initial access stage. As a current user, we have specific permissions to view or manage things within the machine and the AD environment.

Active Directory (AD) Enum

Now, enumerating in the AD environment requires different tools and techniques. Once we confirm that the machine is part of the AD environment, we can start hunting for any variable info that may be used later. In this stage, we are using PowerShell to enumerate for users and groups.

The following PowerShell command is to get all active directory user accounts. Note that we need to use  -Filter argument.

PowerShell

PS C:\Users\thm> Get-ADUser -Filter \*

DistinguishedName : CN=Administrator,CN=Users,DC=thmredteam,DC=com

Enabled : True

GivenName :

Name : Administrator

ObjectClass : user

ObjectGUID : 4094d220-fb71-4de1-b5b2-ba18f6583c65

SamAccountName : Administrator

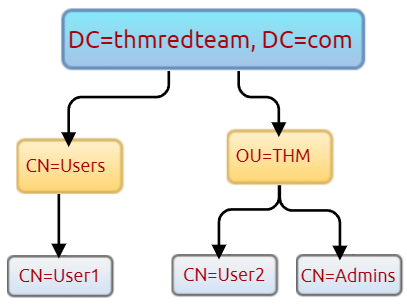
SID : S-1-5-21-1966530601-3185510712-10604624-500

Surname :

UserPrincipalName :

PS C:\Users\thm>

We can also use the [LDAP hierarchical tree structure](http://www.ietf.org/rfc/rfc2253.txt) to find a user within the AD environment. The Distinguished Name (DN) is a collection of comma-separated key and value pairs used to identify unique records within the directory. The DN consists of Domain Component (DC), OrganizationalUnitName (OU), Common Name (CN), and others. The following "CN=User1,CN=Users,DC=thmredteam,DC=com" is an example of DN, which can be visualized as follow:



Using the SearchBase option, we specify a specific Common-Name CN in the active directory. For example, we can specify to list any user(s) that part of Users.

PowerShell

PS C:\Users\thm> Get-ADUser -Filter \* -SearchBase "CN=Users,DC=THMREDTEAM,DC=COM"

DistinguishedName : CN=Administrator,CN=Users,DC=thmredteam,DC=com

Enabled : True

GivenName :

Name : Administrator

ObjectClass : user

ObjectGUID : 4094d220-fb71-4de1-b5b2-ba18f6583c65

SamAccountName : Administrator

SID : S-1-5-21-1966530601-3185510712-10604624-500

Surname :

UserPrincipalName :

Note that the result may contain more than one user depending on the configuration of the CN. Try the command to find all users within the THM OU and answer question 1 below.

Answer the questions below

Use the Get-ADUser -Filter \* -SearchBase command to list the available user accounts within THM OU in the thmredteam.com domain. How many users are available?



 Submit

 Hint

Once you run the previous command, what is the UserPrincipalName (email) of the admin account?



Task 6  Host Security Solution #1

Before performing further actions, we need to obtain general knowledge about the security solutions in place. Remember, it is important to enumerate antivirus and security detection methods on an endpoint in order to stay as undetected as possible and reduce the chance of getting caught.

This task will discuss the common security solution used in corporate networks, divided into Host and Network security solutions.

Host Security Solutions



It is a set of software applications used to monitor and detect abnormal and malicious activities within the host, including:

1. Antivirus software
2. Microsoft Windows Defender
3. Host-based Firewall
4. Security Event Logging and Monitoring
5. Host-based Intrusion Detection System (HIDS)/ Host-based Intrusion Prevention System (HIPS)
6. Endpoint Detection and Response (EDR)

Let's go more detail through the host-based security solutions that we may encounter during the red team engagement.

Antivirus Software (AV)

Antivirus software also known as anti-malware, is mainly used to monitor, detect, and prevent malicious software from being executed within the host.  Most antivirus software applications use well-known features, including Background scanning, Full system scans, Virus definitions. In the background scanning, the antivirus software works in real-time and scans all open and used files in the background. The full system scan is essential when you first install the antivirus. The most interesting part is the virus definitions, where antivirus software replies to the pre-defined virus. That's why antivirus software needs to update from time to time.

