

Setting the Trap



Michael Woolard

Risk and Compliance Manager

@wooly6bear | <https://wooly6bear.wordpress.com>

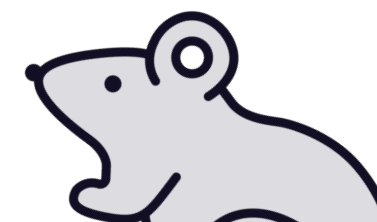
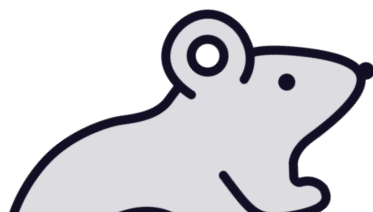
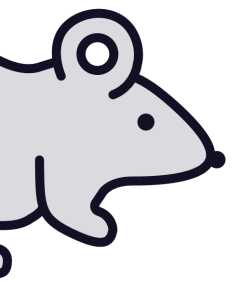
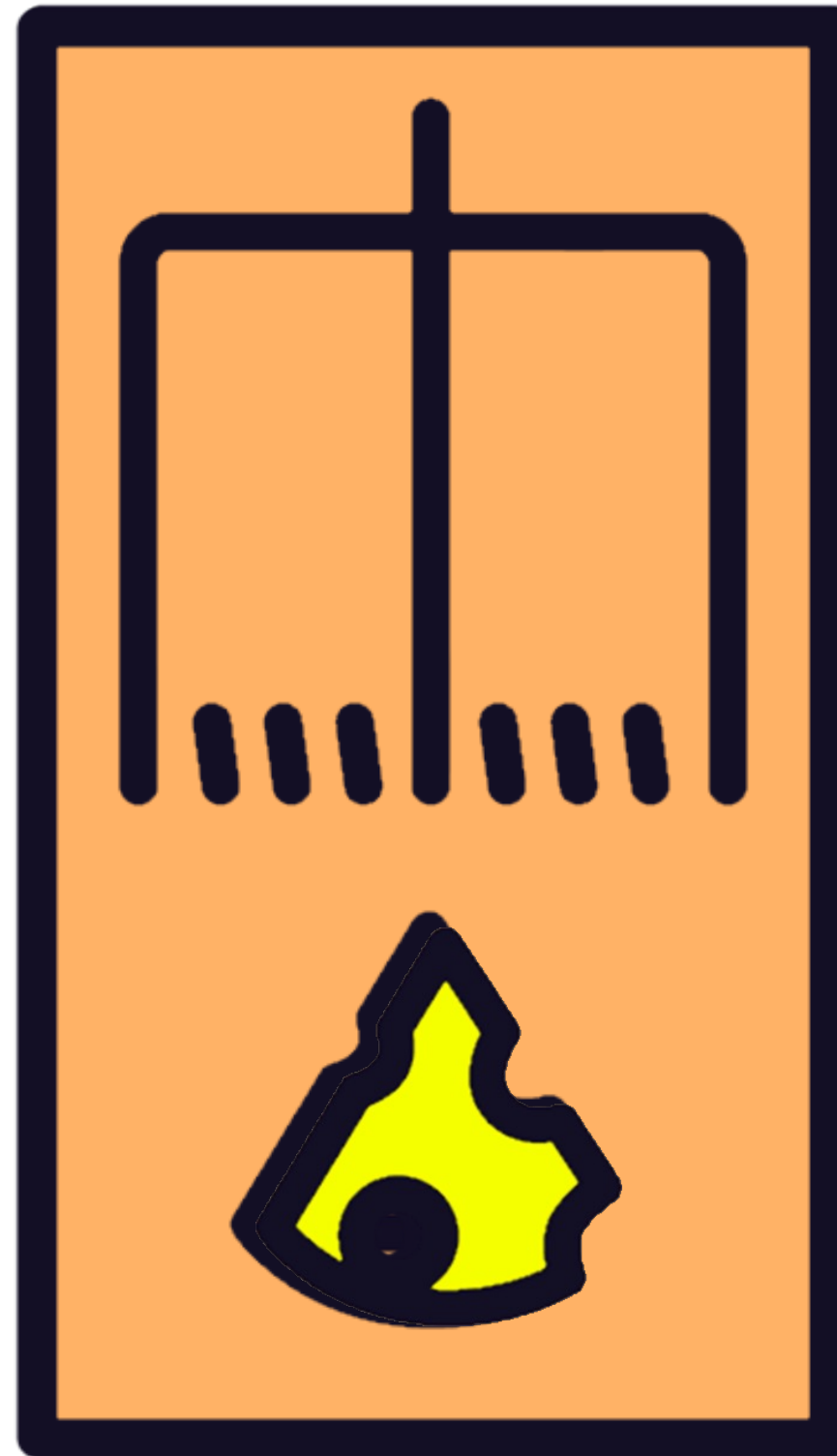




