# Top 3 Security Vulnerabilities in Windows 7

**PRESENTATION**

By Rawan Masoud

# Presentation agenda

-HISTORY OF WINDOWYS 7

-EternalBlue

-Print Spooler Vulnerability

-BlueKeep

-EternalBlue exploit implementation

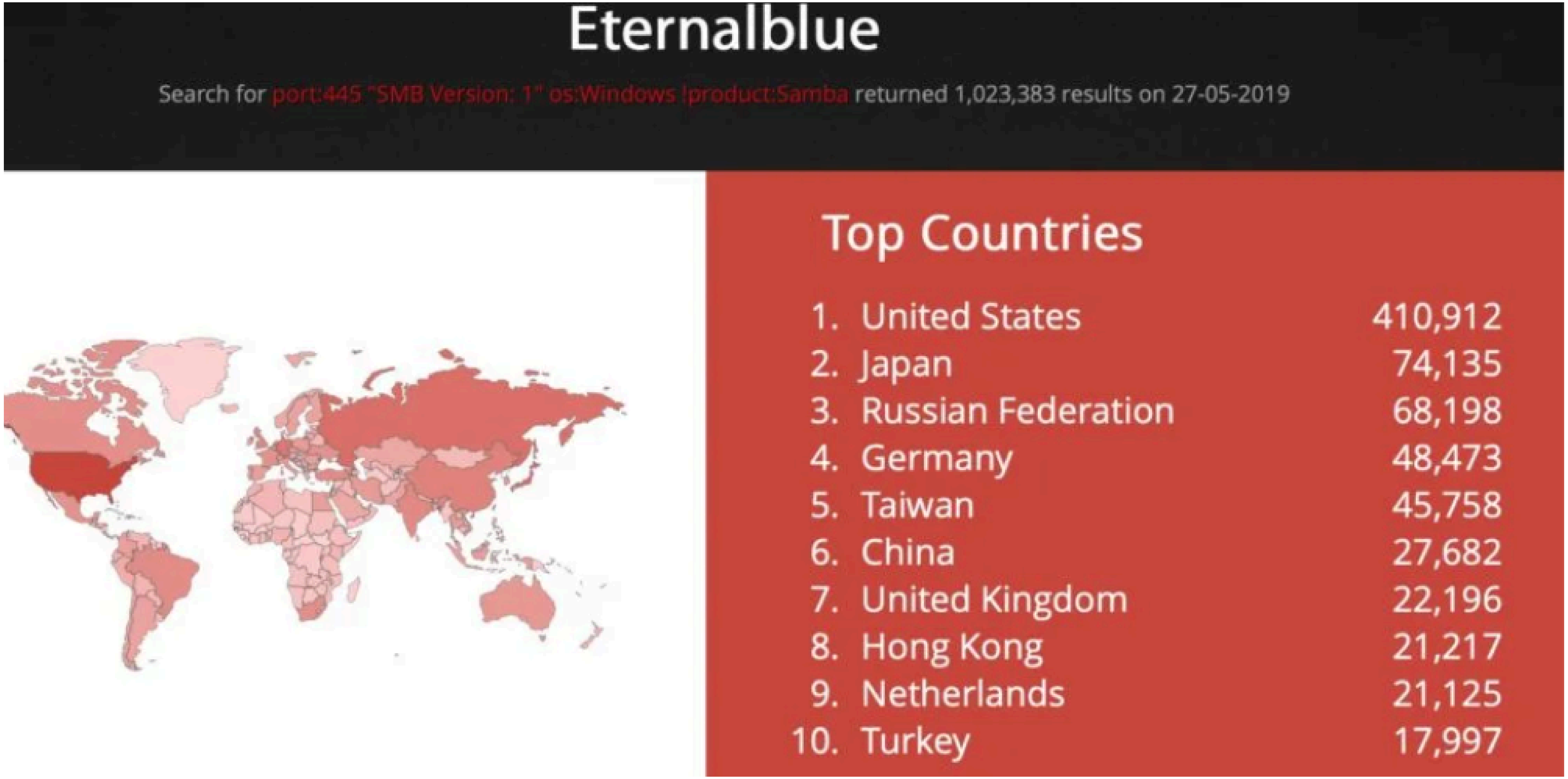
# INTRODUCTION TO WINDOWS 7

- Released in 2009 and widely used worldwide
- Microsoft ended official security support in January 2020
- No security updates or patches since then.
- Still used on many systems—making it a prime target

# 1.ETERNALBLUE (CVE-2017-0144)

- EternalBlue is a critical vulnerability in the SMB
- Type: Remote Code Execution (RCE)
- The vulnerability was discovered secretly by the US National Security Agency (NSA) and then leaked to the public in 2017 by a hacking group called Shadow Brokers.

# WIDESPREAD IS ETERNALBLUE



## Eternalblue

Search for port:445 "SMB Version: 1" os:Windows !product:Samba returned 1,023,383 results on 27-05-2019

### Top Countries

| | | |
|---|---|---|
| 1. | United States | 410,912 |
| 2. | Japan | 74,135 |
| 3. | Russian Federation | 68,198 |
| 4. | Germany | 48,473 |
| 5. | Taiwan | 45,758 |
| 6. | China | 27,682 |
| 7. | United Kingdom | 22,196 |
| 8. | Hong Kong | 21,217 |
| 9. | Netherlands | 21,125 |
| 10. | Turkey | 17,997 |

# HOW DOES THE VULNERABILITY WORK?

- Technical vulnerability: It allows an attacker to remotely execute malicious code on a victim's device without a username or password by exploiting a flaw in the SMB packet handling protocol.

- Classified in global vulnerability lists :
  CVSS rating: 8.1/10 (high severity).

# NOTORIOUS ATTACKS THAT USED ETERNALBLUE:

- WannaCry attack ( 2017 )
- NotPetya attack (2017)

# 2. MS10-061 – PRINT SPOOLER – CVE-2010-2729

- MS10-061 is a critical vulnerability in the Windows Print Spooler service, which controls print job management.

- Discovery date: Announced in September 2010 by Microsoft as part of its monthly Patch Tuesday security updates.

# 2. MS10-061 – PRINT SPOOLER – CVE-2010-2729

- Type: Privilege Escalation and RCE

- The vulnerability occurs due to the service's poor verification of user privileges when adding a network printer.

# ATTACK MECHANISM:

- An attacker exploits the RPC (Remote Procedure Call) protocol to send commands to the Print Spooler service

- Because the service runs with SYSTEM privileges (the highest privilege in Windows), the entire device becomes under the attacker's control.

# NOTORIOUS ATTACKS USING THE VULNERABILITY:

- Stuxnet Attack (2010)
- Severity Rating (CVSS): 9.3/10 (Critical) due to its ease of exploitation and significant impact.

# BLUEKEEP–CVE-2019-0708

- Description: A critical vulnerability in the Remote Desktop Protocol (RDP) service that allows remote code execution (RCE) without user authentication (zero-click).

- Discovery Date: May 2019 (Microsoft announced it and released an emergency update even for older Windows systems such as Windows XP and 7).

# BLUEKEEP–CVE-2019-0708

- Classification: One of the most critical vulnerabilities because it can be exploited to create an internet worm that spreads automatically between machines.

