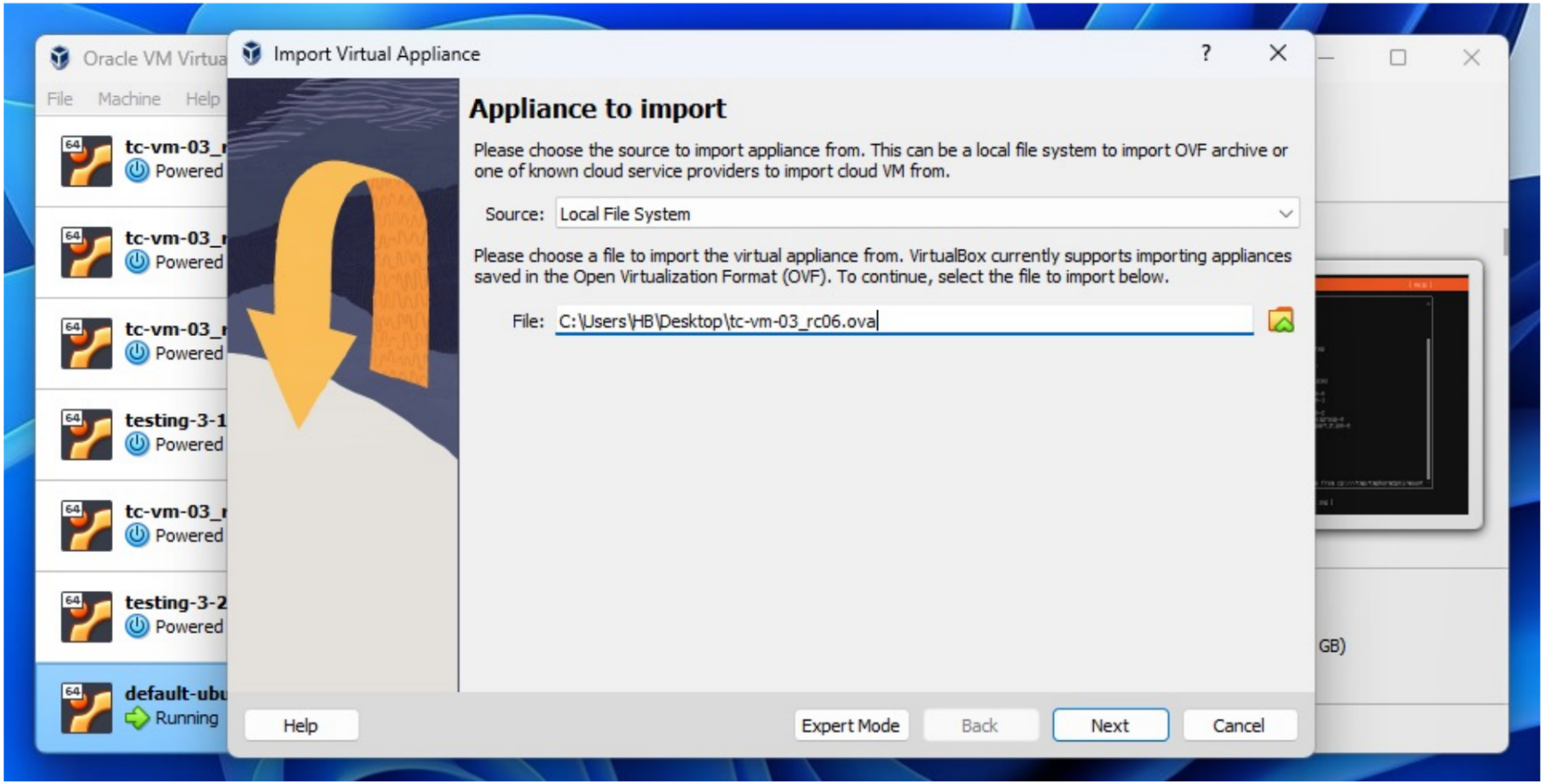
Threats and Countermeasures

Lecture 09:
Defense Evasion

COMP-5830/-6830
Spring 2025

Today: tc-vm-06_rc08

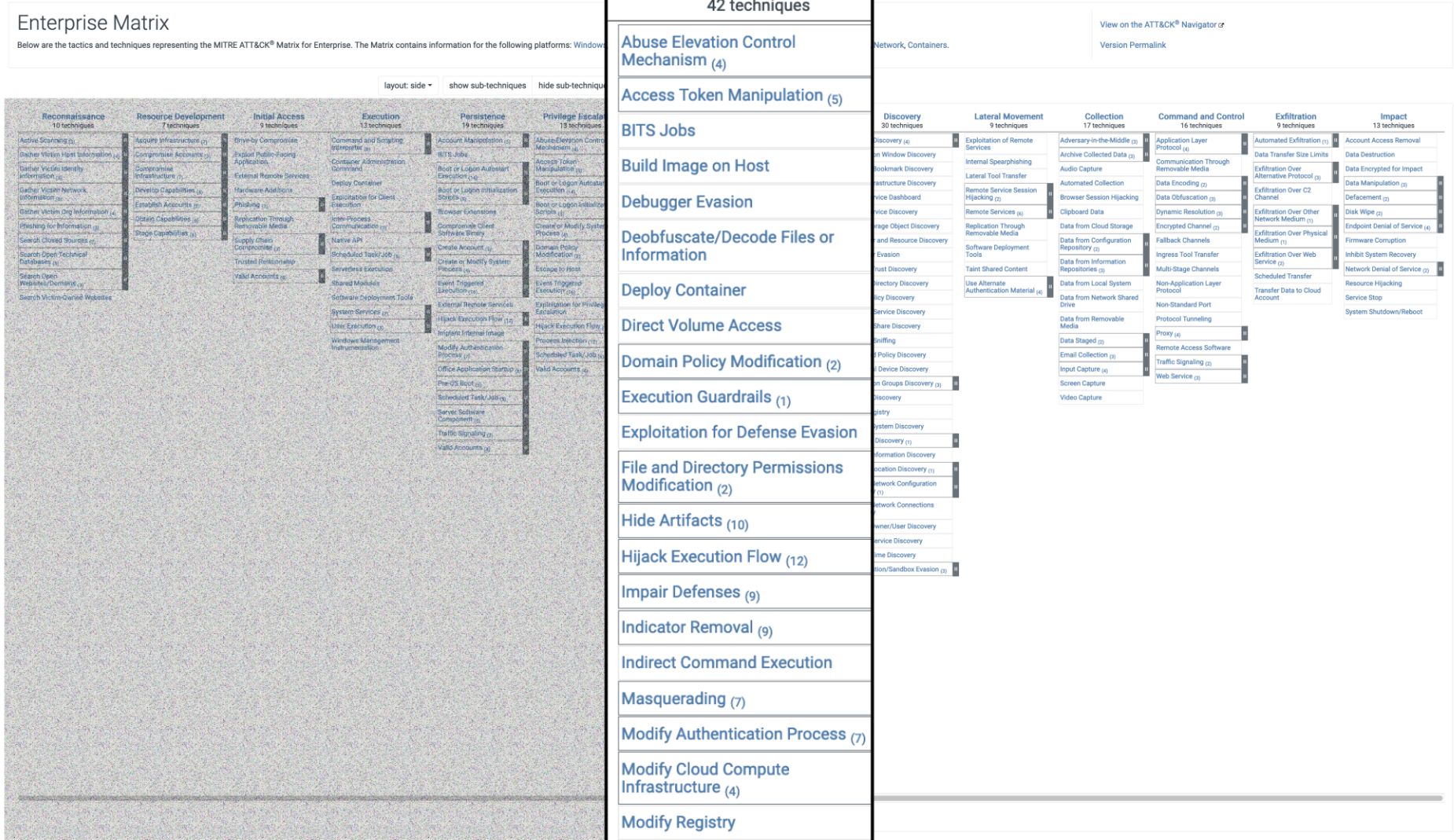


Disk Crypto: AUfw4FfWsJv4SYz52rYdvjoQ

MIDTERM

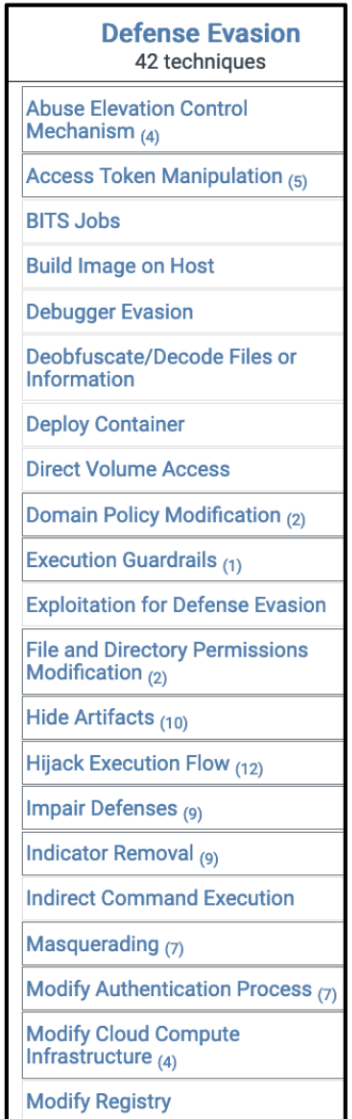
- Grading in-progress, target is Friday
  - Scan and upload as Canvas comment
- Common Point Deductions (current):
  - Poor coverage of target network
  - Faulty interpretation of data and risk
  - Incorrect assertions of facts to the customer

MITRE ATT&CK


Enterprise Matrix
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, Network, Containers.
View on the ATT&CK® Navigator
Version Permalink
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance 10 techniques
Resource Development 7 techniques
Initial Access 9 techniques
Execution 13 techniques
Persistence 19 techniques
Privilege Escalation 13 techniques
Discovery 30 techniques
Lateral Movement 9 techniques
Collection 17 techniques
Command and Control 16 techniques
Exfiltration 9 techniques
Impact 13 techniques
Defense Evasion
42 techniques
Abuse Elevation Control Mechanism (4)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (10)
Hijack Execution Flow (12)
Impair Defenses (9)
Indicator Removal (9)
Indirect Command Execution
Masquerading (7)
Modify Authentication Process (7)
Modify Cloud Compute Infrastructure (4)
Modify Registry

Defense Evasion (MITRE)

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.



Defense Evasion (simplified)

- **GOAL:** Avoid detection during compromise
- EX:
  - Reconfigure ENV
  - Deactivate host-based defenses
  - Suppress own artifacts (data/code/etc)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (4)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (2)
- Execution Guardrails (1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (2)
- Hide Artifacts (10)
- Hijack Execution Flow (12)
- Impair Defenses (9)
- Indicator Removal (9)
- Indirect Command Execution
- Masquerading (7)
- Modify Authentication Process (7)
- Modify Cloud Compute Infrastructure (4)
- Modify Registry

Commonly Deployed Host-Based Defenses

- Anti-Virus

Commonly Deployed Host-Based Defenses

- Anti-Virus
  - Heuristic- and Signature-based detection of unwanted apps/code/malware
  - Automated OS interference to remove and/or quarantine

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS
  - Monitor network traffic for specific heuristics
  - Automated network interference to block interaction

README License

v1.1.0.dev1 20??/??/??

Fail2Ban: ban hosts that cause multiple authentication errors