There are various detection techniques that the antivirus uses, including

* Signature-based detection
* Heuristic-based detection
* Behavior-based detection

Signature-based detection is one of the common and traditional techniques used in antivirus software to identify malicious files. Often, researchers or users submit their infected files into an antivirus engine platform for further analysis by AV vendors, and if it confirms as malicious, then the signature gets registered in their database. The antivirus software compares the scanned file with a database of known signatures for possible attacks and malware on the client-side. If we have a match, then it considers a threat.

Heuristic-based detection uses machine learning to decide whether we have the malicious file or not. It scans and statically analyses in real-time in order to find suspicious properties in the application's code or check whether it uses uncommon Windows or system APIs. It does not rely on the signature-based attack in making the decisions, or sometimes it does. This depends on the implementation of the antivirus software.

Finally, Behavior-based detection relies on monitoring and examining the execution of applications to find abnormal behaviors and uncommon activities, such as creating/updating values in registry keys, killing/creating processes, etc.

As a red teamer, it is essential to be aware of whether antivirus exists or not. It prevents us from doing what we are attempting to do. We can enumerate AV software using Windows built-in tools, such as wmic.

PowerShell

PS C:\Users\thm> wmic /namespace:\\root\securitycenter2 path antivirusproduct

This also can be done using PowerShell, which gives the same result.

PowerShell

PS C:\Users\thm> Get-CimInstance -Namespace root/SecurityCenter2 -ClassName AntivirusProduct

displayName : Bitdefender Antivirus

instanceGuid : {BAF124F4-FA00-8560-3FDE-6C380446AEFB}

pathToSignedProductExe : C:\Program Files\Bitdefender\Bitdefender Security\wscfix.exe

pathToSignedReportingExe : C:\Program Files\Bitdefender\Bitdefender Security\bdservicehost.exe

productState : 266240

timestamp : Wed, 15 Dec 2021 12:40:10 GMT

PSComputerName :

displayName : Windows Defender

instanceGuid : {D58FFC3A-813B-4fae-9E44-DA132C9FAA36}

pathToSignedProductExe : windowsdefender://

pathToSignedReportingExe : %ProgramFiles%\Windows Defender\MsMpeng.exe

productState : 393472

timestamp : Fri, 15 Oct 2021 22:32:01 GMT

PSComputerName :

As a result, there is a third-party antivirus (Bitdefender Antivirus) and Windows Defender installed on the computer. Note that Windows servers may not have SecurityCenter2 namespace, which may not work on the attached VM. Instead, it works for Windows workstations!

Microsoft Windows Defender

Microsoft Windows Defender is a pre-installed antivirus security tool that runs on endpoints. It uses various algorithms in the detection, including machine learning, big-data analysis, in-depth threat resistance research, and Microsoft cloud infrastructure in protection against malware and viruses. MS Defender works in three protection modes: Active, Passive, Disable modes.

Active mode is used where the MS Defender runs as the primary antivirus software on the machine where provides protection and remediation. Passive mode is run when a 3rd party antivirus software is installed. Therefore, it works as secondary antivirus software where it scans files and detects threats but does not provide remediation. Finally, Disable mode is when the MS Defender is disabled or uninstalled from the system.

 We can use the following PowerShell command to check the service state of Windows Defender:

PowerShell

PS C:\Users\thm> Get-Service WinDefend

Status Name DisplayName

------ ---- -----------

Running WinDefend Windows Defender Antivirus Service

Next, we can start using the Get-MpComputerStatus cmdlet to get the current Windows Defender status. However, it provides the current status of security solution elements, including Anti-Spyware, Antivirus, LoavProtection, Real-time protection, etc. We can use select to specify what we need for as follows,

PowerShell

PS C:\Users\thm> Get-MpComputerStatus | select RealTimeProtectionEnabled

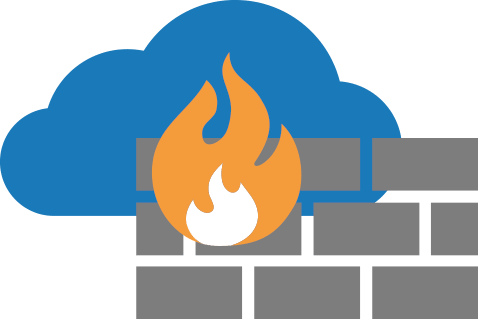
RealTimeProtectionEnabled

-------------------------

False

As a result, MpComputerStatus highlights whether Windows Defender is enabled or not.

