Continuous Monitoring Effectiveness Against Detecting Insider Threat

Steven Austin

Continuous Monitoring Effectiveness Against Detecting Insider Threat

Author: Steven Austin, sjausti@hotmail.com
Advisor: Bryan Simon
Accepted: October 25, 2020

GIAC (GMON) Gold Certification

Abstract

More organizations are implementing some form of Continuous Monitoring, yet there is an increase in insider threat incidents. The number of insider threat incidents has increased by 47% in two years, from 3,200 in 2018 to 4,716 in 2020 (Epstein, 2020). This data shows insider threat is an on-going problem for organizations despite efforts to implement Continuous Monitoring. The results of this research provide organizations with evidence of Continuous Monitoring effectiveness against detecting malicious insider attack techniques.

1. Introduction

More organizations are implementing some form of Continuous Monitoring to detect configuration and software weaknesses (Bejtlich, 2013). In 2017, 61% of US businesses were actively working to adopt Continuous Monitoring as part of its overall risk management strategy ("Ultimate NIST Cyber Security Framework Guide", 2020). Although there is an increase in companies implementing Continuous Monitoring, there has also been an increase in insider threat incidents. The number of incidents due to insider threat has increased by 47% in two years, from 3,200 in 2018 to 4,716 in 2020 (Epstein, 2020). This data brings into question Continuous Monitoring effectiveness against detecting malicious insider attack techniques.

1.1. Malicious Insiders and Continuous Monitoring

Adversaries (internal or external) must complete all phases of an attack to claim success (Lockheed Martin, 2015). The primary differences between an external adversary and an internal adversary (malicious insider) when executing an attack are the malicious insider's level of access and system knowledge. There are four types of malicious insiders: the virtuous insider, the wicked insider, the vengeful insider, and the malevolent insider (Thompson, 2019). The virtuous insider is a well-intended employee who places organizations at risk through risky behavior. The consequences of the virtuous insider actions may be unknown to the employee. The wicked insider knowingly bends rules to either achieve mission objectives (good intentions) or personal interest. The vengeful insider willfully acts out against leadership or the organization as a form of retaliation. A malevolent insider intentionally sabotages a system as some form of personal gain. Malicious insider's motivations may differ, but they all share authorized access, which makes their actions difficult to detect via Continuous Monitoring.

The National Institute of Standards and Technology (NIST) introduced the concept of Continuous Monitoring in NIST Special Publication (SP) 800-37 Risk Management Framework (RMF) for Information Systems and Organizations. NIST defines Continuous Monitoring as monitoring requirements at organizational, procedural, and information system levels. This discussion focuses on Continuous Monitoring at the

system level. The Center for Internet Security (CIS) defines technical guidance for defending systems against cyber threats. The CIS Controls captures system security monitoring under Control #6 Maintenance, Monitoring and Analysis of Audit Logs. The purpose of Control #6 is to ensure adequate system logging and event analysis to identify malicious actors both internal and external. Without complete logging records, an attack may go unnoticed. There are three sub-controls within Control #6 on which the research focuses: 6.2 Activate Audit Logging, 6.3 Enable Detailed Logging, and 6.5 Central Log Management. Activate Audit Logging ensures local logging is enabled on all systems. Detailed Logging enables system logging to include detailed information. Central Log Management ensures that appropriate logs are aggregated to a central log management system for analysis and review.

Is there a correlation between a system's ability to detect malicious insider attack techniques early in the process (prior to becoming an incident) and the rise of insider threat incidents? In an attempt to answer this question, an experiment is conducted that configures a lab environment based on real-world operating systems and configurations, defines insider threat scenarios based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework, and measures scenario success based on the system's ability to detect the event.

2. Identifying Malicious Insiders Experiment

The purpose of the "Identifying Malicious Insiders" experiment is to measure audit configurations' ability to detect common insider threat exploitation techniques. The experiment consists of configuring a lab environment similar to an operational network and defining attack scenarios with example operating system commands for execution.

2.1. Malicious Insider's Experiment Lab Environment

Figure 1 describes the components of the Insider Threat Experiment Lab Environment that consist of: Red Hat Enterprise Linux (RHEL) 7, Windows 10 Workstation, and a Kiwi Syslog Server.

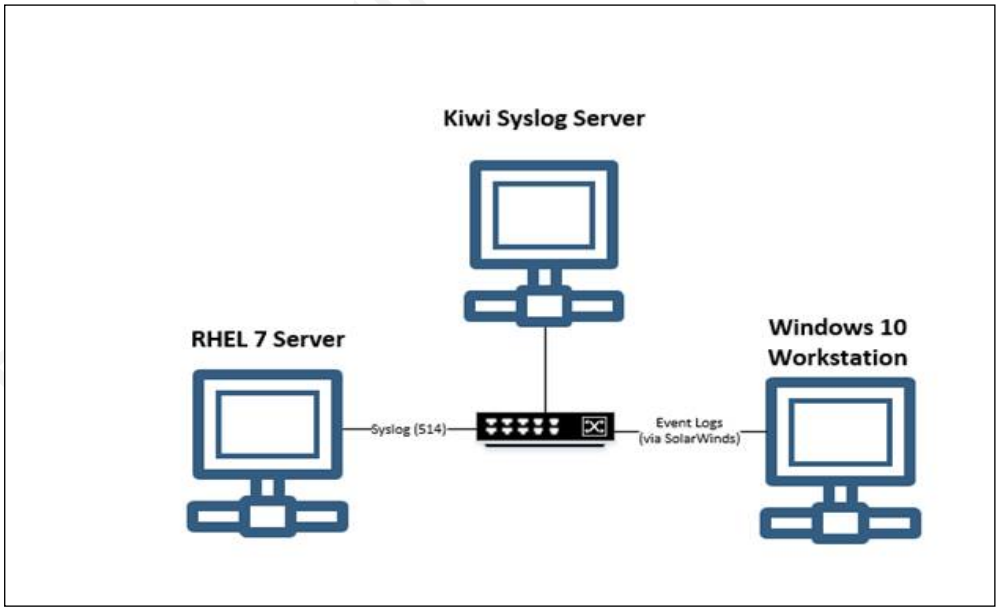

Figure 1 - Insider Threat Experiment Lab Environment

RHEL 7 and Windows 10 Workstation are two of the five most common operating systems used in networks (Melendez, 2019), therefore the output of the experiment relates to real-world examples. The operating systems are configured to forward logs to the Kiwi Syslog Server. Forwarding operating system logs to the Kiwi Syslog Server requires additional operating-system configurations. For RHEL 7, the first step is to verify rsyslog rpm is installed. Next, the system administrator needs to update the

/etc/rsyslog.conf file to include the "auditd" logs and Kiwi Syslog server IP. See RHEL 7 documentation for more information on configuring rsyslog.conf.

Windows 10 Workstation does not natively support sending event log data to a syslog server. Solarwinds Event Log Forwarder for Windows is used to integrate the Windows 10 Workstation logs to the Kiwi Syslog Server. See Solarwinds Event Log Forwarder for more information on integration.