Fail2Ban scans log files like `/var/log/auth.log` and bans IP addresses conducting too many failed login attempts. It does this by updating system firewall rules to reject new connections from those IP addresses, for a configurable amount of time. Fail2Ban comes out-of-the-box ready to read many standard log files, such as those for sshd and Apache, and is easily configured to read any log file of your choosing, for any error you wish.

Though Fail2Ban is able to reduce the rate of incorrect authentication attempts, it cannot eliminate the risk presented by weak authentication. Set up services to use only two factor, or public/private authentication mechanisms if you really want to protect services.

Since v0.10 fail2ban supports the matching of IPv6 addresses.

This README is a quick introduction to Fail2Ban. More documentation, FAQ, and HOWTOs to be found on fail2ban(1) manpage, Wiki, Developers documentation and the website: https://www.fail2ban.org

Installation:

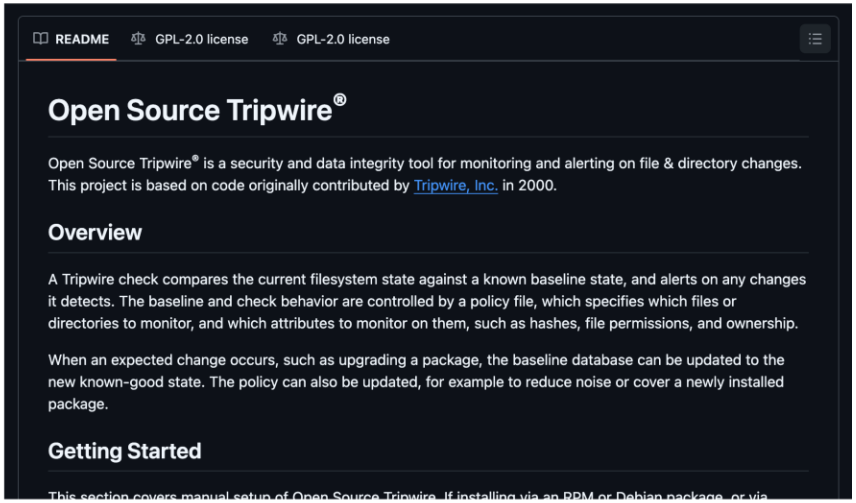
Fail2Ban is likely already packaged for your Linux distribution and can be installed with a simple command

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS
- Filesystem Watchdog

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS
- Filesystem Watchdog
  - Monitors specific filesystem locations for state-changes
  - Automated alerts on contents/metadata changes


README GPL-2.0 license GPL-2.0 license

Open Source Tripwire®

Open Source Tripwire® is a security and data integrity tool for monitoring and alerting on file & directory changes. This project is based on code originally contributed by Tripwire, Inc. in 2000.

Overview

A Tripwire check compares the current filesystem state against a known baseline state, and alerts on any changes it detects. The baseline and check behavior are controlled by a policy file, which specifies which files or directories to monitor, and which attributes to monitor on them, such as hashes, file permissions, and ownership.

When an expected change occurs, such as upgrading a package, the baseline database can be updated to the new known-good state. The policy can also be updated, for example to reduce noise or cover a newly installed package.

Getting Started

This section covers manual setup of Open Source Tripwire. If installing via an RPM or Debian package, or via

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS
- Filesystem Watchdog
- Aggregate logs/alerts

Commonly Deployed Host-Based Defenses

- Anti-Virus
- Network IPS
- Filesystem Watchdog
- Aggregate logs/alerts
  - Stream logs/alerts/etc. to remove location for **independent** storage
  - Allows trend-detection

So…How Do We Fix Our Problems?