3. Host-based Firewall: It is a security tool installed and run on a host machine that can prevent and block attacker or red teamers' attack attempts. Thus, it is essential to enumerate and gather details about the firewall and its rules within the machine we have initial access to.



The main purpose of the host-based firewall is to control the inbound and outbound traffic that goes through the device's interface. It protects the host from untrusted devices that are on the same network. A modern host-based firewall uses multiple levels of analyzing traffic, including packet analysis, while establishing the connection.

A firewall acts as control access at the network layer. It is capable of allowing and denying network packets. For example, a firewall can be configured to block ICMP packets sent through the ping command from other machines in the same network. Next-generation firewalls also can inspect other OSI layers, such as application layers. Therefore, it can detect and block SQL injection and other application-layer attacks.

PowerShell

PS C:\Users\thm> Get-NetFirewallProfile | Format-Table Name, Enabled

Name Enabled

---- -------

Domain True

Private True

Public True

If we have admin privileges on the current user we logged in with, then we try to disable one or more than one firewall profile using the Set-NetFirewallProfile cmdlet.

PowerShell

PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False

PS C:\Windows\system32> Get-NetFirewallProfile | Format-Table Name, Enabled

---- -------

Domain False

Private False

Public False

We can also learn and check the current Firewall rules, whether allowing or denying by the firewall.

PowerShell

PS C:\Users\thm> Get-NetFirewallRule | select DisplayName, Enabled, Description

DisplayName Enabled

----------- -------

Virtual Machine Monitoring (DCOM-In) False

Virtual Machine Monitoring (Echo Request - ICMPv4-In) False

Virtual Machine Monitoring (Echo Request - ICMPv6-In) False

Virtual Machine Monitoring (NB-Session-In) False

Virtual Machine Monitoring (RPC) False

SNMP Trap Service (UDP In) False

SNMP Trap Service (UDP In) False

Connected User Experiences and Telemetry True

Delivery Optimization (TCP-In) True

During the red team engagement, we have no clue what the firewall blocks. However, we can take advantage of some PowerShell cmdlets such as Test-NetConnection and TcpClient. Assume we know that a firewall is in place, and we need to test inbound connection without extra tools, then we can do the following:

PowerShell

PS C:\Users\thm> Test-NetConnection -ComputerName 127.0.0.1 -Port 80

ComputerName : 127.0.0.1

RemoteAddress : 127.0.0.1

RemotePort : 80

InterfaceAlias : Loopback Pseudo-Interface 1

SourceAddress : 127.0.0.1

TcpTestSucceeded : True

PS C:\Users\thm> (New-Object System.Net.Sockets.TcpClient("127.0.0.1", "80")).Connected

True

As a result, we can confirm the inbound connection on port 80 is open and allowed in the firewall. Note that we can also test for remote targets in the same network or domain names by specifying in the -ComputerName argument for the Test-NetConnection.

Answer the questions below

Enumerate the attached Windows machine and check whether the host-based firewall is enabled or not! (Y|N)



 Submit

Using PowerShell cmdlets such Get-MpThreat can provide us with threats details that have been detected using MS Defender. Run it and answer the following: What is the file name that causes this alert to record?



 Submit

 Hint

Enumerate the firewall rules of the attached Windows machine. What is the port that is allowed under the THM-Connection rule?



 Submit

 Hint

In the next task, we will keep discussing the host security solution. I'm ready!



 Completed

Task 7  Host Security Solution #2

In this task, we will keep discussing host security solutions.

Security Event Logging and Monitoring



By default, Operating systems log various activity events in the system using log files. The event logging feature is available to the IT system and network administrators to monitor and analyze important events, whether on the host or the network side. In cooperating networks, security teams utilize the logging event technique to track and investigate security incidents.