2.1.1. RHEL 7 Audit Configuration Analysis

RHEL 7 OS is configured based on the CIS RHEL 7 Benchmark v3.0.0 Audit Guidance. Logs from "auditd" are stored in /var/log/auditd/audit.log. The "auditd" utility produces a significant number of logs as compared to the default RHEL 7 audit configurations. System administrators should verify adequate storage before configuring "auditd." The lab experiment implements all the CIS RHEL 7 Benchmark Audit configurations. Below summarizes key configurations for detecting insider threat attack techniques.

RHEL 7 Audit configuration "4.1.4 Ensure events that modify /user/group information are collected" is significant when detecting malicious insiders. Malicious insiders typically have some form of access and often attempt to identify other accounts for exploitation. Additional monitoring for account management is an early indicator of an attack. RHEL 7 Audit configuration "4.1.7 Ensure login and logout events are collected" tracks potential brute force attempts and account exploitation. RHEL 7 Audit Configuration "4.1.9 Ensure access control permission modification events are collected" monitors changes to file permissions, attributes, ownership, and group. A common technique used by malicious insiders is to modify permissions on key files to maintain persistence. Monitoring permission changes on key files provide in-depth data on potential malicious activities. RHEL 7 Audit Configuration "4.1.10 Ensure unsuccessful unauthorized file access attempts are collected" monitors for unsuccessful attempts to access files. During the data-gathering phase, malicious insiders attempt to gather system information often accessing files that they do not have adequate permissions. RHEL 7 Audit Configuration "4.1.14 Ensure changes to system administration scope (sudoers) is collected" monitors changes to the sudoers file. To persist in an environment, malicious

insiders may attempt to modify privileges. Tracking system administration changes prevents attacks early in the process. Figure 2 captures Linux Audit Configurations.

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EACCES -F auid>=1000 -F
auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EACCES -F auid>=1000 -F
auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EPERM -F auid>=1000 -F
auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat -F exit=-EPERM -F auid>=1000 -F
auid!=-1 -F key=access
-w /var/log/sudo.log -p wa -k actions
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -F auid!=-1 -F
key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -F auid!=-1 -F
key=delete
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /var/log/faillog -p wa -k logins
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
-w /var/log/tallylog -p wa -k logins
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module,delete_module -F key=modules
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -F key=mounts
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=-1 -F
key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=-1 -F
key=perm_mod
-a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -S all -F path=/usr/bin/wall -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/fusermount -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
```

```
-a always,exit -S all -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/bin/write -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/pkexec -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F auid!=-1 -
F key=privileged
-a always,exit -S all -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/netreport -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/usernetctl -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F auid!=-1 -F
key=privileged
-a always,exit -S all -F path=/usr/lib/polkit-1/polkit-agent-helper-1 -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/libexec/utempter/utempter -F perm=x -F auid>=1000 -F auid!=-1 -
F key=privileged
-a always,exit -S all -F path=/usr/libexec/dbus-1/dbus-daemon-launch-helper -F perm=x -F
auid>=1000 -F auid!=-1 -F key=privileged
-a always,exit -S all -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F auid>=1000 -F auid!=-1
-F key=privileged
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k logins
-w /var/log/btmp -p wa -k logins
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-a always,exit -F arch=b64 -S adjtimex,settimeofday -F key=time-change
```

Figure 2: CIS RHEL 7 Benchmark v3.0.0 - Audit Configurations (auditctl -l)

2.1.2. Windows 10 Workstation Audit Configuration Analysis

Windows 10 Workstation is configured based on the CIS Microsoft Windows 10 Enterprise Benchmark Audit Guidance. Windows tracks audit events via Event IDs. The

associated Event ID is identified (if applicable) for each Advanced Audit Policy Configuration. All audit configurations outlined in the benchmark are critical to identifying malicious activities. There are a few specific configurations that warrant more discussion for the lab experiment.

Windows 10 Audit Configuration "17.2.2 Ensure 'Audit Security Group Management' is set to include 'Success'" audits when a security group is created, changed, or deleted. Malicious insiders may attempt to modify privileges to escalate access or maintain persistence. Monitoring privilege changes is critical to identifying malicious insiders. Windows 10 Audit Configuration "17.2.3 Ensure 'Audit User Account Management' is set to 'Success and Failure'" monitors when a user account is created, changed, or deleted. Malicious insiders often attempt to compromise other accounts to hide their activities or maintain persistence. Windows 10 Audit Configuration "17.3.1 Ensure 'Audit PNP Activity' is set to include 'Success'" audits when plug and play detects an external device. Malicious Insiders extract data or transfer malicious software via external devices. Windows 10 Audit Configuration "17.5.6 Ensure 'Audit Special Logon' is set to include 'Success'" detects when someone logs on with administrator-equivalent privileges. Monitoring administrative account access during unusual times may detect malicious activity. Windows 10 Audit Configuration "17.6.4 Ensure 'Audit Removable Storage' is set to 'Success and Failure' monitors user attempts to access file system objects on a removable storage device. This setting identifies a malicious insider's attempt to extract sensitive data or transfer malicious code. Windows 10 Audit Configuration "17.7.1 Ensure 'Audit Audit Policy' is set to include 'Success'" monitors audit policy changes. Malicious insiders with admin level privileges may attempt to modify the audit policy to hide their malicious activities. Figure 3 depicts the Windows 10 Audit Configurations for the lab environment.