Bypass: Deactivate Defenses

MITRE ATT&CK

Privilege Escalation
13 techniques

Defense Evasion
42 techniques

mation for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers

layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	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	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	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	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	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	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Escape to Host	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Event Triggered Execution (16)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	Hijack Execution Flow (12)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (9)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal (9)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
				Scheduled Task/Job (5)		Indirect Command Execution	Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Web Service (3)		
				Server Software Component (5)		Masquerading (7)	Unsecured Credentials (7)	Peripheral Device Discovery		Video Capture			
				Traffic Signaling (2)		Modify Authentication Process (7)		Permission Groups Discovery (3)					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (2)		Remote System Discovery					
						Network Boundary Bridging (1)		Software Discovery (1)					
						Obfuscated Files or Information (9)		System Information Discovery					
						Plist File Modification		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (1)					
						Process Injection (12)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls (6)		Virtualization/Sandbox Evasion (3)					
						System Binary Proxy Execution (13)							
						System Script Proxy Execution (1)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Last modified: 01 April 2022

MITRE ATT&CK

Privilege Escalation
13 techniques

AFTER

Defense Evasion
42 techniques

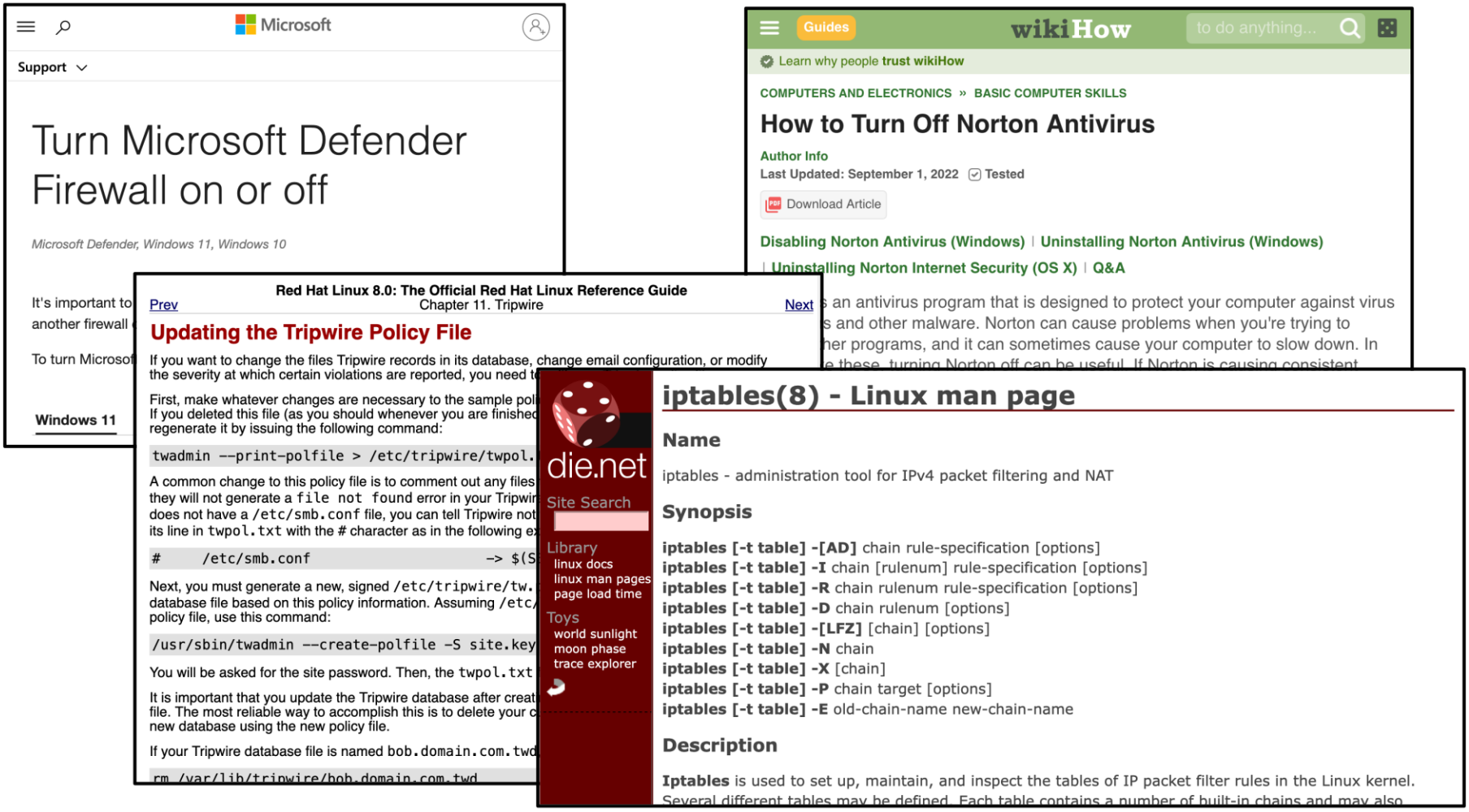
mation for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers

layout: side | show sub-techniques | hide sub-techniques | help

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (7)	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	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (7)	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	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	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	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (3)		Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Escape to Host	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (12)	Process Injection (12)	Event Triggered Execution (16)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (3)	Implant Internal Image	Scheduled Task/Job (5)	Exploitation for Privilege Escalation	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (7)	Valid Accounts (4)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hide Artifacts (10)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (4)	Network Sniffing		Input Capture (4)	Traffic Signaling (2)		
				Scheduled Task/Job (5)		Impair Defenses (9)	Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Web Service (3)		
				Server Software Component (5)		Indicator Removal (9)	Unsecured Credentials (7)	Peripheral Device Discovery		Video Capture			
				Traffic Signaling (2)		Indirect Command Execution		Permission Groups Discovery (3)					
				Valid Accounts (4)		Masquerading (7)		Process Discovery					
						Modify Authentication Process (7)		Query Registry					
						Modify Cloud Compute Infrastructure (4)		Remote System Discovery					
						Modify Registry		Software Discovery (1)					
						Modify System Image (2)		System Information Discovery					
						Network Boundary Bridging (1)		System Location Discovery (1)					
						Obfuscated Files or Information (9)		System Network Configuration Discovery (1)					
						Plist File Modification		System Network Connections Discovery					
						Pre-OS Boot (5)		System Owner/User Discovery					
						Process Injection (12)		System Service Discovery					
						Reflective Code Loading		System Time Discovery					
						Rogue Domain Controller		Virtualization/Sandbox Evasion (3)					
						Rootkit							
						Subvert Trust Controls (6)							
						System Binary Proxy Execution (13)							
						System Script Proxy Execution (1)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (4)							
						Valid Accounts (4)							
						Virtualization/Sandbox Evasion (3)							
						Weaken Encryption (2)							
						XSL Script Processing							

Last modified: 01 April 2022

Bypass: Deactivate Defenses



Microsoft

Support

Turn Microsoft Defender Firewall on or off

Microsoft Defender, Windows 11, Windows 10

It's important to
another firewall

To turn Microsof

Windows 11

Red Hat Linux 8.0: The Official Red Hat Linux Reference Guide

Prev Chapter 11. Tripwire Next

Updating the Tripwire Policy File

If you want to change the files Tripwire records in its database, change email configuration, or modify the severity at which certain violations are reported, you need t

First, make whatever changes are necessary to the sample pol
If you deleted this file (as you should whenever you are finishe
regenerate it by issuing the following command:

```
twadmin --print-polfile > /etc/tripwire/twpol.
```

A common change to this policy file is to comment out any files
they will not generate a `file not found` error in your Tripwir
does not have a `/etc/smb.conf` file, you can tell Tripwire not
its line in `twpol.txt` with the # character as in the following e

```
#     /etc/smb.conf                    -> $(S
```

Next, you must generate a new, signed `/etc/tripwire/tw.`
database file based on this policy information. Assuming `/etc/`
policy file, use this command:

```
/usr/sbin/twadmin --create-polfile -S site.key
```

You will be asked for the site password. Then, the `twpol.txt`

It is important that you update the Tripwire database after creat
file. The most reliable way to accomplish this is to delete your c
new database using the new policy file.