# WHY IS IT CONSIDERED CRITICAL?

- Allows an attacker to take full control of a machine remotely (even without a user present).
- Can spread as a worm across networks
- CVSS Score: 10/10 (highest severity).

# HOW DOES THE VULNERABILITY WORK?

Technical Cause: A flaw in the handling of RDP requests (especially when trying to connect to an unauthenticated device).

# ATTACK MECHANISM:

- An attacker sends a malicious RDP request to port 3389.

- The flaw in the service causes a buffer overflow.

- Malicious code is executed with SYSTEM privileges (the highest privilege).

# HAS IT BEEN EXPLOITED IN ACTUAL ATTACKS?

Large-scale attacks like WannaCry have not been documented, but:

- Exploits for it have been developed in tools like Metasploit.
- Microsoft has warned that exploiting it could lead to a "perfect storm" similar to the one caused by WannaCry.

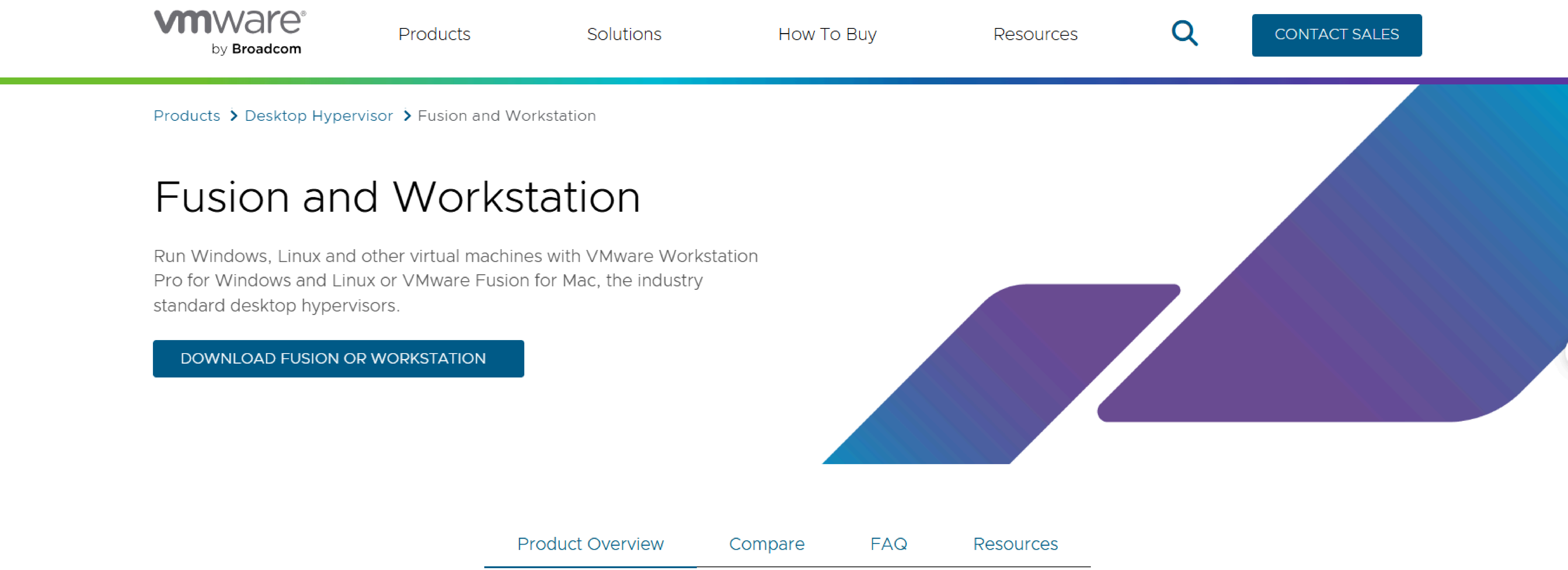
# ETERNALBLUE EXPLOIT IMPLEMENTATION

- Tools
- Technique

# TOOLS

- Virtual machine ( Vmware stations)
- Installing Kali Linux ( attacker )
- Installing Windows 7 ( victim)