```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion Setting,Setting Value
,System,Audit Credential Validation,{0cce923f-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Application Group Management,{0cce9239-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Security Group Management,{0cce9237-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit User Account Management,{0cce9235-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit PNP Activity,{0cce9248-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Process Creation,{0cce922b-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Account Lockout,{0cce9217-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Group Membership,{0cce9249-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Logoff,{0cce9216-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Logon,{0cce9215-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Logon/Logoff Events,{0cce921c-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Special Logon,{0cce921b-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Detailed File Share,{0cce9244-69ae-11d9-bed3-505054503030},Failure,,2
,System,Audit File Share,{0cce9224-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Object Access Events,{0cce9227-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Removable Storage,{0cce9245-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Audit Policy Change,{0cce922f-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Authentication Policy Change,{0cce9230-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Authorization Policy Change,{0cce9231-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit MPSSVC Rule-Level Policy Change,{0cce9232-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Policy Change Events,{0cce9234-69ae-11d9-bed3-505054503030},Failure,,2
,System,Audit Sensitive Privilege Use,{0cce9228-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit IPsec Driver,{0cce9213-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other System Events,{0cce9214-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Security State Change,{0cce9210-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit Security System Extension,{0cce9211-69ae-11d9-bed3-505054503030},Success,,1
,System,Audit System Integrity,{0cce9212-69ae-11d9-bed3-505054503030},Success and Failure,,3
~
```

Figure 3 - Windows 10 Audit Configurations

2.2. Malicious Insider's Attack Scenario Definition

MITRE released the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework in 2015. The ATT&CK Framework outlines up-to-date attack techniques based on real-world data. The ATT&CK Framework provides 12 tactics that are exploited across various operating systems to include Windows, Mac, and Linux environments. The insider threat experiment focuses on four MITRE Framework tactical areas: Privilege Escalation, Credential Discovery, Maintain Persistence, and Data Exfiltration. Techniques are executed on RHEL 7 and Windows 10 Workstation.

Privilege Escalation consists of techniques that malicious insiders use to gain elevated system permissions. A system's ability to detect the misuse of administrative privileges is critical to detecting malicious insiders (CIS, 2019). Due to restricting account privileges, malicious insiders often require additional privileges to execute their objectives. The Privilege Escalation experiment measures a system's ability to detect a malicious insider. RHEL 7 Privilege Escalation techniques include: attempting to switch to a higher privileged user, set higher-level privileges on an executable using setgid/setuid, and executing privileged commands using "sudo." Windows 10 privilege

escalation techniques include: activating the local admin account and logging onto the system and modifying the screen saver registry key to execute a test executable.

Malicious insiders may attempt to compromise other accounts to hide their activities. The credential discovery experiment looks at an operating system auditing capability to detect account discovery techniques. RHEL 7 credential discovery techniques include: accessing the contents of /etc/passwd and /etc/shadow, accessing another user's Bash History file, and accessing the password policy for root. Windows 10 credential discovery techniques include obtaining a listing of local system accounts, enumerating shared drives, accessing the password policy, and accessing local groups. Outside of planned activities, credential discovery techniques are atypical for an operational environment. A system with the ability to detect credential discovery techniques early in the process can potentially prevent an insider incident.

Another goal of a malicious insider is to maintain persistence. Maintaining persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. RHEL 7 techniques review the system's ability to detect: modifying a user's SSH authorized_keys, using the scheduling utility to execute a test script, creating a rogue service, updating a user's shell to execute malicious content, and updating the PAM module to modify authentication rules. Windows 10 techniques include using Background Intelligent Transfer Service (BITS) to transfer a malicious file and adding a test script to the startup registry key. Continuous Monitoring's ability to detect maintaining persistence techniques allows early detection of malicious activities.

The final technique this experiment focuses is the OS's ability to detect transferring data to/from an external device. Malicious insiders often attempt to extract sensitive data or transfer malicious files to the targeted machine to further execute their kill chain. The RHEL 7 technique mounts a USB directory and attaches a USB drive to the device. The Windows 10 technique attaches a USB drive to the device. Since Windows Plug and Play is already enabled, the device automatically mounts.

3. Malicious Insider's Test Execution and Results

Appendix A: Insider Threat Attack Scenarios - RHEL 7 outlines the detailed execution steps and results for each RHEL 7 scenario. Appendix B: Insider Threat Attack Scenarios - Windows 10 outlines the execution steps and results for Windows 10. Section 3.1 RHEL 7 Test Execution and Results Summary and Section 3.2 Windows 10 Test Execution and Results Summary reviews the test execution results and provides additional analysis based on key observations. Reference the appendices for detailed execution steps and results for all scenarios.

3.1. RHEL 7 Test Execution and Results Summary

Table 3.1 summarizes the RHEL 7 test execution and results. RHEL 7 has a 75% detection rate based on the defined scenarios.

MITRE ATT&CK Scenarios	Total Techniques	Detected	Not Detected
Privilege Escalation	3	3	0
Maintain Persistence	7	6	1
Credential Discovery	4	1	3
Data Exfiltration	2	2	0
Total	**16**	**12**	**4**

Table 3.1 RHEL 7 Attack Summary

RHEL 7 audit configurations detected 3 out of 3 of the Privilege Escalation scenarios. The "switch user to root" audit logs captured the date and time a user switched to root. Users typically access systems with a lower-privileged account and use "sudo" to execute privileged commands. A user switching to the root user is not a typical scenario and the proper verification/responses should be defined once detected. The "set uid/gid command" was detected via the audit log configurations. Below is an example of the audit logs for "set uid: u+s test.sh":

Attack Scenario	Summary	Linux Commands	Log Summary
Privilege Escalation	An adversary may perform shell escapes or exploit vulnerabilities in an application with the setuid or setgid bits to run the code in a different user's context.	As root user, create a shell script, and change user id/group id to that user. • Set uid flag for file: chmod u+s test.sh	Logs Detected: ***Yes*** • Set uid flag for File: ***Yes***

(Set uid flag for file: chmod u+s test.sh)

type=SYSCALL ***(Highlight #1)*** msg=audit(1598730400.076:5928): arch=c000003e syscall=268 success=yes exit=0 a0=ffffffffffffff9c a1=230f0f0 a2=9ed a3=7ffdc67a37a0 items=1 ppid=18098 pid=18366 ***(Highlight #2)*** auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="chmod"***(Highlight #3)*** exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="perm_mod"