There are various categories where the Windows operating system logs event information, including the application, system, security, services, etc. In addition, security and network devices store event information into log files to allow the system administrators to get an insight into what is going on.

We can get a list of available event logs on the local machine using the Get-EventLog cmdlet.

PowerShell

PS C:\Users\thm> Get-EventLog -List

Max(K) Retain OverflowAction Entries Log

------ ------ -------------- ------- ---

512 7 OverwriteOlder 59 Active Directory Web Services

20,480 0 OverwriteAsNeeded 512 Application

512 0 OverwriteAsNeeded 170 Directory Service

102,400 0 OverwriteAsNeeded 67 DNS Server

20,480 0 OverwriteAsNeeded 4,345 System

15,360 0 OverwriteAsNeeded 1,692 Windows PowerShell

Sometimes, the list of available event logs gives you an insight into what applications and services are installed on the machine! For example, we can see that the local machine has Active Directory, DNS server, etc. For more information about the Get-EventLog cmdlet with examples, visit the [Microsoft documents website](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-eventlog?view=powershell-5.1).

In corporate networks, log agent software is installed on clients to collect and gather logs from different sensors to analyze and monitor activities within the network. We will discuss them more in the Network Security Solution task.

System Monitor (Sysmon)



Windows System Monitor sysmon is a service and device driver. It is one of the Microsoft Sysinternals suites. The sysmon tool is not an essential tool (not installed by default), but it starts gathering and logging events once installed. These logs indicators can significantly help system administrators and blue teamers to track and investigate malicious activity and help with general troubleshooting.

One of the great features of the sysmon  tool is that it can log many important events, and you can also create your own rule(s) and configuration to monitor:

* Process creation and termination
* Network connections
* Modification on file
* Remote threats
* Process and memory access
* and many others

For learning more about sysmon, visit the Windows document page [here](https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon).

As a red teamer, one of the primary goals is to stay undetectable, so it is essential to be aware of these tools and avoid causing generating and alerting events. The following are some of the tricks that can be used to detect whether the sysmon is available in the victim machine or not.

We can look for a process or service that has been named "Sysmon" within the current process or services as follows,

PowerShell

PS C:\Users\thm> Get-Process | Where-Object { $\_.ProcessName -eq "Sysmon" }

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName

------- ------ ----- ----- ------ -- -- -----------

373 15 20212 31716 3316 0 Sysmon

or look for services as follows,

PowerShell

PS C:\Users\thm> Get-CimInstance win32\_service -Filter "Description = 'System Monitor service'"

**#** or

Get-Service | where-object {$\_.DisplayName -like "\*sysm\*"}

It also can be done by checking the Windows registry

PowerShell

PS C:\Users\thm> reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Sysmon/Operational

All these commands confirm if the sysmon tool is installed. Once we detect it, we can try to find the sysmon configuration file if we have readable permission to understand what system administrators are monitoring.

PowerShell

PS C:\Users\thm> findstr /si '<ProcessCreate onmatch="exclude">' C:\tools\\*

C:\tools\Sysmon\sysmonconfig.xml:

C:\tools\Sysmon\sysmonconfig.xml:

For more detail about the Windows sysmon tool and how to utilize it within endpoints, we suggest trying the TryHackMe room: [Sysmon](https://tryhackme.com/room/sysmon" \t "_blank).

Host-based Intrusion Detection/Prevention System (HIDS/HIPS)