If your Tripwire database file is named `bob.domain.com.twd`

```
rm /var/lib/tripwire/bob.domain.com.twd
```

Guides wikiHow to do anything...

Learn why people trust wikiHow

COMPUTERS AND ELECTRONICS » BASIC COMPUTER SKILLS

How to Turn Off Norton Antivirus

Author Info
Last Updated: September 1, 2022 Tested

Download Article

Disabling Norton Antivirus (Windows) | Uninstalling Norton Antivirus (Windows)
| Uninstalling Norton Internet Security (OS X) | Q&A

s an antivirus program that is designed to protect your computer against virus
s and other malware. Norton can cause problems when you're trying to
her programs, and it can sometimes cause your computer to slow down. In
e these, turning Norton off can be useful. If Norton is causing consistent

die.net

Site Search

Library
linux docs
linux man pages
page load time

Toys
world sunlight
moon phase
trace explorer

iptables(8) - Linux man page

Name

iptables - administration tool for IPv4 packet filtering and NAT

Synopsis

iptables [-t table] -[AD] chain rule-specification [options]
iptables [-t table] -I chain [rulenum] rule-specification [options]
iptables [-t table] -R chain rulenum rule-specification [options]
iptables [-t table] -D chain rulenum [options]
iptables [-t table] -[LFZ] [chain] [options]
iptables [-t table] -N chain
iptables [-t table] -X [chain]
iptables [-t table] -P chain target [options]
iptables [-t table] -E old-chain-name new-chain-name

Description

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also

- Most defenses are **best effort** via either *signature* or *heuristic* checks
  - Signature: specific indicator
  - Heuristic: collection of non-indicators constituting a likely indicator

Bypass: Encrypt/Obfuscate

- Most defenses are **best effort** via either *signature* or *heuristic* checks
  - Signature: specific indicator
  - Heuristic: collection of non-indicators constituting a likely indicator

```
openssl aes-256-cbc
     -d -salt
     -k f361cf6aa41474db459c55b99c58c609
     -in xxxx.ovpn.enc -out xxxx.ovpn
```

Code Obfuscation

- Signature-based malware detectors often rely solely on ***constants*** in the malware
  - String, sequence of instructions, etc.

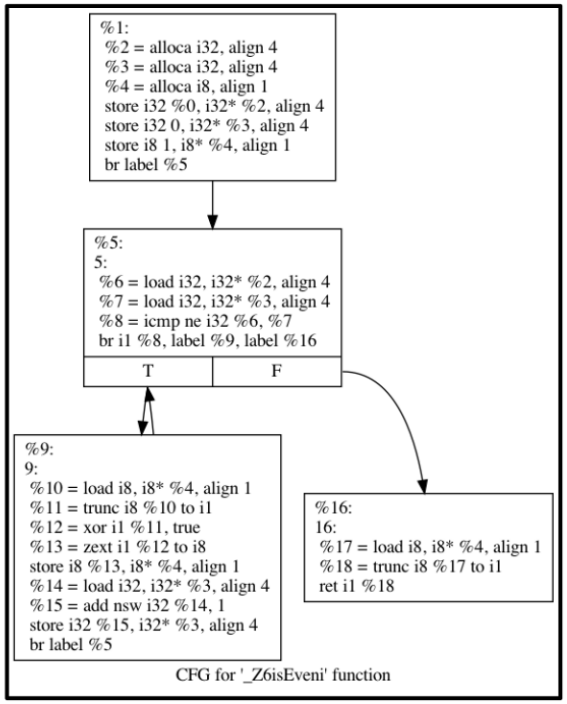
Code Obfuscation

- Signature-based malware detectors often rely solely on ***constants*** in the malware
  - String, sequence of instructions, etc.
- Approaches:
  - Remove unneeded constants ("strip" binaries)

```
❯ diff -duw <(size -Ax hello) <(size -Ax hello.debug)
--- /proc/self/fd/17    2022-03-04 16:14:48.135230786 -0500
+++ /proc/self/fd/18    2022-03-04 16:14:48.135230786 -0500
@@ -1,4 +1,4 @@
-hello  :
+hello.debug  :
 section               size     addr
 .interp               0x1c    0x318
 .note.gnu.property    0x30    0x338
@@ -27,6 +27,15 @@
 .data                 0x10   0x4000
 .bss                   0x8   0x4010
 .comment              0x25      0x0
-Total                0x7e9
+.debug_aranges        0x30      0x0
+.debug_info           0x35      0x0
+.debug_abbrev         0x15      0x0
+.debug_line           0xe8      0x0
+.debug_str            0x2f      0x0
+.debug_addr           0x10      0x0
+.debug_line_str       0x1f5     0x0
+.debug_gnu_pubnames   0x1c      0x0
+.debug_gnu_pubtypes   0xa7      0x0
+Total                0xc42
```

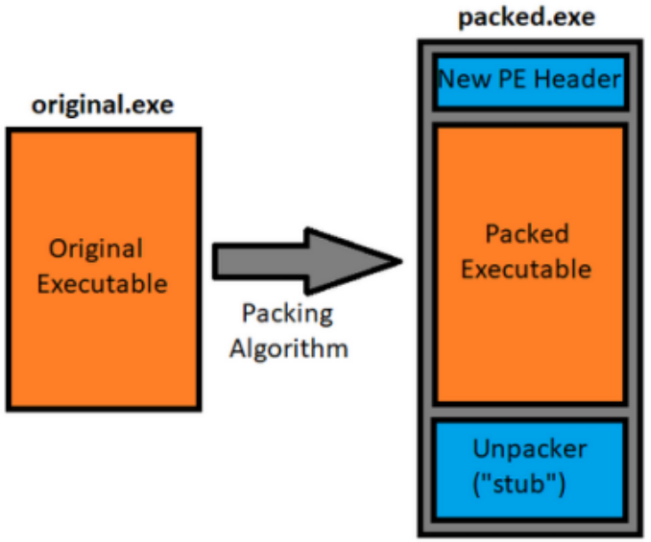
Code Obfuscation

- Signature-based malware detectors often rely solely on ***constants*** in the malware
  - String, sequence of instructions, etc.
- Approaches:
  - Use difficult-to-analyze control-flows (compilers can optimize far beyond humans)



Code Obfuscation

- Signature-based malware detectors often rely solely on ***constants*** in the malware
  - String, sequence of instructions, etc.
- Approaches:
  - Use difficult-to-analyze binary layouts ("packed" binaries or custom compilation)