type=CWD msg=audit(1598730400.076:5928): ***(Highlight #4)*** cwd="/tmp"
type=PATH msg=audit(1598730400.076:5928): item=0 ***(Highlight #4)*** name="test.sh" inode=16784427 dev=fd:00 mode=0100755 ouid=0 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598730400.076:5928): proctitle=63686D6F6400752B7300746573742E7368

When capturing audit logs, it is important to identify the date, time, the user who executed the action, and the object in which the action was executed. A security operations analyst identifying this information based on the logs requires an in-depth knowledge of the RHEL 7 operating system. Highlight #1, as seen above, is the Epoch Time ("1598730400.076") and audit event ID ("5928") of the executed scenario. An analyst can convert epoch time to normal time using the "date -d@ <epoch time>" command. Highlight #2 captures the user (auid=1000) who executed the action. The analyst will need to convert the "auid" to the actual user. Highlight #3 captures the action (/usr/bin/chmod) that was executed and Highlight #4 captures the object in which the action was executed ("/tmp/test.sh). A SOC team should involve product experts who can interpret audit logs to ensure malicious activities don't go undetected.

RHEL 7 audit configurations detected 6 out of 7 of the Maintain Persistence scenarios. The RHEL 7 audit configurations failed to detect trap commands added when

the "Exit" interrupt is signaled. The trap command catches signals and executes code when the signal occurs. A SOC analyst loses insight into a malicious user attempting to maintain persistence due to a lack of auditing of when the trap command is utilized. The trap command is executed at the same privilege levels as the user who entered the command. Given the uptime of some servers, a command could be executed days or weeks later. A SOC can limit user privileges to help combat this threat.

RHEL 7 audit configurations detected 1 out of 4 of the Credential Discovery scenarios. It did not detect a user accessing the contents of "/etc/passwd" or "/etc/shadow." Adversaries may attempt to crack passwords by accessing the passwd and shadow files. The system's failure to detect when these critical files are accessed impacts a SOCs ability to identify early phases of a potential attack. A possible recommendation is to configure additional monitoring on the passwd and shadow files. As with any configuration updates, a SOC should analyze other impacts (frequency of logs) before making any changes.

RHEL 7 audit configurations detected the Data Exfiltration (Transferring Data to/from an External Device) scenarios. The audit logs did not include the files transferred but did capture that a USB was connected and mounted. RHEL 7's ability to detect this scenario is significant. Many malicious insiders' scenarios include transferring data to/from a targeted system. A SOC should have appropriate response scenarios when this event is detected to combat insider threats.

3.2. Windows 10 Test Execution and Results Summary

Table 3.2 summarizes the Windows 10 Workstation test execution and results. Windows 10 Workstation audit configurations detected 77% of the attack scenarios.

Table 3.2 Windows 10 Workstation Attack Summary

MITRE ATT&CK Scenarios	Total Techniques	Detected	Not Detected
Privilege Escalation	2	1	1
Maintain Persistence	2	1	1
Credential Discovery	4	4	0

MITRE ATT&CK Scenarios	Total Techniques	Detected	Not Detected
Extract Data	1	1	0
Total	**9**	**7**	**2**

Windows 10 audit configurations detected 1 out of 2 of the Privilege Escalation scenarios. Windows 10 audit logs for enumerating local users via the "net user" command are summarized below:

Attack Scenario	Summary	Windows Commands	Log Summary
Privilege Escalation	Adversaries may obtain (via enumerating users) and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.	Access Administrator account: • Enumerate local users: net user	Logs Detected: ***Yes*** • Enumerate local users: Yes (Event ID 4798)

Enumerate Local Users (Event ID 4798)

A user's local group membership was enumerated.
Subject:
Security ID: WINDEV2007EVAL\User
Account Name: User
Account Domain: WINDEV2007EVAL
Logon ID: 0x1FEB9EC
User:
Security ID: WINDEV2007EVAL\Administrator
Account Name: Administrator
Account Domain: WINDEV2007EVAL
Process Information:
Process ID: 0xfcc
Process Name: C:\Windows\System32\net1.exe

Windows 10 Event ID 4798 tracks local user account enumeration. The enumeration of local user's audit logs is very detailed and provides sufficient information to identify and respond to an attack. Critical information in the enumerating local user's audit log

includes: ***Event ID:*** 4798, ***Task Executed***: "A user's local group membership was enumerated", ***User who Executed the Task***: "WINDEV2007EVAL\User", **User Enumerated:** "WINDEV2007EVAL\Administrator". Event time is a critical component and although not captured in the example, it was captured in the Windows detailed event logs. The Windows 10 Privilege Escalation technique of modifying the Windows screen saver registry value was not detected. Malicious insiders often manipulate registry values to escalate privileges or maintain persistence. A SOC's ability to detect unauthorized registry changes is imperative to identifying possible attacks.

Windows 10 audit configurations detected 1 out of 2 of the Maintain Persistence scenarios. Adding an executable to the "Run" registry key was not detected. Modifying the "Run" and "Start" registry values is a key technique used by malicious actors to maintain persistence. The inability of Windows 10 audit configurations to detect this scenario introduces significant risk to the security operations. More research is needed (that is beyond the scope of this paper) as to why auditing registry value changes is not included in the Windows 10 CIS Benchmarks. Windows 10 Audit configurations did detect transferring files using the Background Intelligent Transfer Service (BITS) service.

Windows 10 audit configurations detected 100% of the Credential Discovery techniques via Event ID 4688:

Attack Scenario	**Summary**	**Windows Commands**	**Log Summary**
Credential Discovery	Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.	Attempt to get local user information by typing: ***net user*** and ***net localgroup***	Logs Detected: • net user: Yes - Event ID 4688 (Process Creation) • net localgroup: Yes - Event ID 4688 (Process Creation)
Net User Command (Event ID: 4688)			

A new process has been created.

Creator Subject:
- Security ID: WINDEV2007EVAL\User
- Account Name: User
- Account Domain: WINDEV2007EVAL
- Logon ID: 0x36474B0

Target Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Process Information:
- New Process ID: 0x1c40
- New Process Name: C:\Windows\System32\net.exe
- Token Elevation Type: %%1937
- Mandatory Label: Mandatory Label\High Mandatory Level
- Creator Process ID: 0xd84
- Creator Process Name: C:\Windows\System32\cmd.exe
- Process Command Line:

The "Security ID" field identifies the user who executed the action. The "New Process Name" identifies the processes name, but not the parameters. A SOC analyst who understands the "net" command parameter is critical in order to determine the type of response. The "net" command parameters are not included in the Windows audit logs, which impacts an analyst's ability to review the impact of the command.

A critical scenario exercised by malicious insiders is connecting unauthorized external devices and attempting to extract data or installing malware. Windows 10 audit configurations identified this attack scenario under Event ID 6416:

Attack Scenario	Summary	Windows Commands	Log Summary
Exfiltration	Adversaries may attempt to exfiltrate data over a USB connected physical device.	Connect USB to Computer	Logs Detected: Yes • Event ID: 6416 A new external device was recognized by the system

(Event ID: 6416)

A new external device was recognized by the system.

