CHAPTER 3

Remote Triage

Chapter Overview

01

Finding Evil

Connections, processes, services, accounts, files, autostarts, and WMI

02

Triage Toolkit

Sysinternals, live query commands, and response methodology

03

Guarding Your Credentials

Logon types, credential attacks, and safe IR access methods

Finding Evil

Live triage without destroying evidence

Rogue Connections

netstat -naob: lists all connections with the owning executable (requires admin)

Get-NetTCPConnection: PowerShell equivalent — easily filterable and scriptable

ESTABLISHED state to unknown external IPs: primary C2 indicator

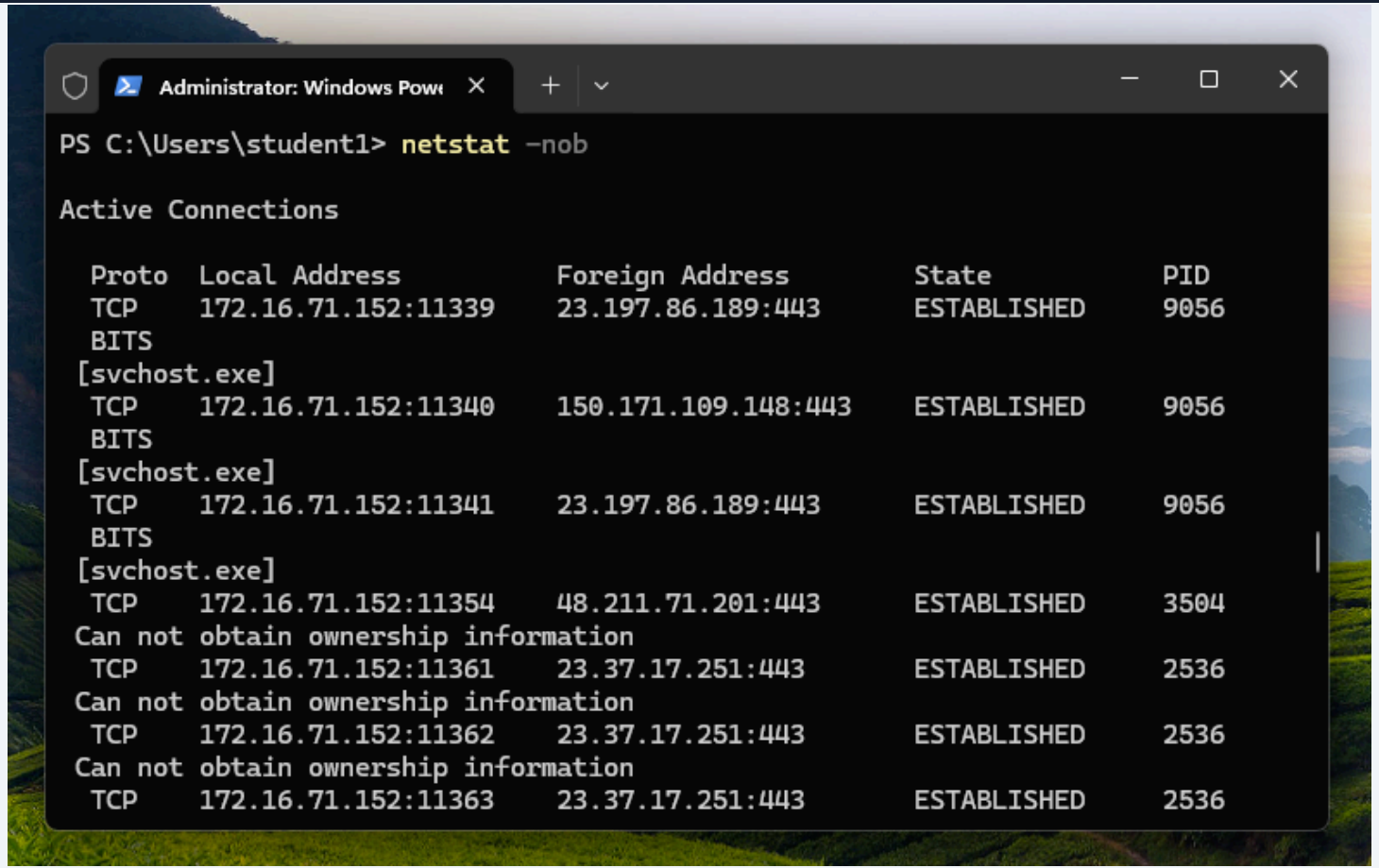
LISTENING on non-standard ports: backdoor waiting for attacker callback