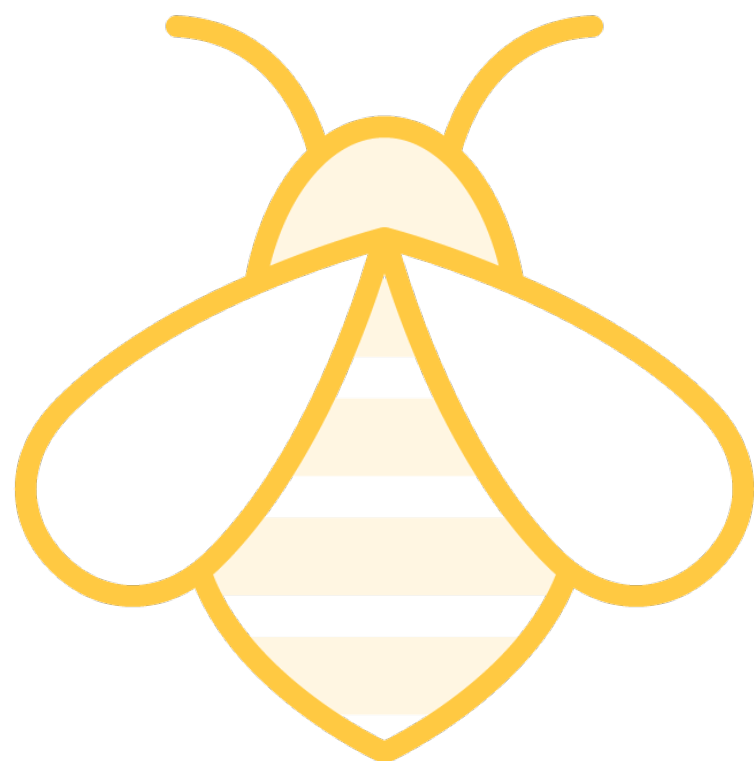
What Kind of Traps Can Be Set



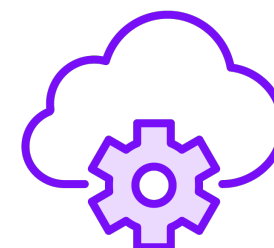
Honeypot



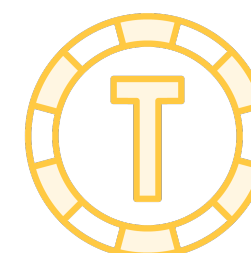
Create a Honeypot



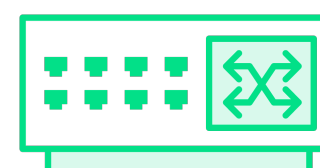
Files



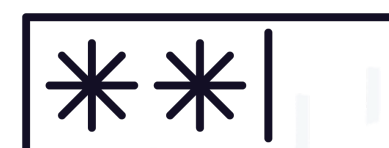
Services



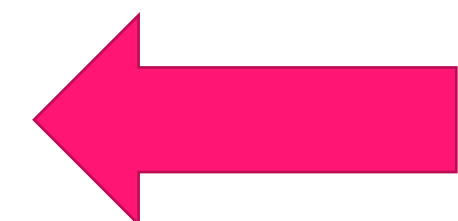
Tokens



Ports



**Credentia
s**





Honeypot: Create a Honeypot



Honeyport



<https://github.com/gfoss/PowerShell-Honeyport/blob/master/honeyport.ps1>



honeyportCIM.ps1 in course exercise files



PowerShell 7



HoneyPortCIM.ps1



HoneyPortCIM. ps1

Notes

Log Aggregator / SIEM / EDR

- 1003
- 1002

Noisy





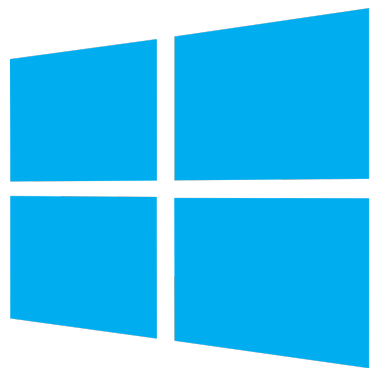
Honeypot: Create a Honeytoken



Honeytoken



<https://github.com/Blumira/Kerberoast-Detection>



Domain Controller



Powershell 7



Local Group Policy Editor

File Action View Help



Local Computer Policy

Computer Configuration

Software Settings

Windows Settings

Name Resolution Policy

Scripts (Startup/Shutdown)