# STEPS TO DOWNLOAD THE  (VMWARE STATION)

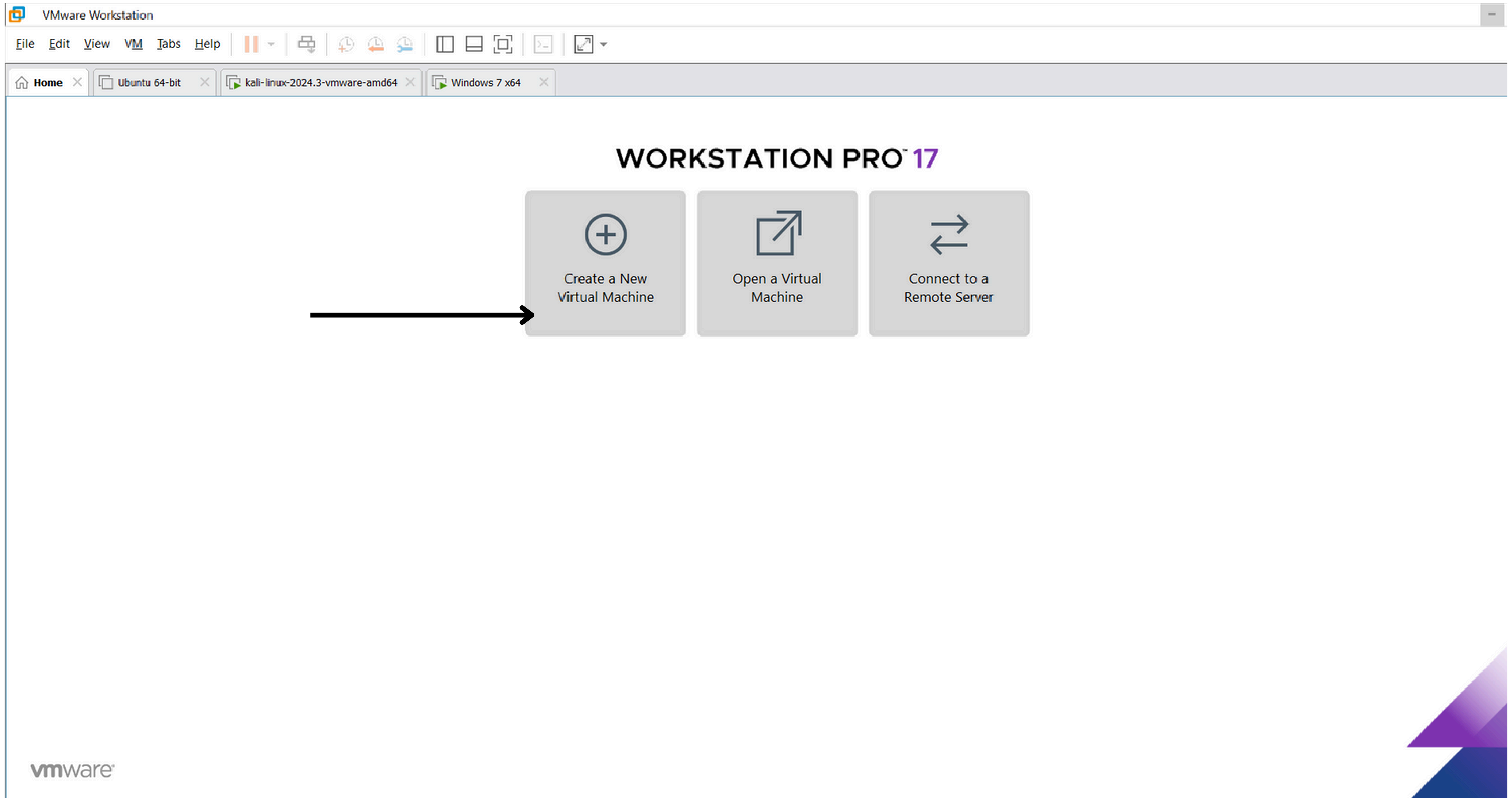


Fusion and Workstation

Run Windows, Linux and other virtual machines with VMware Workstation Pro for Windows and Linux or VMware Fusion for Mac, the industry standard desktop hypervisors.

**https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusiont**

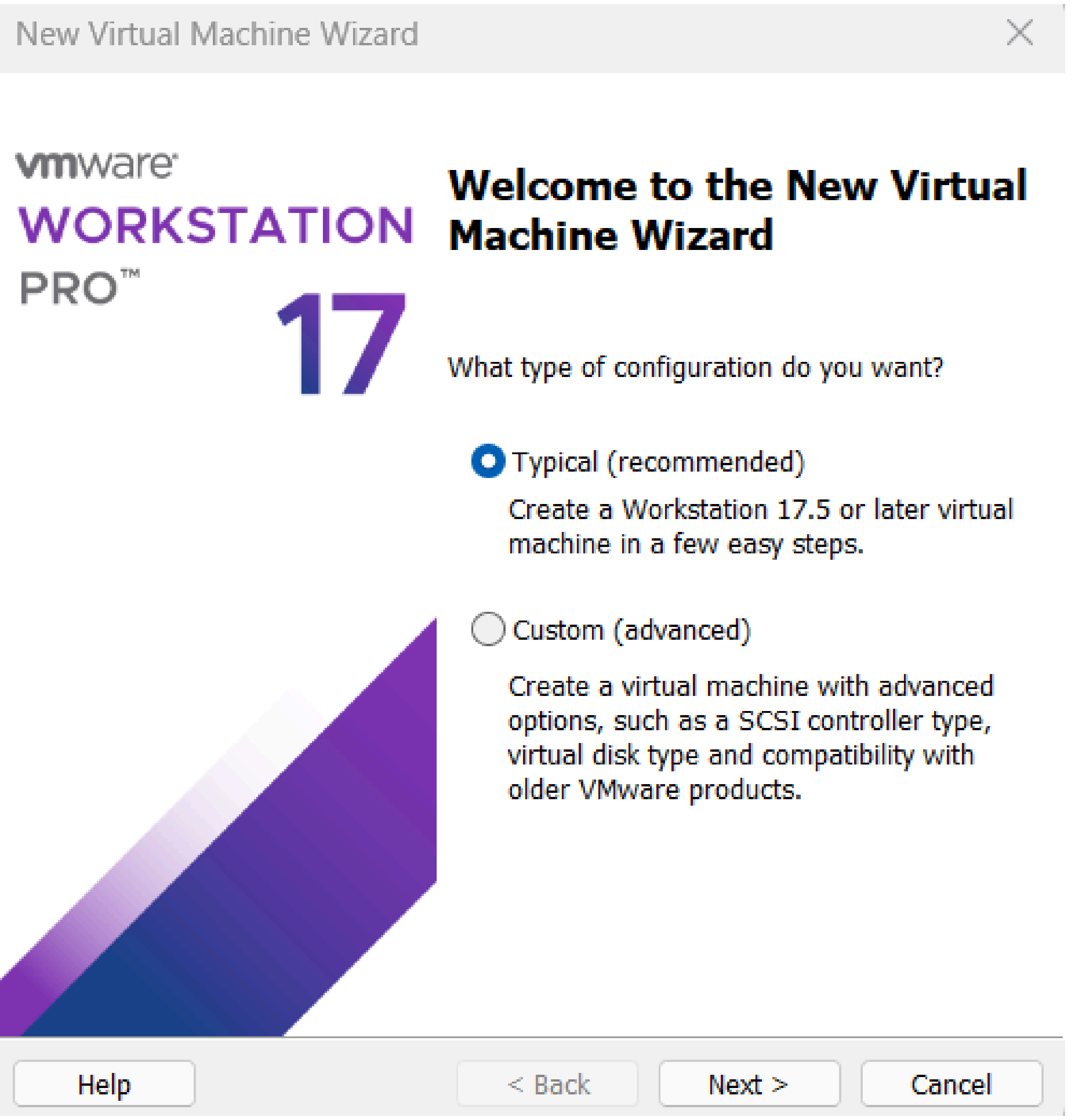
# STEPS TO DOWNLOAD (KALI LINUX )


VMware Workstation
File Edit View VM Tabs Help
Home
Ubuntu 64-bit
kali-linux-2024.3-vmware-amd64
Windows 7 x64
WORKSTATION PRO 17
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server
vmware

# STEPS TO INSTALL

# (KALI LINUX OR WINDOWS 7 ON VMWARE )

1



New Virtual Machine Wizard

**Welcome to the New Virtual Machine Wizard**

What type of configuration do you want?