```
Subject:
    Security ID:            SYSTEM
    Account Name:           WINDEV2007EVAL$
    Account Domain:         WORKGROUP
    Logon ID:               0x3E7

Device ID:    SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Generic&Prod_Mass_Storage&Rev_1100#062419-
10390&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

Device Name:    SEC511

Class ID:           {eec5ad98-8080-425f-922a-dabf3de3f69a}

Class Name:    WPD

Vendor IDs:    -

Compatible IDs:
        wpdbusenum\fs
        SWD\Generic
```

The Windows event logs capture pertinent information about the device including Name and ID. Event ID 6416 does not capture the user who connected the device, but the user can be correlated from other Windows 10 logs such as Logon/Log offs.

4. Conclusion

Continuous Monitoring detects insider threat techniques at a high rate. Given Continuous Monitoring insider threat detection capability, why is there an increase in insider threat incidents? The experiment showed that a system's ability to detect insider threat attack techniques is only part of what is needed to stop insider threat incidents. An organization developing an Insider Threat Program that includes sufficient staff with the appropriate expertise and an auditing strategy based on the latest attack techniques is critical to combating insider threat attacks.

The two operating systems in this experiment produced over 6,000 security logs within six hours. The majority of the logs were determined to be normal system activities and not a result of the attack scenarios. If this is expanded to hundreds of operating systems over twenty-four hours, the amount of audit data can quickly become difficult to manage. To manage the logs, a security analyst needs to know their network and the system components within the network. Malicious insiders can go undetected if the analysts do not have sufficient knowledge to interpret the audit logs received.

Due to the number of audit logs received, organizations should have an insider threat program that includes an audit strategy and sufficient staff to execute that strategy. Organizations can start with industry frameworks to help determine the tools and techniques for malicious insiders. The SOC staffing plan should include sufficient resources to manage the audit logs, but also implement separation of duties. An organization that is not sufficiently staffed may have individuals acting in multiple roles that increase the risk that a malicious insider will go undetected. If John is a malicious insider who is both the System Administrator and the Security Monitor, John will probably not detect himself. Separating key positions lowers the risk of a malicious insider going undetected.

Based on the Insider Threat audit strategy, a SOC should consider additional audit configurations beyond industry standards to detect targeted attack techniques. The MITRE ATT&CK Framework has several techniques that modify Windows 10 registry values, but the Windows 10 CIS Benchmark does not enable registry auditing. The

Windows 10 Advanced Audit Policy has a "Audit Registry" setting under "**Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access**". The "Audit Registry" policy setting allows you to audit access and modifications to registry objects. A security audit event is generated only for objects that have system access control lists (SACLs) specified, and only if the type of access requested and the account making the request match the settings in the SACL. Monitoring registry changes enhances a SOC's ability to detect potential insider threats.

References

Beena A. L; Humayoon, K. S. (2019, March 7-8). *Information Security Insider Threats in Organizations and Mitigation Techniques.* IEEE Magazines and Journals. https://ieeexplore.ieee.org/document/8995088

Bejtlich, Richard. (2013). The Practice of Network Security Monitoring (Kindle Locations 333-334). No Starch Press.

Center for Internet Security (CIS). (2019, April 1). CIS Controls version 7. Retrieved from https://www.cisecurity.org/

Claycomb W. R., Huth C. L., Phillips B., Flynn L., and McIntire D. (2013, October 8-11). Identifying indicators of insider threats: Insider IT sabotage. IEEE Magazines and Journals. https://ieeexplore.ieee.org/document/6922038

Cole, E. (2017, August). Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey. SANS Institute Information Security Reading Room. https://www.sans.org/reading-room/whitepapers/analyst/defending-wrong-enemy-2017-insider-threat-survey-37890

Epstein, J. (2020, January 29). 2020 Cost of Insider threats. Ponemon Institute Study. https://www.observeit.com/cost-of-insider-threats/

Lockheed Martin. (2015). Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Melendez, Steven (2019, April 19). Five Common Operating Systems. https://smallbusiness.chron.com/five-common-operating-systems-28217.html

MITRE. (2015). MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework. Retrieved from https://attack.mitre.org/

NIST. (2018, December). NIST Special Publication 800-37: Risk Management Framework for Information Systems and Organizations Revision 2. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

RHEL 7 Audit Events - Understanding Audit Log Files. (2020, September 04). Retrieved from https://access.redhat.com/documentation/enus/red_hat_enterprise_linux/6/html/security_guide/sec-understanding_audit_log_files

Solarwinds. (2020, August). Event Log Fowarder for Windows. Retrieved from https://www.solarwinds.com/free-tools/event-log-forwarder-for-windows?CMP=SYN-RVW-4SYS-SW_NA_X_RR_CPC_FT_EN_LMSI_SW-ELF-X_PDP_X-X

Thompson, E. E. (2019). The Insider Threat - Assessment and Mitigation of Risks. CRC Press. https://www.crcpress.com

Ultimate NIST Cyber Security Framework Guide - Unpack the NIST CSF in 10 Minutes or Less. (2020, September 04). Retrieved from https://www.cybersaint.io/ultimate-nist-cybersecurity-framework-adoption-guide?utm_term=nist%20cyber%20framework&utm_campaign=NIST+CSF&utm_source=adwords&utm_medium=ppc&hsa_cam=924792662&hsa_grp=51829911532&hsa_mt=b&hsa_src=g&hsa_kw=nist%20cyber%20framework&hsa_tgt=kwd-307430380993&hsa_net=adwords&hsa_acc=8017196505&hsa_ver=3&hsa_ad=269747481293&gclid=EAIaIQobChMI-57ZurTO6wIVA9bACh0Syw-0EAMYASAAEgLjgfD_BwE

Appendix A: Insider Threat Attack Scenarios - RHEL 7

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
Privilege Escalation	T1078.001	Initial Access → Default Accounts	Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.	As an unprivileged user, attempt to access the root account • Switch user to root: su - root	Logs Detected: ***Yes***
	(Logs: "su - root") Aug 27 22:26:15 localhost su: pam_unix(su-l:session): session opened for user root by user1 (uid=1000)				

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1548.001	Privilege Escalation → Abuse Elevation Control Mechanism → Setuid/Setgid	An adversary may perform shell escapes or exploit vulnerabilities in an application with the setuid or setgid bits to get code running in a different user's context.	As root user, create a shell script, and change user id/group id to that user. • Create executable file: vi /tmp/test.sh • Change Permissions: chmod 755 test.sh • Set uid flag for file: chmod u+s test.sh • Set gid flag for file: chmod g+s test.sh • Execute shell script: ./tmp/test.sh	Logs Detected: ***Yes*** • Create Executable File: ***No*** • Change Permissions: ***Yes*** • Set uid flag for File: ***Yes*** • Set gid flag for file: **Yes** • Execution of shell script: ***No***