Deployed Printers

Security Settings

Account Policies

Local Policies

Windows Defender Firewall

Network List Manager Policies

Public Key Policies

Software Restriction Policies

Application Control Policies

IP Security Policies on Local Computer

Advanced Audit Policy Configuration

System Audit Policies

Account Logon

Account Management

Detailed Tracking

DS Access

Logon/Logoff

Object Access

Policy Change

Privilege Use

System

Subcategory

Audit Credential Validation

Audit Kerberos Authentication Service

Audit Kerberos Service Ticket Operations

Audit Other Account Logon Events

Audit Events

Not Configured

Not Configured

Not Configured

Not Configured

Create Service Account Honeypot

Step 1 – Create a non-admin user account (example: backupexec)

Step 2 – Add a SPN to the account (see below)

Step 3 – Confirm the SPN was created > **setspn -Q */* | findstr backupsvc**

```
C:\Users\Administrator>setspn -a backupsvc/Win2019Server backupexec
Checking domain DC=PLURALSIGHT,DC=local

Registering ServicePrincipalNames for CN=backup svc,CN=Users,DC=PLURALSIGHT,DC=local
        backupsvc/Win2019Server
Updated object
```



Dogemira.ps1

- *Event ID: 4769*
- *Encryption type: 0x17*
- *Ticket options: 0x40810000*
- *SPN Name: <Name of your honeycred / SPN name>*





Monitor for Bad Credentials



Invoke-Fail2Ban



<https://github.com/wiredpulse/Invoke-Fail2Ban>



Invoke-Fail2Ban.ps1 in course exercise files



<https://cyberfibers.com/2019/08/invoke-fail2ban/>



Invoke-Fail2Ban

Honey Cred Admin Properties

Member Of Dial-in Environment Sessions
Remote control Remote Desktop Services Profile COM+
General Address Account Profile Telephones Organization

User logon name:
 @PLURALSIGHT.local

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never
☐ End of:



Invoke-Fail2Ban.ps1



Maintain the Look of an Active User



Hack the Hacker



When Was the Account Created?

When Did the Account Last Logon?

When Was the Password Last Changed?

Correlation to Another Non-Admin Account?



Hack the Hacker

```
$RegPath = "HKLM:\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon"
```

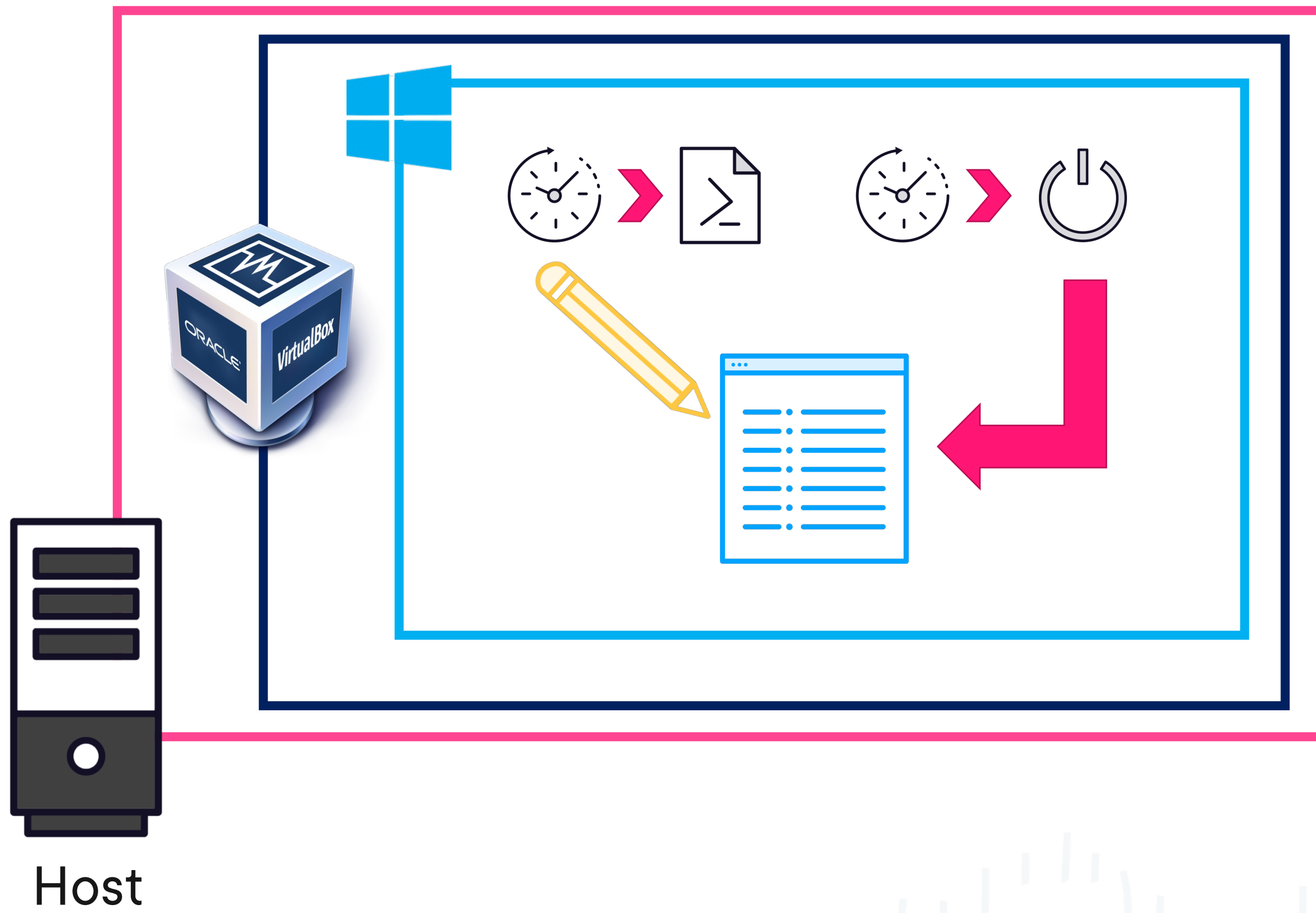
```
$DefaultUsername = "honeycredusername"
```

```
$DefaultPassword = "honeycredpassword"
```

```
Set-ItemProperty $RegPath "AutoAdminLogon" -value "1" -type String
```

```
Set-ItemProperty $RegPath "DefaultUsername" -value  
"$DefaultUsername" -type String
```