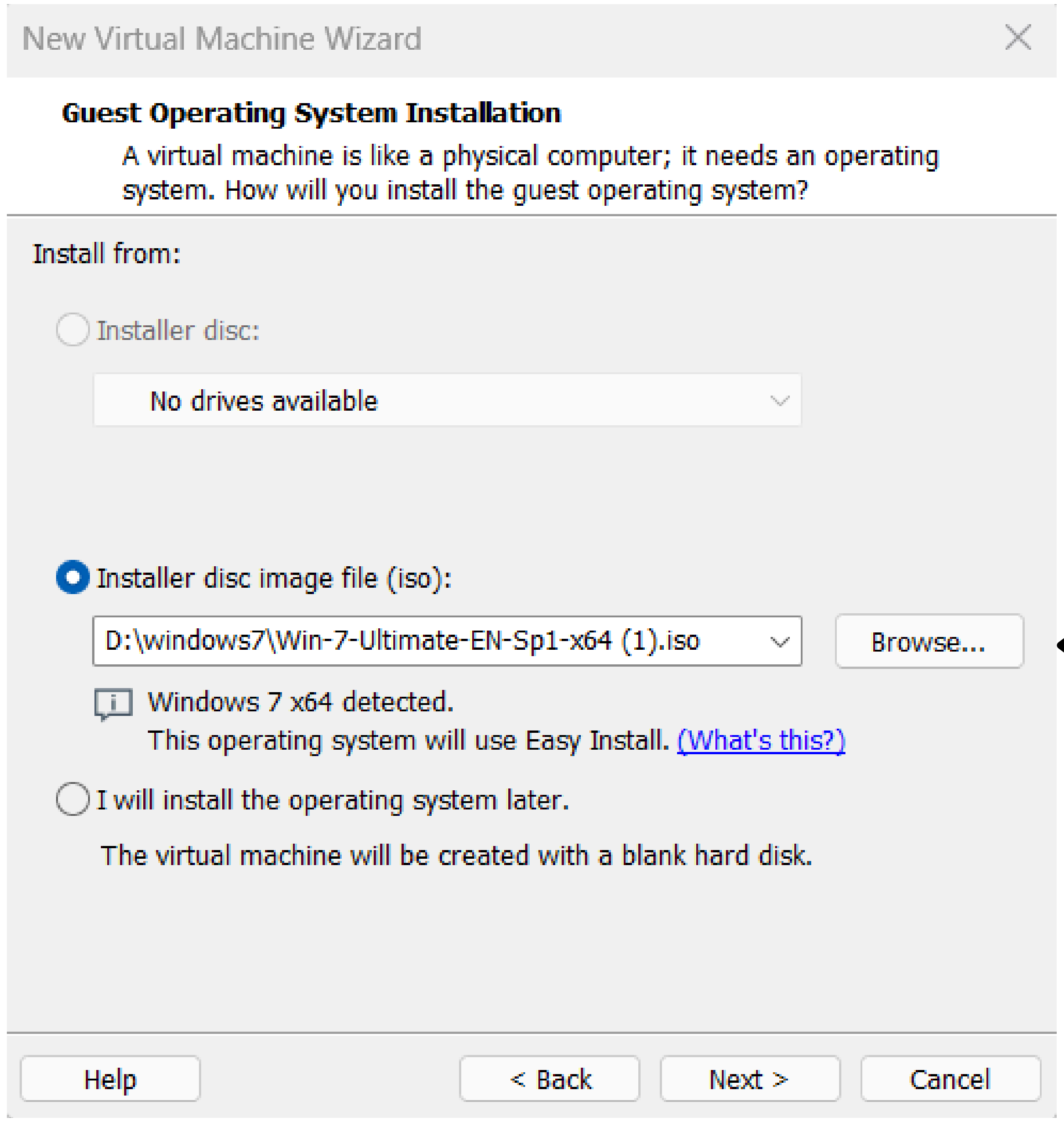
● Typical (recommended)

Create a Workstation 17.5 or later virtual machine in a few easy steps.

○ Custom (advanced)

Create a virtual machine with advanced options, such as a SCSI controller type, virtual disk type and compatibility with older VMware products.

2



New Virtual Machine Wizard

**Guest Operating System Installation**

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

○ Installer disc:

No drives available

● Installer disc image file (iso):

D:\windows7\Win-7-Ultimate-EN-Sp1-x64 (1).iso

Windows 7 x64 detected.
This operating system will use Easy Install. (What's this?)

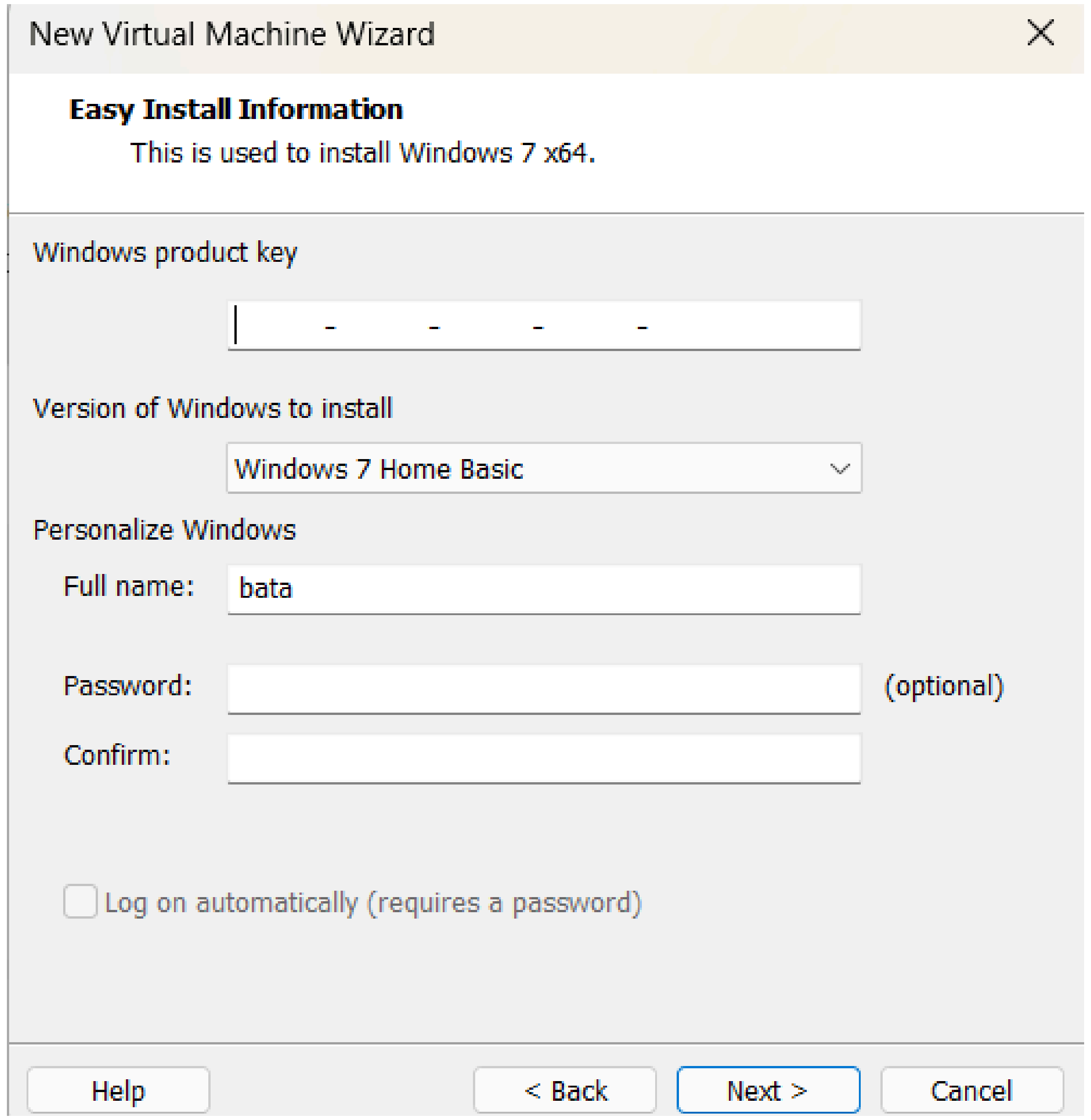
○ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

From this option we can choose the operating system file we want (it must be iso)

# STEPS TO INSTALL
# (KALI LINUX OR WINDOWS 7 ON VMWARE )

3



New Virtual Machine Wizard

**Easy Install Information**

This is used to install Windows 7 x64.