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Change Permissions: chmod 755 test.sh) type=SYSCALL msg=audit(1598730305.567:5922): arch=c000003e syscall=268 success=yes exit=0 a0=ffffffffffffff9c a1=e070f0 a2=1ed a3=7fff0900f960 items=1 ppid=18098 pid=18364 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="chmod" exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="perm_mod" type=CWD msg=audit(1598730305.567:5922): cwd="/tmp" type=PATH msg=audit(1598730305.567:5922): item=0 name="test.sh" inode=16784427 dev=fd:00 mode=0100755 ouid=0 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598730305.567:5922): proctitle=63686D6F6400373535007465737 42E7368 ***(Set uid flag for file: chmod u+s test.sh)*** type=SYSCALL msg=audit(1598730400.076:5928): arch=c000003e syscall=268 success=yes exit=0 a0=ffffffffffffff9c a1=230f0f0 a2=9ed a3=7ffdc67a37a0 items=1 ppid=18098 pid=18366 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="chmod" exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="perm_mod" type=CWD msg=audit(1598730400.076:5928): cwd="/tmp" type=PATH msg=audit(1598730400.076:5928): item=0 name="test.sh" inode=16784427 dev=fd:00 mode=0100755 ouid=0 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598730400.076:5928): proctitle=63686D6F6400752B7300746573742E7368 ***(Set gid flag for file: chmod g+s test.sh)*** type=SYSCALL msg=audit(1598730511.611:5937): arch=c000003e syscall=268 success=yes exit=0 a0=ffffffffffffff9c a1=15390f0 a2=ded a3=7ffef49b7620 items=1 ppid=18098 pid=18367 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="chmod" exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="perm_mod" type=CWD msg=audit(1598730511.611:5937): cwd="/tmp" type=PATH msg=audit(1598730511.611:5937): item=0 name="test.sh" inode=16784427 dev=fd:00 mode=0104755 ouid=0 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598730511.611:5937): proctitle=63686D6F6400672B7300746573742E7368			

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1548.003	Privilege Escalation → Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the suoders file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.	• Modify /etc/sudoers file to enable "No Password" when executing sudo commands • Add user to the "Wheel" group with "usermod -aG wheel <username>" command • As the user added to the "Wheel" group, execute "sudo vi /etc/sudoers" command	Logs Detected: • Modify /etc/sudoers: ***Yes*** • Add user to the "Wheel" Group: ***Yes*** • Execute "sudoers vi" command: ***Yes***

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Modify /etc/sudoers) type=PATH msg=audit(1598635526.778:3613): item=2 name="/etc/sudoers" inode=16784460 dev=fd:00 mode=0100440 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.778:3613): item=3 name="/etc/sudoers~" inode=16784460 dev=fd:00 mode=0100440 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.778:3614): item=0 name="/etc/sudoers" objtype=UNKNOWN cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.778:3615): item=1 name="/etc/sudoers" inode=16777285 dev=fd:00 mode=0100640 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.782:3616): item=0 name="/etc/sudoers" inode=16777285 dev=fd:00 mode=0100640 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.782:3617): item=0 name="/etc/sudoers" inode=16777285 dev=fd:00 mode=0100640 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.783:3618): item=0 name="/etc/sudoers" inode=16777285 dev=fd:00 mode=0100440 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598635526.783:3619): item=1 name="/etc/sudoers~" inode=16784460 dev=fd:00 mode=0100440 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 ***(Add user to the "Wheel" Group)*** type=SYSCALL msg=audit(1598636207.674:3664): arch=c000003e syscall=87 success=yes exit=0 a0=5641de438080 a1=7ffcf1462fb0 a2=1 a3=2 items=2 ppid=15934 pid=16427 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=3 comm="usermod" exe="/usr/sbin/usermod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="delete" type=CWD msg=audit(1598636207.674:3664): cwd="/usr/bin" type=PATH msg=audit(1598636207.674:3664): item=0 name="/etc/" inode=16777281 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598636207.674:3664): item=1 name="/etc/passwd.16427" inode=16784460 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 ***(Execute "sudoers vi" command)*** Aug 28 14:31:05 localhost sudo: saustin : TTY=tty5 ; PWD=/boot ; USER=root ; COMMAND=/bin/vi /etc/sudoers Aug 28 14:31:05 localhost sudo: pam_unix(sudo:session): session opened for user root by saustin(uid=0)				

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
Maintain Persistence	T1098.004	Persistence → Account Manipulation → SSH Authorized Keys	Adversaries may modify the SSH authorized_keys file to maintain persistence on a victim host. Linux distributions and macOS commonly use key-based authentication to secure the authentication process of SSH sessions for remote management.	• As a regular user, Modify PubkeyAuthencatication to "Yes" and in /etc/ssh/sshd_config file • As a regular user, Generate keys using "ssh-keygen" • Modify <user-home>/.ssh/authorized_keys to configure remote access	Logs Detected: • Access/Modify /etc/ssh/sshd_config as a regular user: ***Yes*** • Generate keys using "ssh-keygen": ***Yes*** • Modify authorized keys: ***Yes***

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Access/Modify /etc/ssh/sshd_config as a regular user) Aug 28 15:09:47 localhost sudo: saustin : TTY=tty5 ; PWD=/boot ; USER=root ; COMMAND=/bin/vi /etc/ssh/sshd_config Aug 28 15:09:47 localhost sudo: pam_unix(sudo:session): session opened for user root by saustin(uid=0) ***(Generate keys using "ssh-keygen")*** type=USER_CMD msg=audit(1598642903.831:4139): pid=16709 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/saustin" cmd="ssh-keygen" terminal=tty5 res=success' ***(Modify authorized keys)*** type=PATH msg=audit(1598643308.816:4172): item=1 name=".id_rsa.pub.swx" inode=16784466 dev=fd:00 mode=0100600 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643308.816:4173): item=1 name=".id_rsa.pub.swp" inode=16784464 dev=fd:00 mode=0100600 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643308.817:4174): item=0 name=".id_rsa.pub.swp" inode=16784464 dev=fd:00 mode=0100600 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.615:4178): item=2 name="id_rsa.pub" inode=16784463 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.615:4178): item=3 name="id_rsa.pub~" inode=16784463 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.620:4179): item=0 name="id_rsa.pub" inode=17011846 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.620:4180): item=0 name="id_rsa.pub" inode=17011846 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.620:4181): item=1 name="id_rsa.pub~" inode=16784463 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598643316.620:4182): item=1 name="/home/saustin/.ssh/.id_rsa.pub.swp" inode=16784464 dev=fd:00 mode=0100644 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:ssh_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0		

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1053.001	Execution → Scheduled Task/Job	Adversaries may abuse the ***at*** utility to perform task scheduling for initial or recurring execution of malicious code.	• As a root user add a crontab command: crontab -e 0 3 * * * /temp/test.sh	Logs Detected: • Add Crontab: ***Yes***
	(Add Crontab) type=SYSCALL msg=audit(1598710015.468:4582): arch=c000003e syscall=59 success=yes exit=0 a0=d28230 a1=d284d0 a2=cf13d0 a3=7ffd60700f20 items=2 ppid=17146 pid=17211 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=3 comm="crontab" exe="/usr/bin/crontab" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="privileged" type=EXECVE msg=audit(1598710015.468:4582): argc=2 a0="crontab" a1="-e"				
	T1136.001	Persistence → Create Account → Local Account	Adversaries may create a local account to maintain access to victim systems.	• As a general user, execute the following command: sudo useradd user2	Logs Detected: • Add User: ***Yes***
	(Add User) type=EXECVE msg=audit(1598710504.259:4735): argc=3 a0="sudo" a1="useradd" a2="user2" type=SYSCALL msg=audit(1598710504.290:4741): arch=c000003e syscall=87 success=yes exit=0 a0=564fb12d70f0 a1=7ffe31452d70 a2=1 a3=2 items=2 ppid=17289 pid=17291 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=3 comm="useradd" exe="/usr/sbin/useradd" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="delete"				

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1543.002	Persistence → Create or Modify System Process →Systemd Service	Adversaries may create or modify systemd services to repeatedly execute malicious payloads as part of persistence.	• As root user: Modify /usr/lib/system/system/vmtoolsd.service to execute /tmp/test.sh	Logs Detected: • Modify system service: ***Yes***