- All defenses rely on ability to ***see*** the artifacts of maliciousness

Bypass: Hide

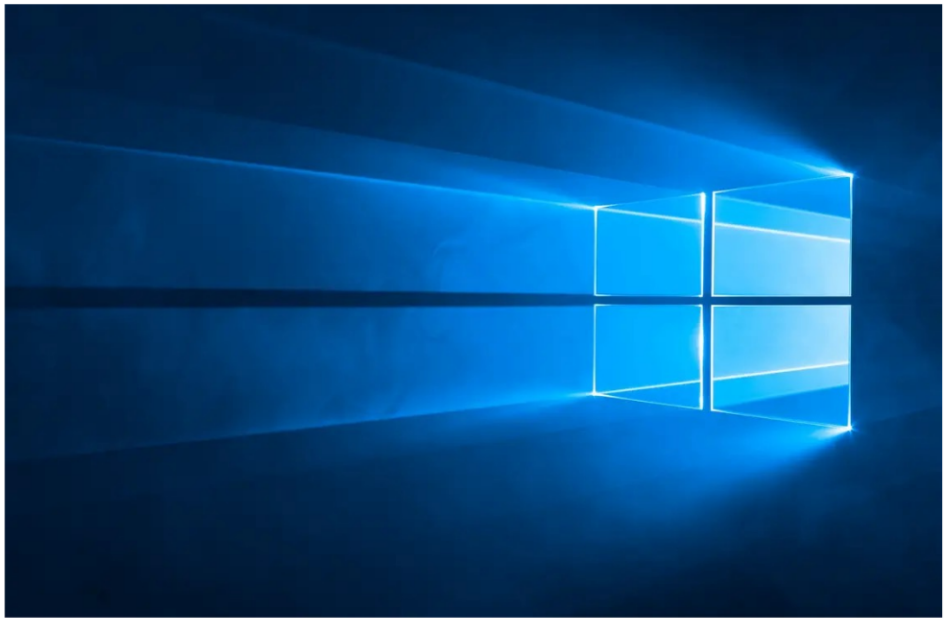
- All defenses rely on ability to ***see*** the artifacts of maliciousness

Don't Disrupt Usage

- People start looking when things seem "off"

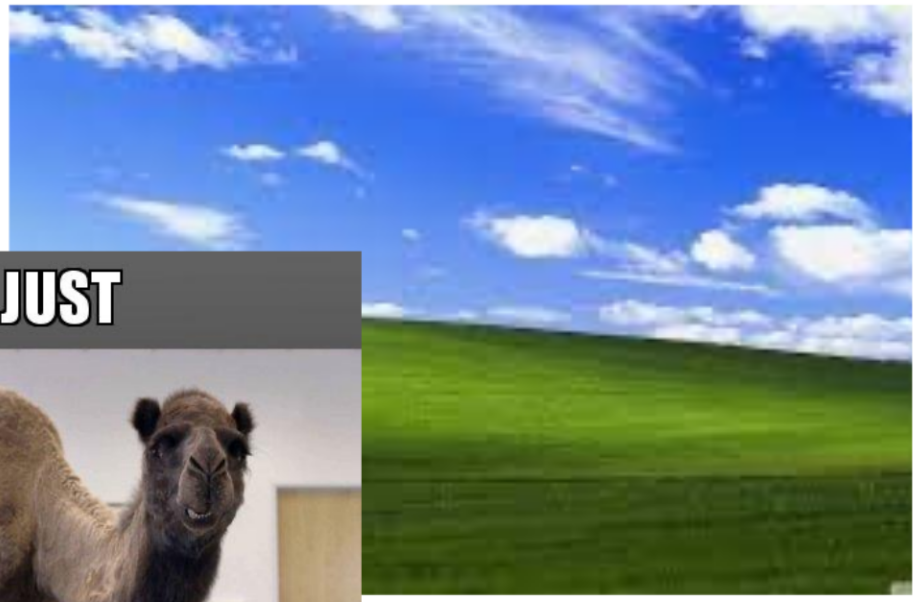
Don't Disrupt Usage

- People start looking when things seem "off"



Don't Disrupt Usage

- People start looking when things seem "off"



Direct Volume Access

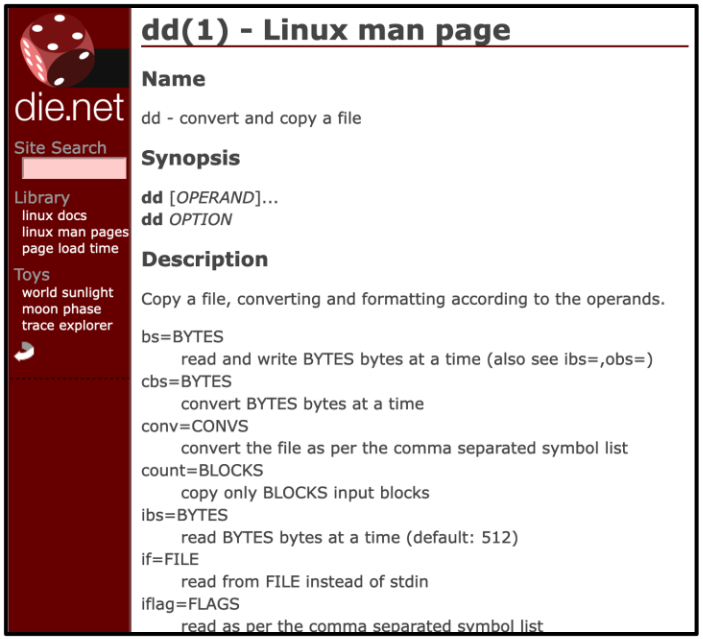
- OS mediates access to HW

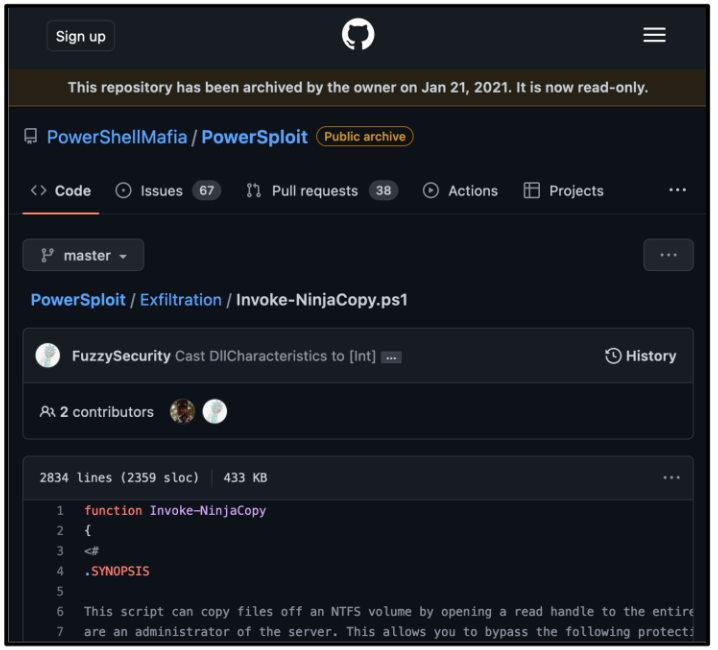
Direct Volume Access

- OS mediates access to HW
  - …except when it doesn't…

Direct Volume Access

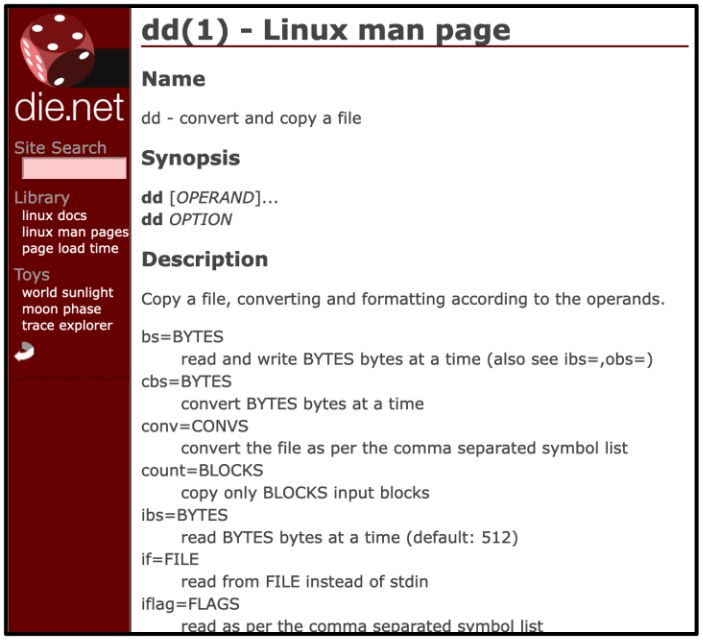
- OS mediates access to HW
  - …except when it doesn't…