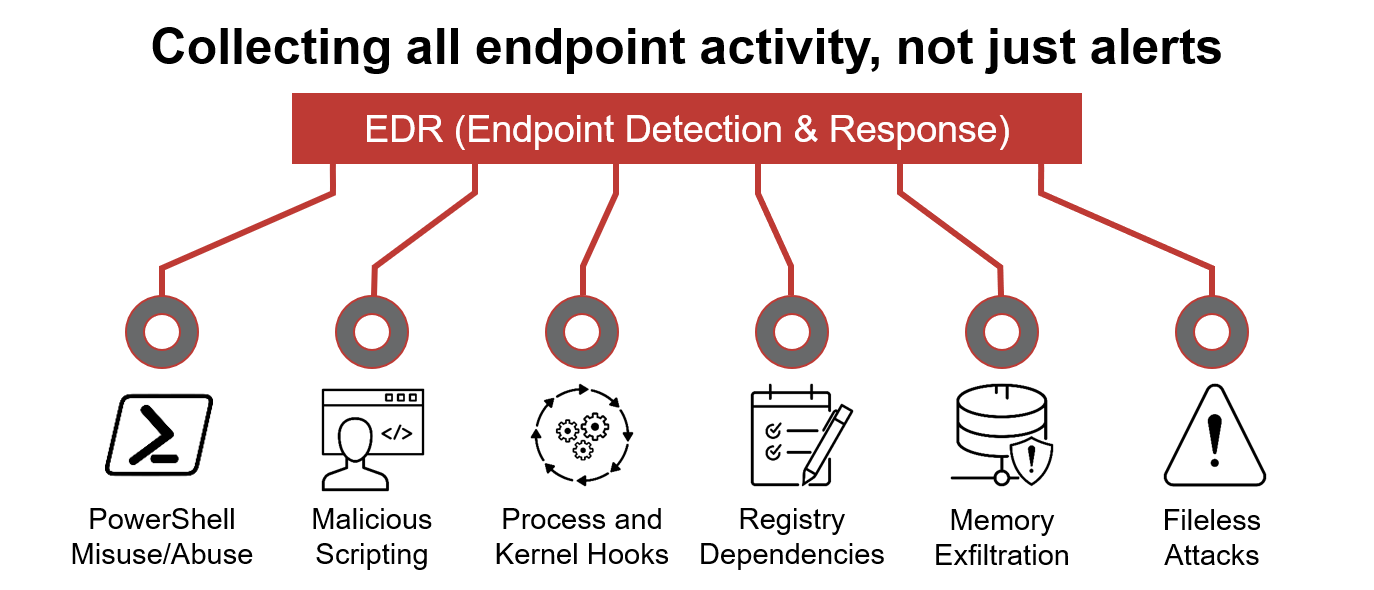
**HIDS**stands for Host-based Intrusion Detection System. It is software that has the ability to monitor and detect abnormal and malicious activities in a host. The primary purpose of HIDS is to detect suspicious activities and not to prevent them. There are two methods that the host-based or network intrusion detection system works, including:

* Signature-based IDS - it looks at checksums and message authentication.
* Anomaly-based IDS looks for unexpected activities, including abnormal bandwidth usage, protocols, and ports.

Host-based Intrusion Prevention Systems (**HIPS**) works by securing the operating system activities which where is installed. It is a detecting and prevention solution against well-known attacks and abnormal behaviors. HIPS is capable of auditing log files of the host, monitoring processes, and protecting system resources. HIPS is a mixture of best product features such as antivirus, behavior analysis, network, application firewall, etc.

There is also a network-based IDS/IPS, which we will be covering in the next task.

Endpoint Detection and Response (EDR)



It is also known as Endpoint Detection and Threat Response (EDTR). The EDR is a cybersecurity solution that defends against malware and other threats. EDRs can look for malicious files, monitor endpoint, system, and network events, and record them in a database for further analysis, detection, and investigation. EDRs are the next generation of antivirus and detect malicious activities on the host in real-time.

EDR analyze system data and behavior for making section threats, including

* Malware, including viruses, trojans, adware, keyloggers
* Exploit chains
* Ransomware

Below are some common EDR software for endpoints

* Cylance
* Crowdstrike
* Symantec
* SentinelOne
* Many others

Even though an attacker successfully delivered their payload and bypassed EDR in receiving reverse shell, EDR is still running and monitors the system. It may block us from doing something else if it flags an alert.

We can use scripts for enumerating security products within the machine, such as [Invoke-EDRChecker](https://github.com/PwnDexter/Invoke-EDRChecker) and [SharpEDRChecker](https://github.com/PwnDexter/SharpEDRChecker" \t "_blank). They check for commonly used Antivirus, EDR, logging monitor products by checking file metadata, processes, DLL loaded into current processes, Services, and drivers, directories.

***Answer the questions below***

We covered some of the common security endpoints we may encounter during the red team engagement. Let's discuss the network-based security solutions in the next task!



 Completed