	(Modify System service) type=SYSCALL msg=audit(1598723303.889:5103): arch=c000003e syscall=87 success=yes exit=0 a0=2095560 a1=7ffc80ca3c40 a2=7ffc80ca3c40 a3=7ffc80ca35e0 items=2 ppid=17575 pid=17594 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="vi" exe="/usr/bin/vi" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="delete" type=CWD msg=audit(1598723303.889:5103): cwd="/usr/lib/systemd/system" type=PATH msg=audit(1598723303.889:5103): item=0 name="/usr/lib/systemd/system" inode=50843498 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:systemd_unit_file_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598723303.889:5103): item=1 name=".vmtoolsd.service.swx" inode=51294779 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:systemd_unit_file_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0			
	T1546.004	Persistence → Event Triggered Execution → .bash_profile/.bashrc	Adversaries may establish persistence by executing malicious content triggered by a user's shell. ~/.bash_profile and ~/.bashrc are shell scripts that contain shell commands.	• As root user: Modify <user home>/.bashrc to execute /tmp/test.sh	Logs Detected: • Modify .bashrc: ***Yes***

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Modify .bashrc) type=PROCTITLE msg=audit(1598724245.539:5230): proctitle=7669002E626173687263 type=SYSCALL msg=audit(1598724245.539:5231): arch=c000003e syscall=87 success=yes exit=0 a0=e71280 a1=1 a2=2 a3=1 items=2 ppid=17575 pid=17697 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="vi" exe="/usr/bin/vi" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="delete" type=CWD msg=audit(1598724245.539:5231): cwd="/home/saustin" type=PATH msg=audit(1598724245.539:5231): item=0 name="/home/saustin/" inode=17213864 dev=fd:00 mode=040700 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_home_dir_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598724245.539:5231): item=1 name="/home/saustin/.bashrc.swp" inode=17213871 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:user_home_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598724245.539:5231): proctitle=7669002E626173687263				
	T1546.005	Persistence → Event Triggered Execution → Trap	Adversaries may establish persistence by executing malicious content triggered by an interrupt signal. The trap command allows programs and shells to specify commands that will be executed upon receiving interrupt signals.	• As a root user: Add a command when Exit trap is signaled: trap '/tmp/test.sh; exit' ERR EXIT	Logs Detected: ***No***

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1556.003	Defense Evasion → Modify Authentication Process → Pluggable Authentication Module	Adversaries may modify pluggable authentication modules (PAM) to access user credentials or enable otherwise unwarranted access to accounts.	• Modify pam file /etc/pam.d/system-auth-ac to increase the "retry" limit	Logs Detected: ***Yes*** • Modify PAM file
	(Modify PAM File - /etc/pam.d/system-auth-ac) type=PATH msg=audit(1598725231.327:5373): item=1 name=".system-auth-ac.swpx" inode=843998 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725231.327:5374): item=1 name=".system-auth-ac.swp" inode=843980 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725231.327:5375): item=0 name=".system-auth-ac.swp" inode=843980 dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.567:5379): item=2 name="system-auth-ac" inode=843960 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.567:5379): item=3 name="system-auth-ac~" inode=843960 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.573:5380): item=0 name="system-auth-ac" inode=843998 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.573:5381): item=0 name="system-auth-ac" inode=843998 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.573:5382): item=0 name="system-auth-ac" inode=843998 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.573:5383): item=1 name="system-auth-ac~" inode=843960 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598725240.573:5384): item=1 name="/etc/pam.d/.system-auth-ac.swp" inode=843980 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 objtype=DELETE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0		

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
Credential Access (Discovery)	T1003.008	Credential Access → OS Credential Dumping → /etc/passwd and /etc/shadow	Adversaries may attempt to dump the contents of /etc/passwd and /etc/shadow to enable offline password cracking.	• As a Root user attempt to output contents of /etc/passwd and /etc/shadow to another file	Logs Detected: • Access /etc/passwd: ***No*** • Access /etc/shadow: ***No***
	T1552.003	Credential Access → Unsecured Credentials → Bash History	Adversaries may search the bash command history on compromised systems for insecurely stored credentials.	• Access user's bash history file: cat <user>/.bash_history	Logs Detected: ***No***
	T1201	Discovery → Password Policy Discovery	Adversaries may attempt to access detailed information about the password policy used within an enterprise network.	• Access password policy for root: chage -l root	Logs Detected: • Access password policy: ***Yes***
	(Access Password Policy) type=SYSCALL msg=audit(1598726129.731:5461): arch=c000003e syscall=59 success=yes exit=0 a0=1c718c0 a1=1c88110 a2=1c603d0 a3=7fff4dedf5e0 items=2 ppid=17818 pid=17837 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="chage" exe="/usr/bin/chage" subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 key="privileged" type=EXECVE msg=audit(1598726129.731:5461): argc=3 a0="chage" a1="-l" a2="root" type=CWD msg=audit(1598726129.731:5461): cwd="/root" type=PATH msg=audit(1598726129.731:5461): item=0 name="/bin/chage" inode=50841045 dev=fd:00 mode=0104755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:passwd_exec_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0			

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	T1069.001	Discovery → Permission Group Discovery → Local Groups	Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group.	• As a non-privileged user, execute: groups <user> command	Logs Detected: ***No***
Data Exfiltration	T1570	Lateral Movement → Lateral Tool Transfer	Adversaries may transfer tools or other files between systems in a compromised environment.	• As a non-privileged user, transfer a file to an external computer using SCP: scp <file> <user>@<host>:/file path	Log Detected: ****Yes - IP Tables wasn't configured to log***
	T1052	Exfiltration → Exfiltration Over Physical Medium → Exfiltration over USB	Adversaries may attempt to exfiltrate data over a USB connected physical device.	• Mount USB directory: mount /dev/sda1 /mnt • Attach USB and transfer file	Logs Detected: • Mount USB Directory: Yes • Attach USB and Transfer File: Yes

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Mount USB) type=SYSCALL msg=audit(1598729486.552:5782): arch=c000003e syscall=59 success=yes exit=0 a0=95c9c0 a1=9735a0 a2=94b3d0 a3=7ffc13cb4d60 items=2 ppid=18038 pid=18082 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="mount" exe="/usr/bin/mount" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="privileged" type=EXECVE msg=audit(1598729486.552:5782): argc=3 a0="mount" a1="/dev/sda1" a2="/mnt" type=CWD msg=audit(1598729486.552:5782): cwd="/" type=PATH msg=audit(1598729486.552:5782): item=0 name="/bin/mount" inode=50893333 dev=fd:00 mode=0104755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:mount_exec_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598729486.552:5782): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=81357 dev=fd:00 mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:ld_so_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598729486.552:5782): proctitle=6D6F756E74002F6465762F73646131002F6D6E74 type=SYSCALL msg=audit(1598729486.577:5783): arch=c000003e syscall=165 success=yes exit=0 a0=562455e6f150 a1=562455e6f240 a2=562455e76ed0 a3=c0ed0000 items=2 ppid=18038 pid=18082 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=32 comm="mount" exe="/usr/bin/mount" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="mounts" type=CWD msg=audit(1598729486.577:5783): cwd="/" type=PATH msg=audit(1598729486.577:5783): item=0 name="/mnt" inode=16777425 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:mnt_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1598729486.577:5783): item=1 name="/dev/sda1" inode=10469 dev=00:05 mode=060660 ouid=0 ogid=6 rdev=08:01 obj=system_u:object_r:fixed_disk_device_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PROCTITLE msg=audit(1598729486.577:5783): proctitle=6D6F756E74002F6465762F73646131002F6D6E74				