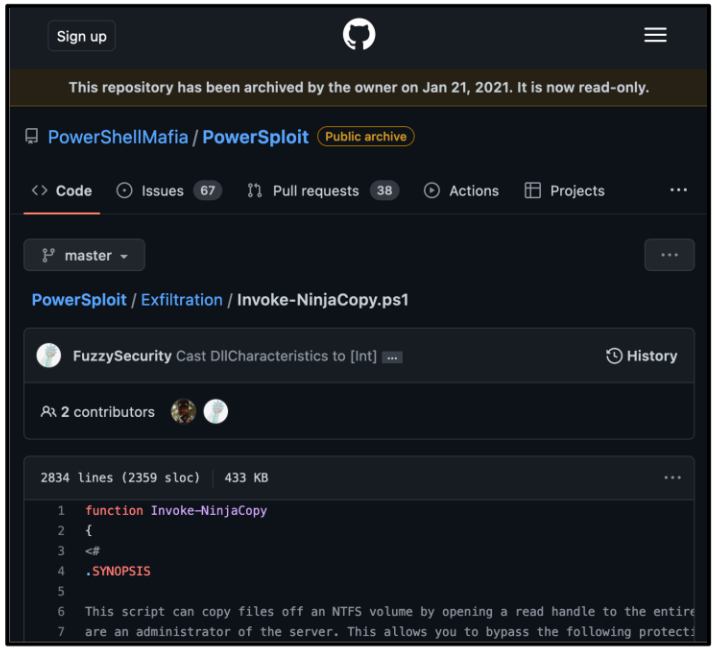




Direct Volume Access

- OS mediates access to HW
  - …except when it doesn't…





- Direct HW access allows …non-traditional… HW usage

Direct Volume Access

How

1. Open handle to disk
2. Parse filesystem metadata
3. Reconstruct own storage map (inodes, data blocks, etc)

Direct Volume Access

How

1. Open handle to disk
2. Parse filesystem metadata
3. Reconstruct own storage map (inodes, data blocks, etc)

What Can Be Used For

- Bypass OS access control and protections
- Access to “special” files (NTDS.dit, registry, etc)
- Recover *deleted* data
- Out-of-Band modification to files
- Storing artifacts