Windows product key

- - - -

Version of Windows to install

Windows 7 Home Basic

Personalize Windows

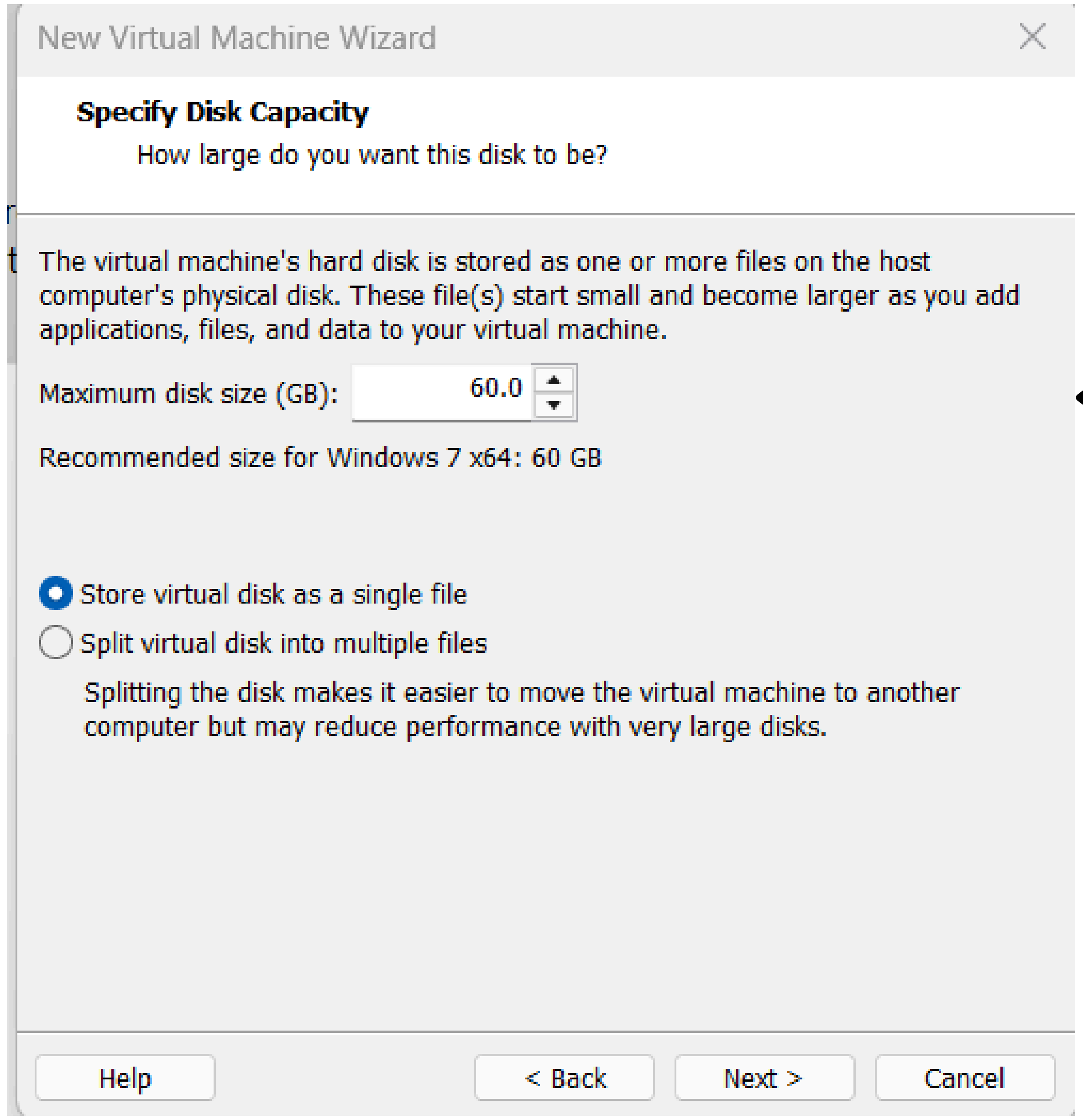
Full name: bata

Password: (optional)

Confirm:

□ Log on automatically (requires a password)

4



New Virtual Machine Wizard

**Specify Disk Capacity**

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB): 60.0

Recommended size for Windows 7 x64: 60 GB

● Store virtual disk as a single file

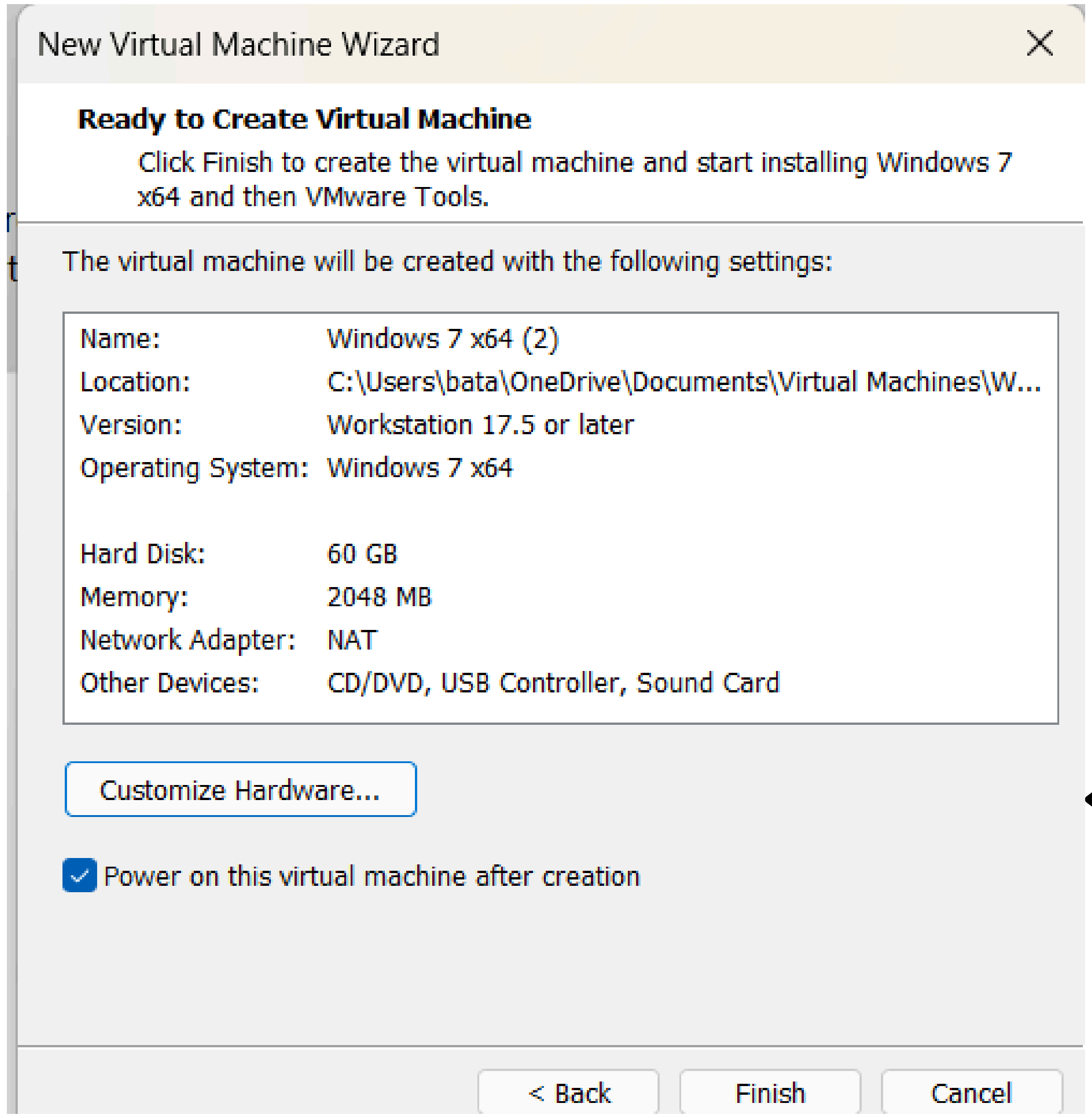
○ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