Start up and Shut down Virtualbox VM

C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" list vms

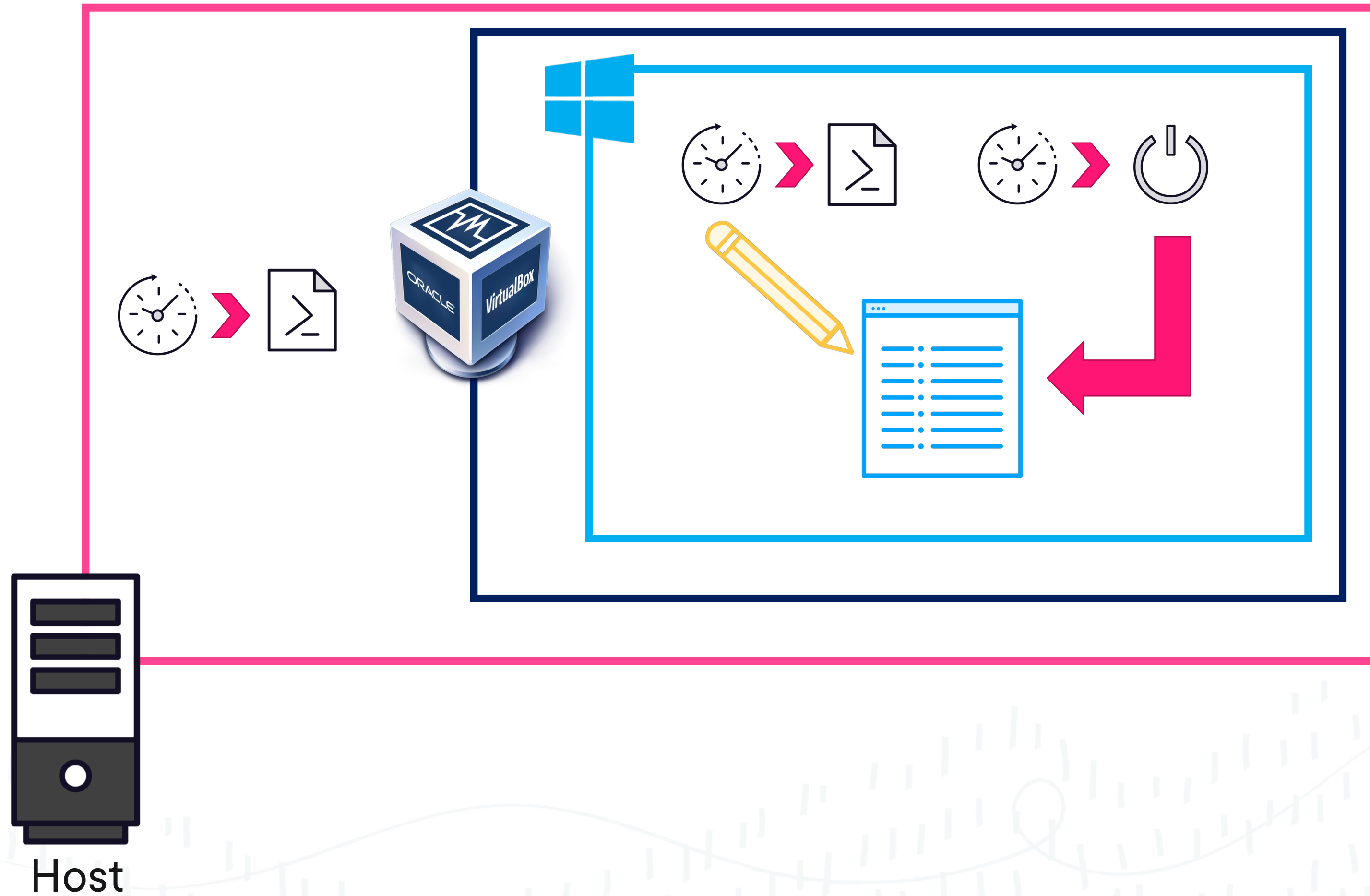
<https://www.virtualbox.org/manual/ch08.html#vboxmanage-startvm>