Direct Volume Access

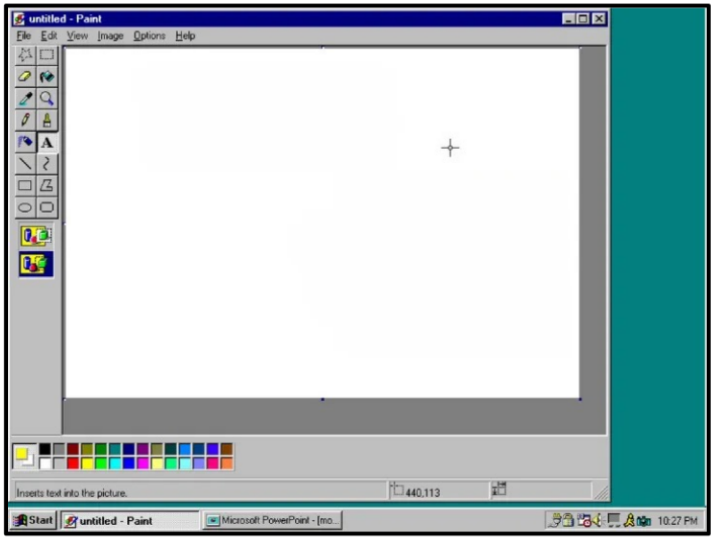
- OS m
  - …ex

- Direct HW access allows …non-traditional… HW usage

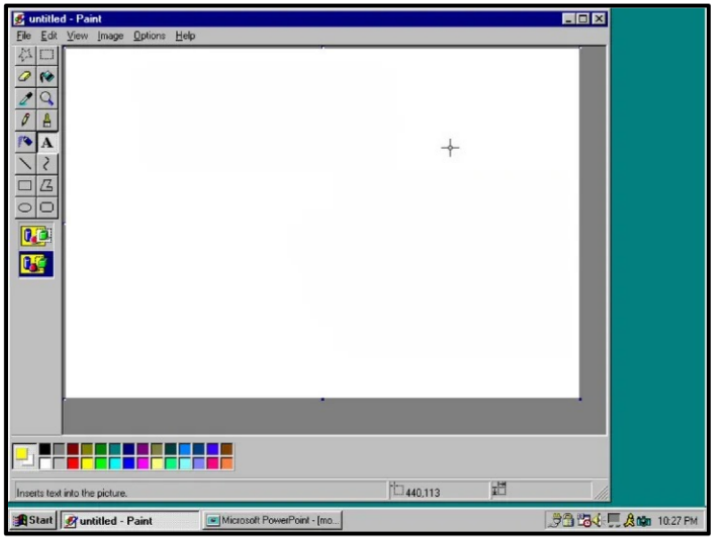
Masquerading Tools/Services

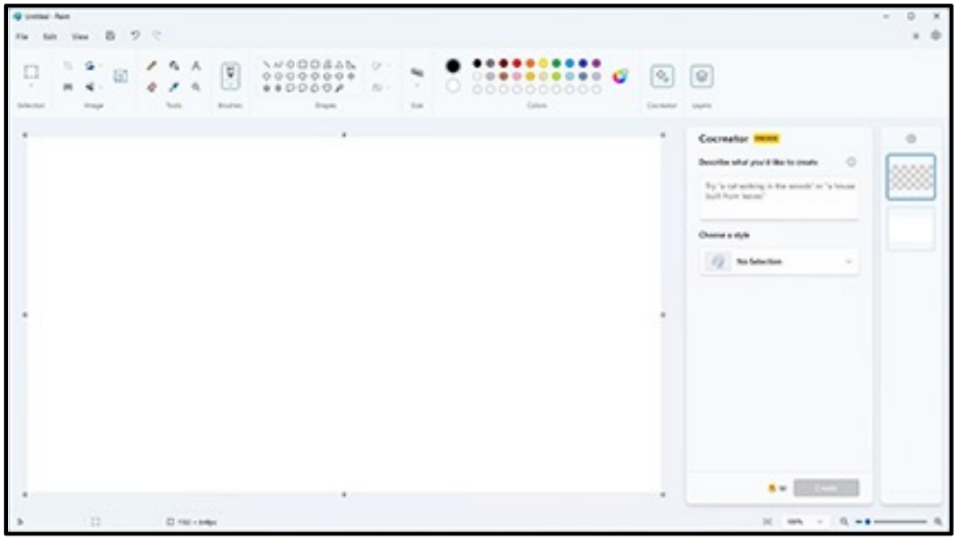
Masquerading Tools/Services

Masquerading Tools/Services

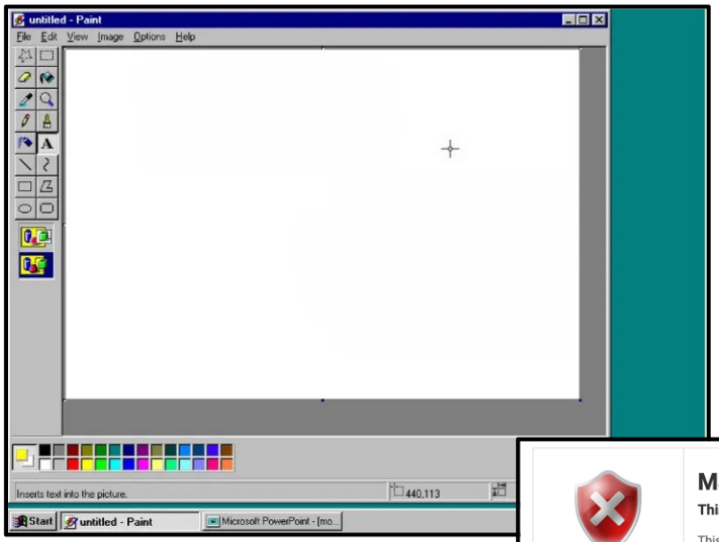


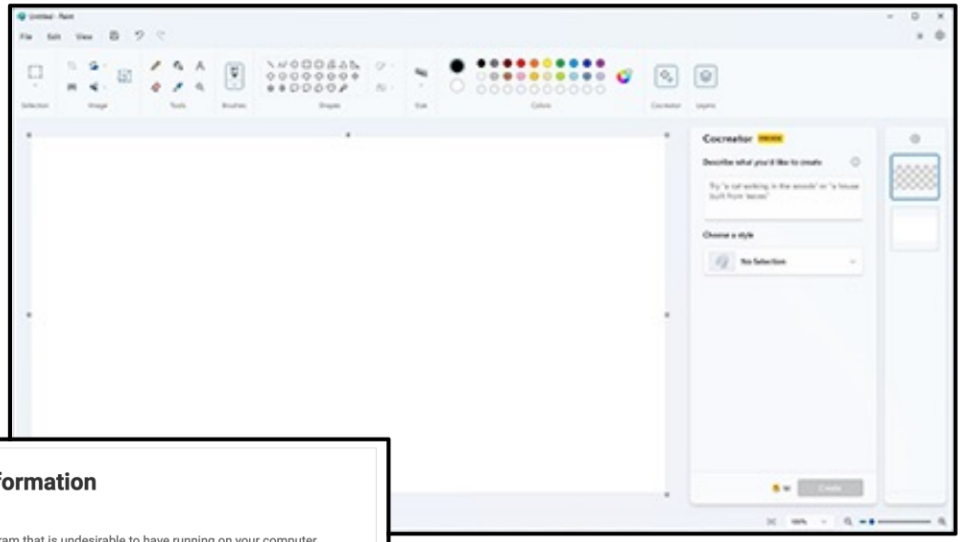
Masquerading Tools/Services





Masquerading Tools/Services





MSPAINTER.EXE Information

This is an undesirable program.

This file has been identified as a program that is undesirable to have running on your computer. This consists of programs that are misleading, harmful, or undesirable.

If the description states that it is a piece of malware, you should immediately run an antivirus and antispyware program. If that does not help, feel free to ask us for assistance in the **forums**.

Name	MS Paint
Filename	**mspainter.exe**
Command	mspainter.exe
Description	A variant of the **IRCBot** family of worms and IRC backdoor Trojans.
File Location	%System%
Startup Type	This startup entry is started automatically from a Run, RunOnce, RunServices, or RunServicesOnce entry in the registry.
HijackThis Category	**O4 Entry**

Masquerading Tools/Services

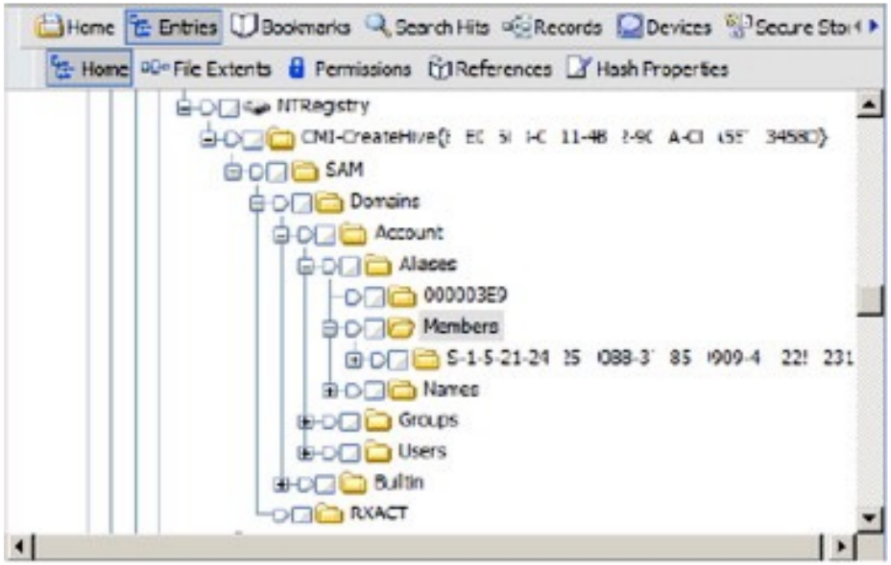
```
karim@Ubuntu2204:~$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.5 166784 11844 ?        Ss   21:56   0:01 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    21:56   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   21:56   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   21:56   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   21:56   0:00 [slub_flushwq]
root           6  0.0  0.0      0     0 ?        I<   21:56   0:00 [netns]
root          10  0.0  0.0      0     0 ?        I    21:56   0:00 [kworker/u4:0-events_power_efficie
root          11  0.0  0.0      0     0 ?        I<   21:56   0:00 [mm_percpu_wq]
root          12  0.0  0.0      0     0 ?        I    21:56   0:00 [rcu_tasks_kthread]
root          13  0.0  0.0      0     0 ?        I    21:56   0:00 [rcu_tasks_rude_kthread]
root          14  0.0  0.0      0     0 ?        I    21:56   0:00 [rcu_tasks_trace_kthread]
root          15  0.0  0.0      0     0 ?        S    21:56   0:00 [ksoftirqd/0]
root          16  0.0  0.0      0     0 ?        I    21:56   0:00 [rcu_preempt]
root          17  0.0  0.0      0     0 ?        S    21:56   0:00 [migration/0]
root          18  0.0  0.0      0     0 ?        S    21:56   0:00 [idle_inject/0]
root          19  0.0  0.0      0     0 ?        S    21:56   0:00 [cpuhp/0]
root          20  0.0  0.0      0     0 ?        S    21:56   0:00 [cpuhp/1]
root          21  0.0  0.0      0     0 ?        S    21:56   0:00 [idle_inject/1]
root          22  0.0  0.0      0     0 ?        S    21:56   0:00 [migration/1]
root          23  0.0  0.0      0     0 ?        S    21:56   0:00 [ksoftirqd/1]
```