← Minimum ( 20GB)

# STEPS TO INSTALL
# (KALI LINUX OR WINDOWS 7 ON VMWARE )

5



New Virtual Machine Wizard

**Ready to Create Virtual Machine**

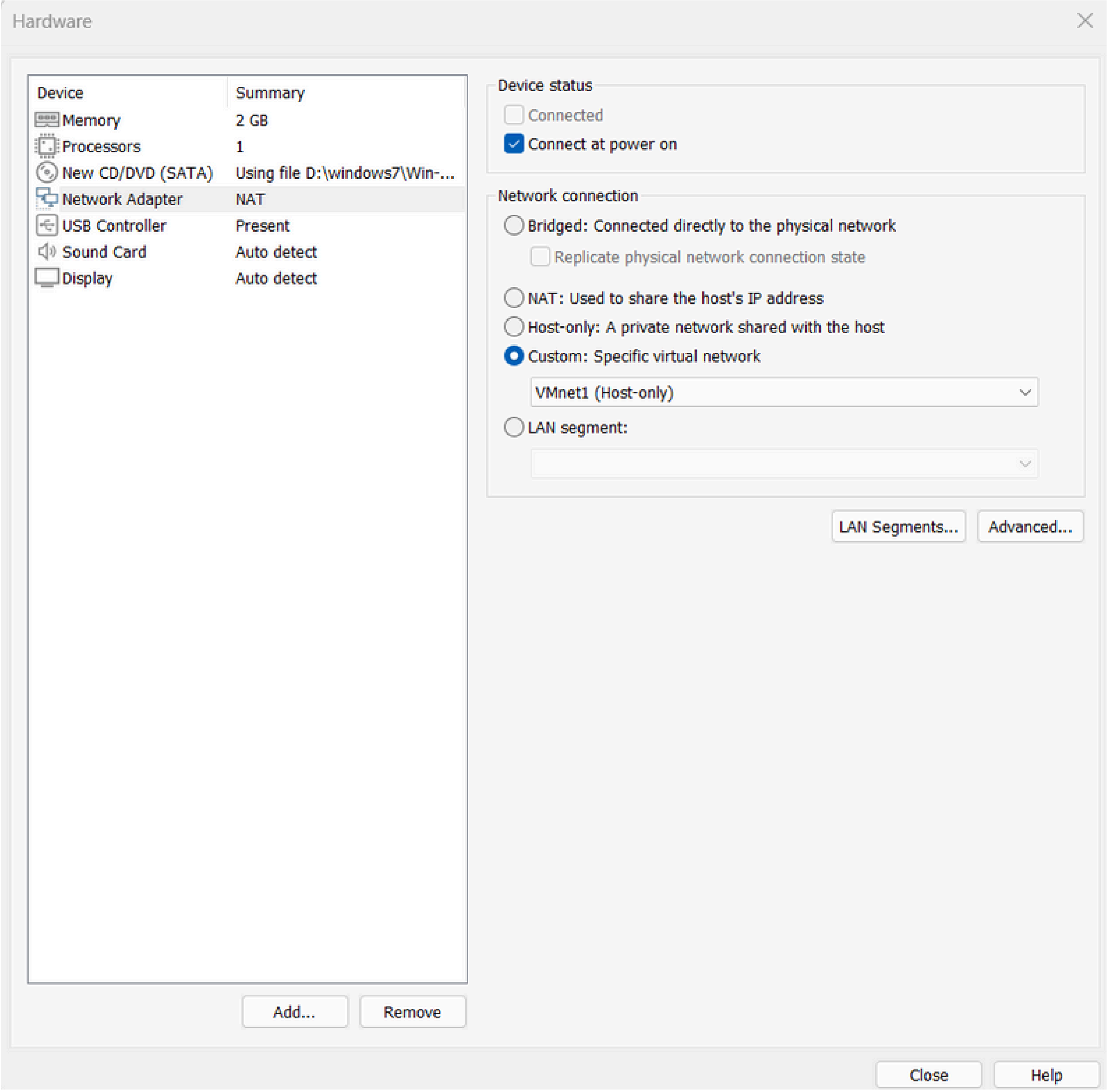
Click Finish to create the virtual machine and start installing Windows 7 x64 and then VMware Tools.

The virtual machine will be created with the following settings:

| | |
|---|---|
| Name: | Windows 7 x64 (2) |
| Location: | C:\Users\bata\OneDrive\Documents\Virtual Machines\W... |
| Version: | Workstation 17.5 or later |
| Operating System: | Windows 7 x64 |
| Hard Disk: | 60 GB |
| Memory: | 2048 MB |
| Network Adapter: | NAT |
| Other Devices: | CD/DVD, USB Controller, Sound Card |

☑ Power on this virtual machine after creation

6



Hardware

| Device | Summary |
|---|---|
| Memory | 2 GB |
| Processors | 1 |
| New CD/DVD (SATA) | Using file D:\windows7\Win-... |
| Network Adapter | NAT |
| USB Controller | Present |
| Sound Card | Auto detect |
| Display | Auto detect |