"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" startvm (name of vm)

<https://www.virtualbox.org/manual/ch08.html#vboxmanage-controlvm>

"C:\Program Files\Oracle\VirtualBox\VBoxManage.exe" controlvm (name of vm)
shutdown





Hack the Hacker

```
# Specify here the username whose password to reset.
```

```
$username = '(user account)'
```

```
# Import the System.Web .NET assembly
```

```
Add-Type -AssemblyName 'System.Web'
```

```
# Generate a random password that is 12-characters long with five non-AlphaNumeric characters.
```

```
$randomPassword = [System.Web.Security.Membership]::GeneratePassword(12, 5)
```

```
# Convert the plain text password to a secure string.
```

```
$newPassword = $randomPassword | ConvertTo-SecureString -AsPlainText -Force
```

```
# Reset the user password
```

```
Set-ADAccountPassword -Identity $username -NewPassword $newPassword -Reset
```

```
# Display the new password
```

```
$randomPassword
```





Review Attack Patterns



TT&CK Matrix for Enterprise

show sub-techniques

show sub-techniques

show sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques
Active Scanning (3)	Acquire Infrastructure (7) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)		Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery		Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limit
Gather Victim Identity Information (3)		External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery		Audio Capture	Exfiltration Over Alternative Protocols	
Gather Victim Network Information (6)		Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery		Automated Collection	Exfiltration Over Cloud Channels	
Gather Victim Org Information (4)		Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard		Browser Session Hijacking	Exfiltration Over Network Medium	
Phishing for Information (3)		Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery		Clipboard Data		
Search Closed Sources (2)		Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery		Data from Cloud Storage		
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Domain Policy Modification (2)	Modify Authentication Process (7)	Container and Resource Discovery		Data from Configuration Repository (2)		
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Interception	Debugger Evasion		Data from Information Repositories (3)		
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System		
		System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Hide Artifacts (10)	Network Sniffing	File and Directory Discovery	Data from Network Shared Drive				
		User Execution (3)	Windows Management Instrumentation	Scheduled Task/Job (5)	Hijack Execution Flow (12)	Indicator Removal (9)	Group Policy Discovery	Data from Removable Media				
				Implant Internal Image	Process Injection (12)	Indirect Command Execution	Network Service Discovery	Email Collection (3)				
				Modify Authentication Process (7)	Scheduled Task/Job (5)	Masquerading (7)	Network Share Discovery	Input Capture (4)				
				Office Application Startup (6)	Valid Accounts (4)	Modify Authentication Process (7)	Network Sniffing	Screen Capture				
				Pre-OS Boot (5)		Modify Cloud Compute Infrastructure (4)	Permission Groups Discovery (3)	Video Capture				
				Scheduled			Process Discovery					

- Phishing reports
- AV alerts
- EDR alerts
- WAF logs
- IAM & MFA
- Server resources
- Production Incidents
- Security Incidents

Port Scanning



Brute Force



Kerberoasting



Auditing