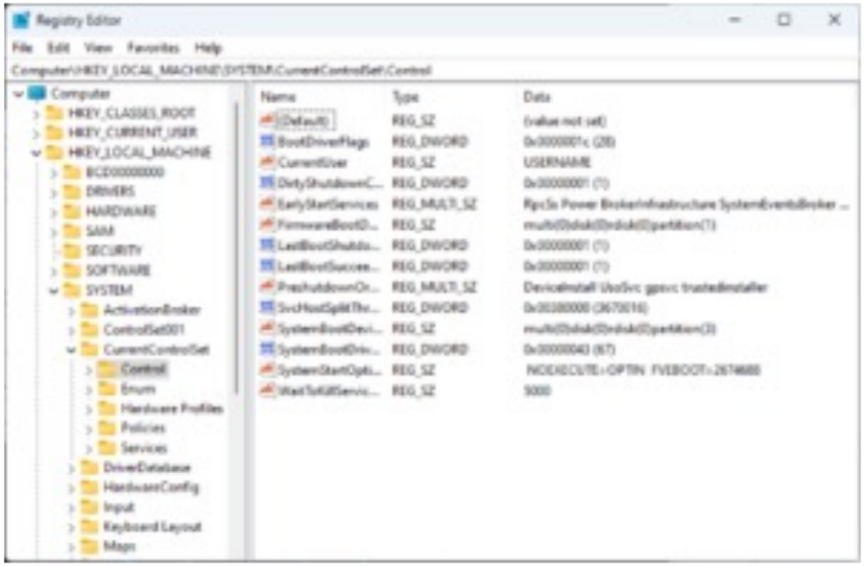
OS "protection" Features

OS "protection" Features

OS "protection" Features

- OSes have features to hide various artifacts for legitimate reasons
  - Protect important system files and administrative task execution
  - Avoid disrupting user work environments
  - Prevent users from changing files/features





OS "protection" Features

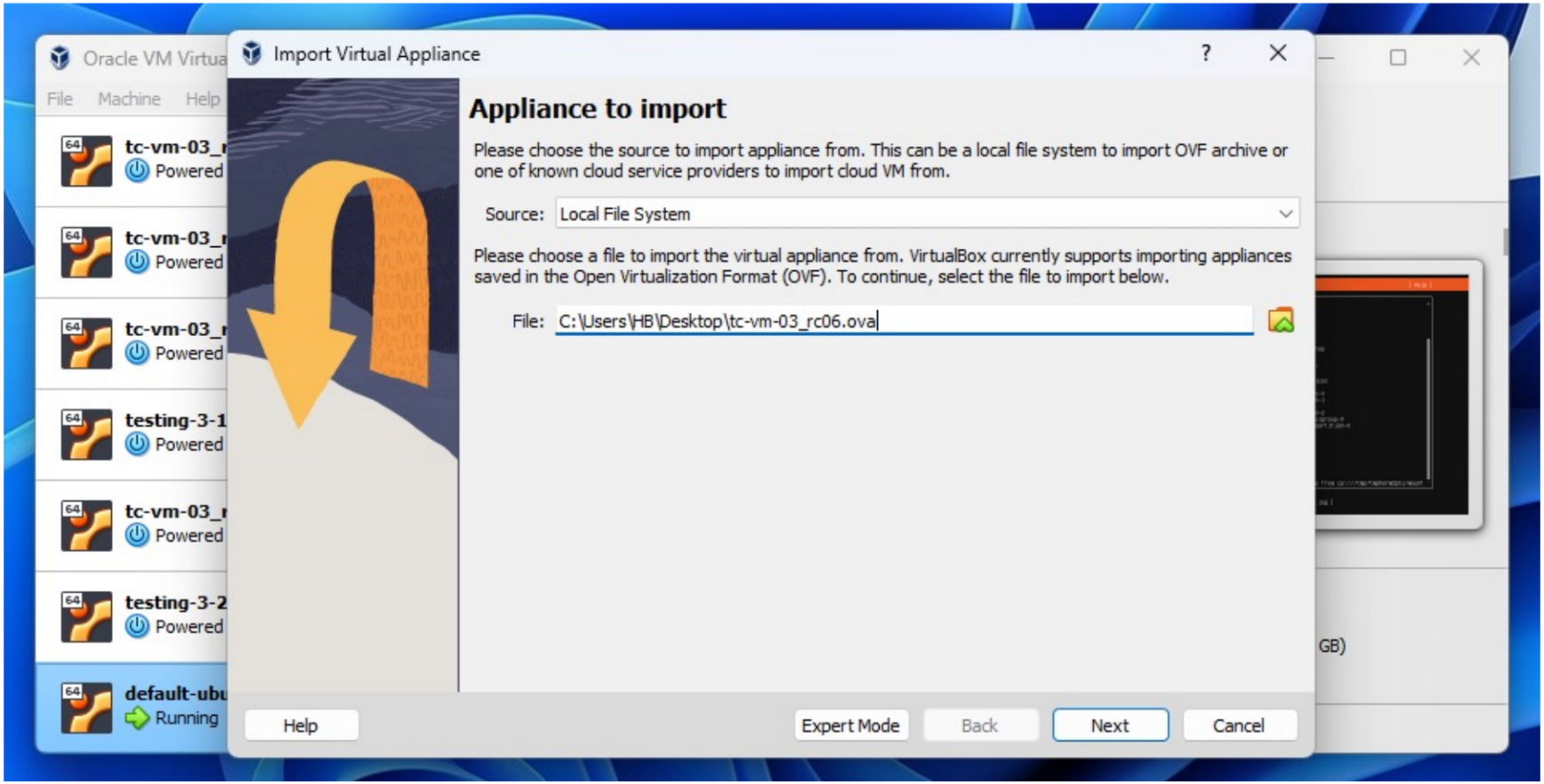
- OSes have features to hide various artifacts for legitimate reasons
  - Protect important system files and administrative task execution
  - Avoid disrupting user work environments
  - Prevent users from changing files/features
- Sub-techniques include:
  - Hidden Files and Directories
  - Hidden Users
  - NTFS File Attributes – Alternate Data Streams
  - Hidden File System
  - Virtual Instances
  - VBA Stomping

Threats and Countermeasures

Lecture 09:
Defense Evasion

COMP-5830/-6830
Spring 2025

Today: tc-vm-06_rc08



Disk Crypto: AUfw4FfWsJv4SYz52rYdvjoQ

Per-Startup Kali Config

When connecting to the local VM, have to setup Kali networking ***every time you boot***.

- `ifconfig eth0 down`
  - Stop auto-detect
- `ifconfig eth0 192.168.66.XXX netmask 255.255.255.0`
  - Set Kali VM's IP address
- `ip route add 192.168.66.0/24 dev eth0`
  - Tell Kali how to route to imported VM (1x only)

VM Usage

- Previous *approaches* are valid but must modify *mechanism* to bypass defenses
- Is setup to **intentionally** tell you (the attacker) when you've triggered defenses
  - Fail2Ban, TripWire, a *very* simple AV
  - Prints messages to the target-VM's screen when maliciousness is detected
- Demonstrates a basic, working implementation of Fail2Ban and TripWire

Things to do

- Brute-force user password w/ Fail2Ban
  - Username: `amy@`
  - Password: `Password`*XX*

Two digits (0-9)

- Run `linPEAS` without triggering AV alert
- Determine TripWire coverage(what files/dirs)
- Recover from a TripWire alert without deactivating/re-configuring
  - Demonstrates relative difficulty of recovering once triggered vs. not triggering
- Reconfigure TripWire to ignore `/etc/`

Threats and Countermeasures

Lecture 09:
Defense Evasion

COMP-5830/-6830
Spring 2025