Device status

☐ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

☐ Replicate physical network connection state

○ NAT: Used to share the host's IP address

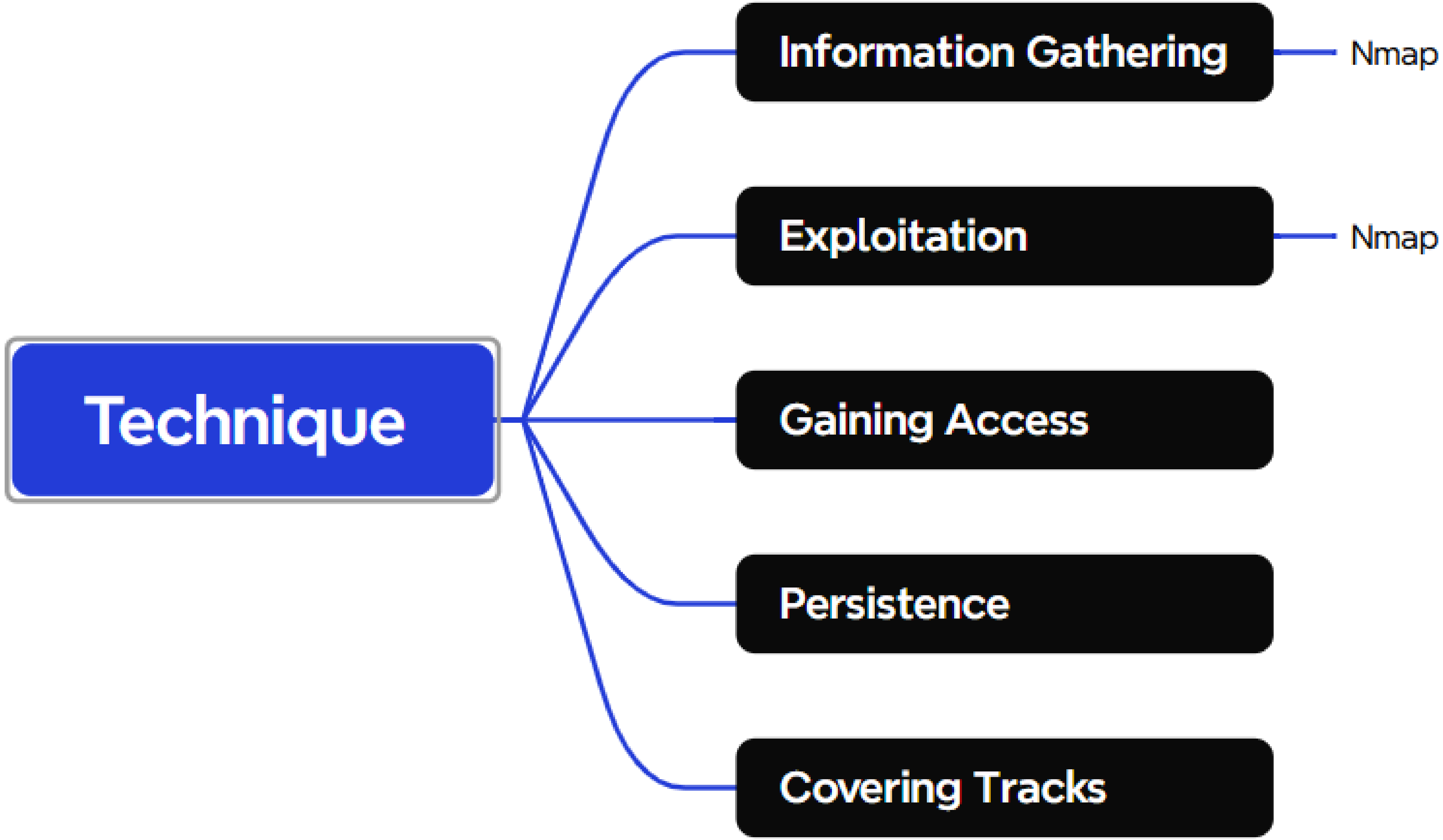
○ Host-only: A private network shared with the host

● Custom: Specific virtual network

VMnet1 (Host-only)

○ LAN segment:

# TECHNIQUE



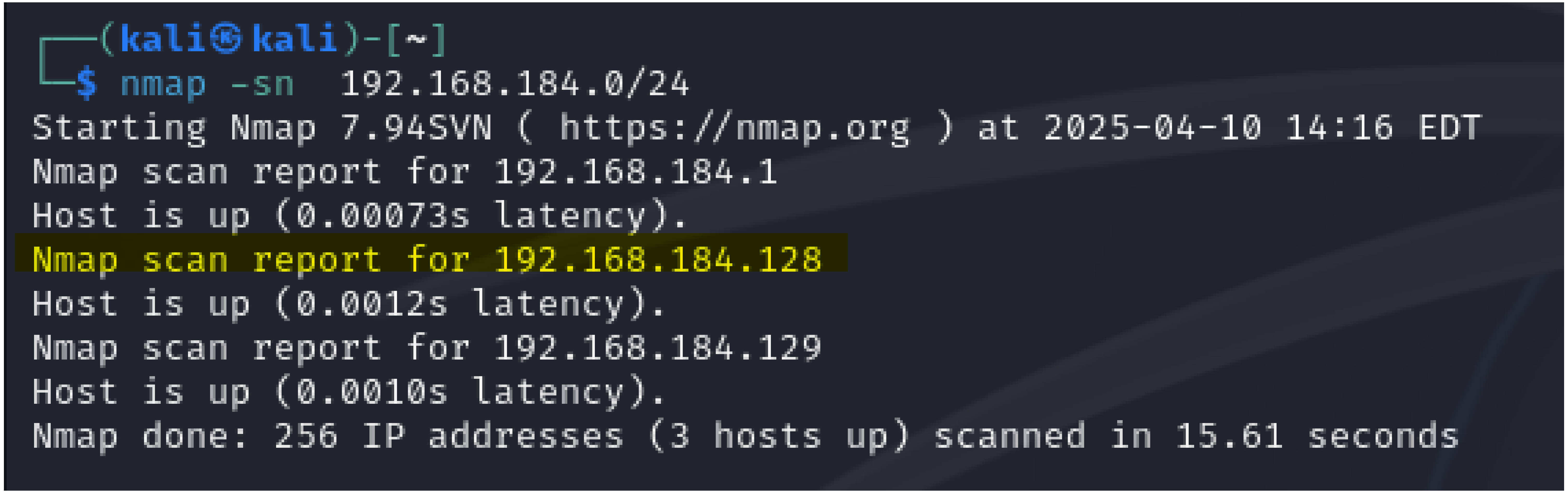
Technique
Information Gathering
Nmap
Exploitation
Nmap
Gaining Access
Persistence
Covering Tracks

# INFORMATION GATHERING

- Is the victim machine running Windows 7?
- Is the SMB port (port 445) open?
- Is the system exploitable?