Attack Scenario	ID	Technique Title	Summary	Linux Commands	Logs
	(Attach USB) type=SYSCALL msg=audit(1602437099.333:7041): arch=c000003e syscall=165 success=yes exit=0 a0=1d21010 a1=1d48a30 a2=1d489c0 a3=6 items=6 ppid=20335 pid=20336 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=tty5 ses=47 comm="mount.exfat" exe="/usr/sbin/mount.exfat-fuse" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="mounts" type=CWD msg=audit(1602437099.333:7041): cwd="/" type=PATH msg=audit(1602437099.333:7041): item=0 name="/mnt" inode=16777425 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:mnt_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1602437099.333:7041): item=1 name="/dev/sdb1" inode=135323 dev=00:05 mode=060660 ouid=0 ogid=6 rdev=08:11 obj=system_u:object_r:fixed_disk_device_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1602437099.333:7041): item=2 name=(null) inode=9 dev=00:06 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:debugfs_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1602437099.333:7041): item=3 name=(null) inode=135393 dev=00:06 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:debugfs_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1602437099.333:7041): item=4 name=(null) inode=135393 dev=00:06 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:debugfs_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 type=PATH msg=audit(1602437099.333:7041): item=5 name=(null) inode=135394 dev=00:06 mode=0100444 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:debugfs_t:s0 objtype=CREATE cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0		

Appendix B - Insider Threat Attack Scenarios - Windows 10 Workstation

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
Privilege Escalation	T1078.001	Initial Access → Default Accounts	Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.	Access Administrator account: • Enumerate local users: net user • Activate Admin account: net user administrator /active:yes • Logon as Admin user	Logs Detected: ***Yes*** • Enumerate local users: Yes (Event ID 4798) • Activate Admin account: Yes (Event ID 4722) (Event ID 4738) • Logon as Admin user: Yes (Event ID 4672)

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	Enumerate Local Users (Event ID 4798) A user's local group membership was enumerated. Subject: Security ID: WINDEV2007EVAL\User Account Name: User Account Domain: WINDEV2007EVAL Logon ID: 0x1FEB9EC User: Security ID: WINDEV2007EVAL\Administrator Account Name: Administrator Account Domain: WINDEV2007EVAL Process Information: Process ID: 0xfcc Process Name: C:\Windows\System32\net1.exe ***Activate Admin Account (Event ID 4722)*** A user account was enabled. Subject: Security ID: WINDEV2007EVAL\User Account Name: User Account Domain: WINDEV2007EVAL Logon ID: 0x1FEB9EC Target Account: Security ID: WINDEV2007EVAL\Administrator Account Name: Administrator Account Domain: WINDEV2007EVAL				

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	Activate Admin Account (Event ID 4738) A user account was changed. Subject: Security ID: WINDEV2007EVAL\User Account Name: User Account Domain: WINDEV2007EVAL Logon ID: 0x1FEB9EC Target Account: Security ID: WINDEV2007EVAL\Administrator Account Name: Administrator Account Domain: WINDEV2007EVAL Changed Attributes: SAM Account Name: Administrator Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: 8/31/2020 5:44:48 PM Account Expires: <never> Primary Group ID: 513 AllowedToDelegateTo: - Old UAC Value: 0x211 New UAC Value: 0x210 User Account Control: Account Enabled User Parameters: <value not set> SID History: - Logon Hours: All				

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	Logon as Admin user (Event ID 4672) Special privileges assigned to new logon. Subject: Security ID: SYSTEM Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege				
	T1543.003	Privilege Escalation → Event Triggered Execution → Screensaver	Adversaries may establish persistence by executing malicious content triggered by user inactivity.	• Start regedit command • Access the HKCU\Control Panel\Desktop\ Key • Modify scrnsave.exe to c:\tmp\test.exe	Logs Detected: No

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
Maintain Persistence	T1098.004	Persistence → BIT Jobs	Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM).	• Execute a File Transfer using BITS Transfer: Start-BitsTransfer -source <source file> -Destination <Destination> -Transfertype Download	Logs Detected: ***Yes*** • Execute a File Transfer using BITS - Yes, Event ID 7040
	Execute a File Transfer using BITS (Event ID 7040) The start type of the Background Intelligent Transfer Service was changed from demand start to auto start.				

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	T1053.001	Persistence -> Boot or Logon Autostart Execution -> Registry Run Keys/Startup Folder	Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.	Add Script to Run Registry key: Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Logs Detected: • Add Script to Run Registry Key - ***No***
Credential Access	TI087.001	Discovery → Local Account	Adversaries may attempt to get a listing of local system accounts. This information can help adversaries determine which local accounts exist on a system to aid in follow-on behavior.	• Attempt to get local user information by typing: ***net user*** and ***net localgroup***	Logs Detected: • net user: Yes - Event ID 4688 (Process Creation) • net localgroup: Yes - Event ID 4688 (Process Creation)

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	T1135	Discovery → Network Share Discovery	Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.	• Enumerate shared drives: net view \remotesystem and net share	Logs Detected: Yes • net share: Event ID 4688 (Process Creation) • net view \remotesystem: Event ID 4688 (Process Creation)
	T1201	Discovery → Password Policy Discovery	Adversaries may attempt to access detailed information about the password policy used within an enterprise network.	• Access password policy: net accounts	Logs Detected: ***Yes*** • net accounts: Event ID 4688 (Process Creation)
	T1069.001	Discovery → Permission Group Discovery → Local Groups	Adversaries may attempt to find local system groups and permission settings. The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group.	• Execute command to see local group: net localgroup	Logs Detected: ***Yes*** • net localgroup: Event ID 4688 (Process Creation)

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
	Net User Command (Event ID: 4688) A new process has been created. Creator Subject: Security ID: WINDEV2007EVAL\User Account Name: User Account Domain: WINDEV2007EVAL Logon ID: 0x36474B0 Target Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Process Information: New Process ID: 0x1c40 New Process Name: C:\Windows\System32\net.exe Token Elevation Type: %%1937 Mandatory Label: Mandatory Label\High Mandatory Level Creator Process ID: 0xd84 Creator Process Name: C:\Windows\System32\cmd.exe Process Command Line:				
Exfiltration	T1052	Exfiltration → Exfiltration Over Physical Medium → Exfiltration over USB	Adversaries may attempt to exfiltrate data over a USB connected physical device.	• Connect USB to Computer	Logs Detected: Yes • Event ID: 6416 A new external device was recognized by the system

Attack Scenario	ID	Technique Title	Summary	Windows Commands	Logs
(Event ID: 6416) A new external device was recognized by the system. Subject: Security ID: SYSTEM Account Name: WINDEV2007EVAL$ Account Domain: WORKGROUP Logon ID: 0x3E7 Device ID: SWD\WPDBUSENUM_??_USBSTOR#Disk&Ven_Generic&Prod_Mass_Storage&Rev_1100#062419-10390&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b} Device Name: SEC511 Class ID: {eec5ad98-8080-425f-922a-dabf3de3f69a} Class Name: WPD Vendor IDs: - Compatible IDs: wpdbusenum\fs SWD\Generic					

Last Updated: November 26th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Essentials Australia 2021	**Melbourne, AU**	**Feb 15, 2021 - Feb 20, 2021**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**