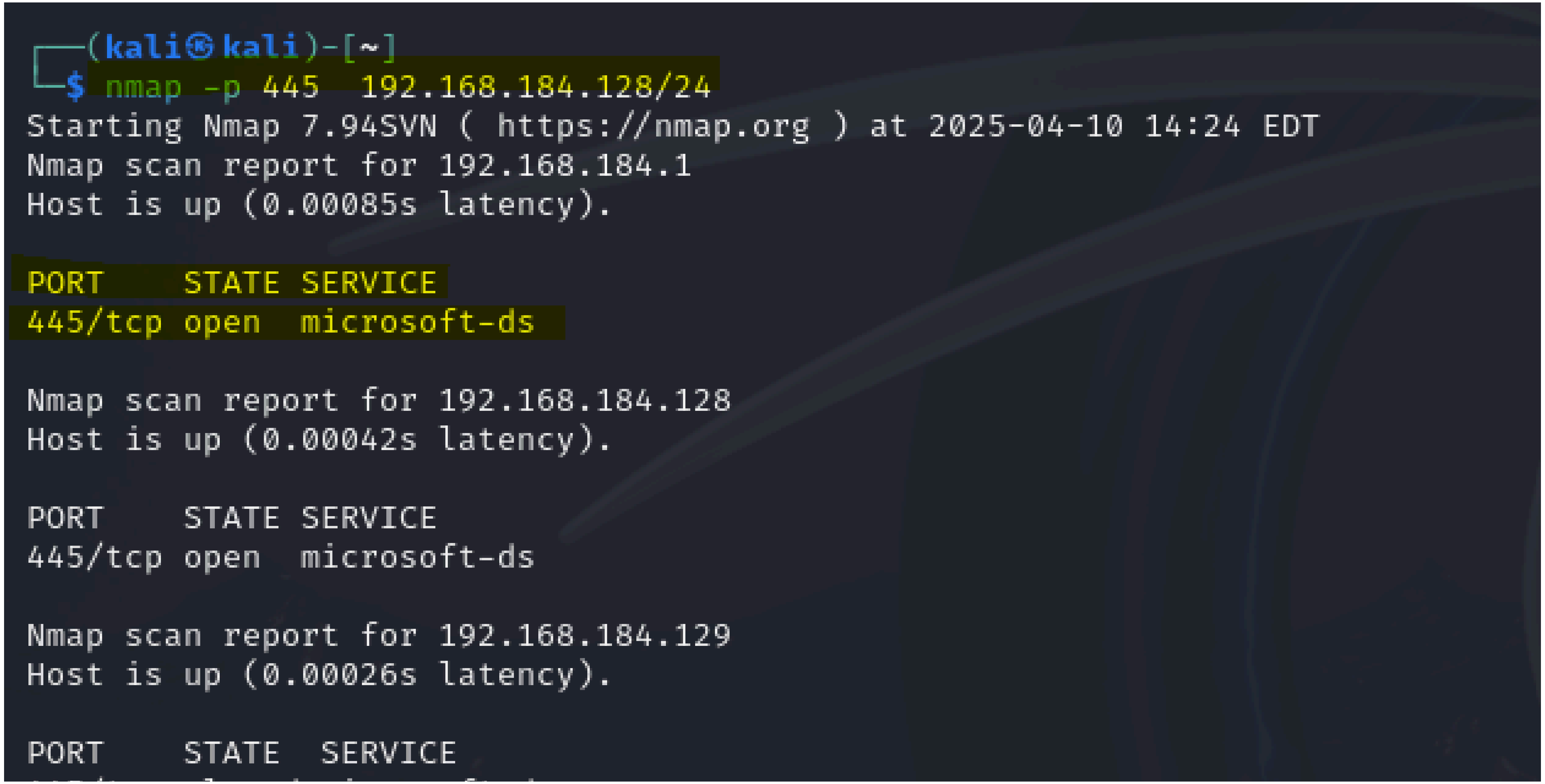
**Nmap**

# INFORMATION GATHERING



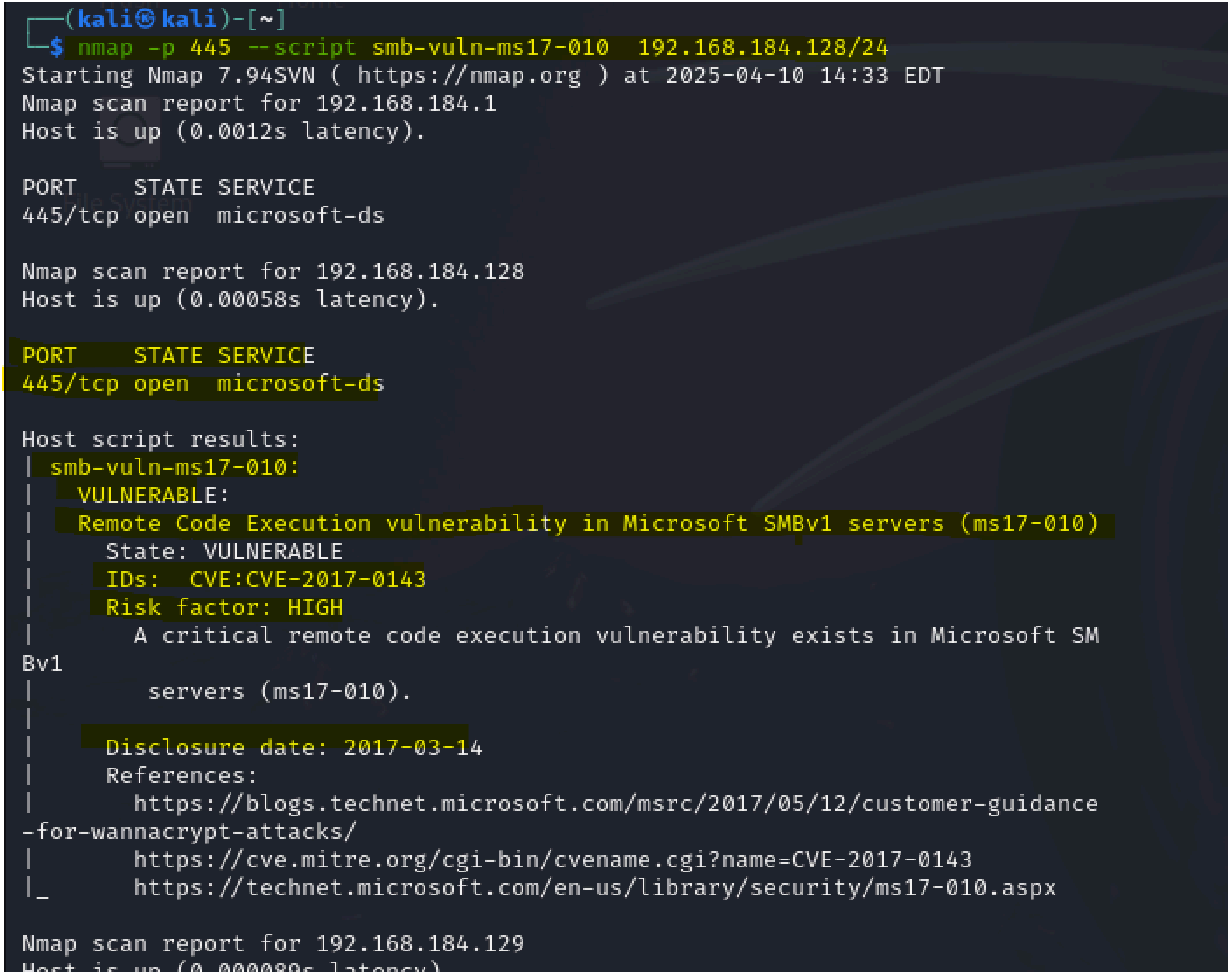
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn  192.168.184.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-10 14:16 EDT
Nmap scan report for 192.168.184.1
Host is up (0.00073s latency).
Nmap scan report for 192.168.184.128
Host is up (0.0012s latency).
Nmap scan report for 192.168.184.129
Host is up (0.0010s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.61 seconds
```

# INFORMATION GATHERING



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445  192.168.184.128/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-10 14:24 EDT
Nmap scan report for 192.168.184.1
Host is up (0.00085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap scan report for 192.168.184.128
Host is up (0.00042s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap scan report for 192.168.184.129
Host is up (0.00026s latency).

PORT    STATE  SERVICE
```

# INFORMATION GATHERING



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 445 --script smb-vuln-ms17-010  192.168.184.128/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-10 14:33 EDT
Nmap scan report for 192.168.184.1
Host is up (0.0012s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap scan report for 192.168.184.128
Host is up (0.00058s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap scan report for 192.168.184.129
Host is up (0.000089s latency).
```

# THANK YOU