TIME_WAIT / CLOSE_WAIT accumulation: may indicate automated C2 beaconing

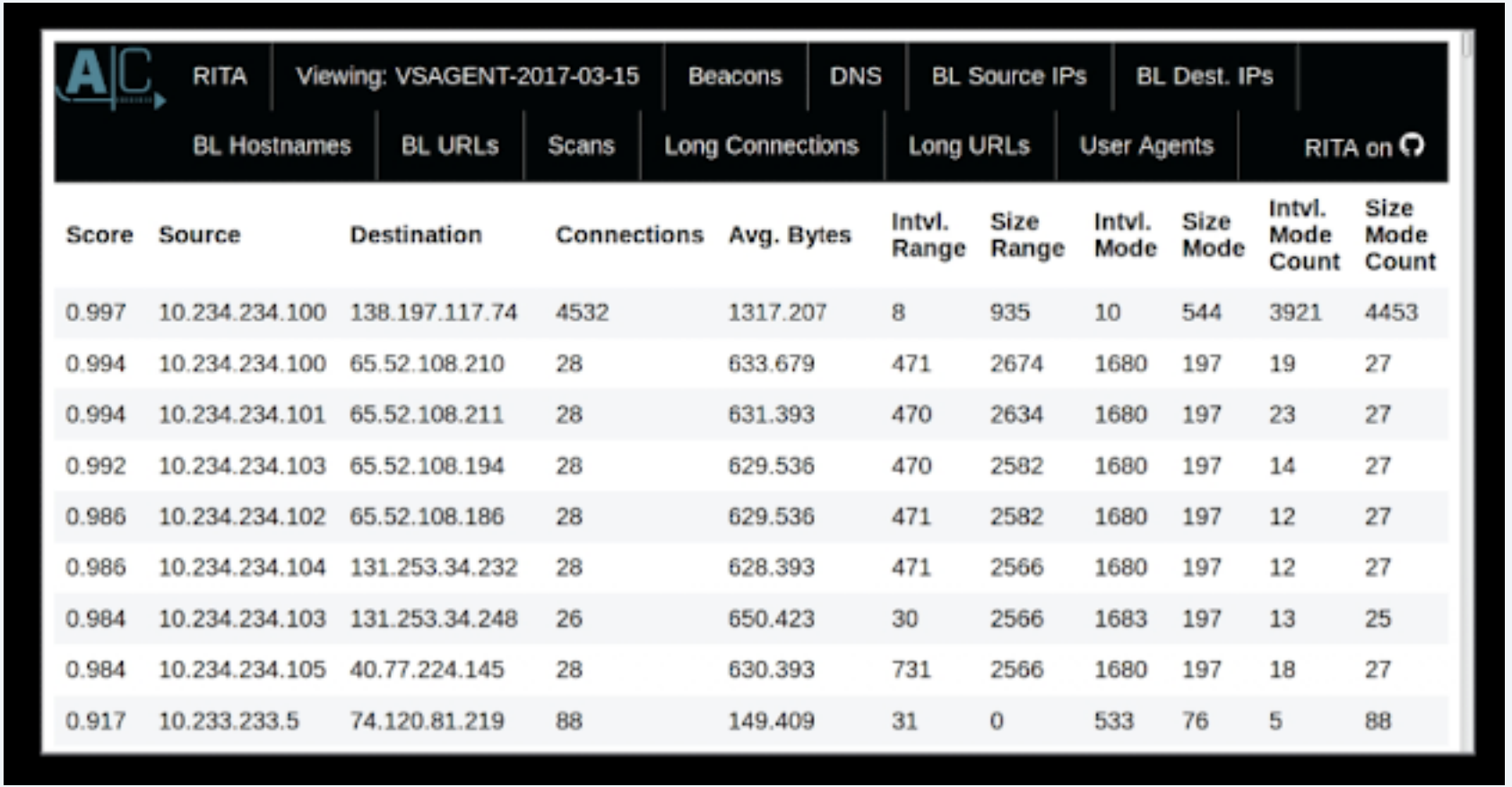
Cross-reference PID from netstat against running process list for full picture

TCPView (Sysinternals): GUI view of connections with real-time updates

Netstat


Administrator: Windows Powe
PS C:\Users\student1> netstat -nob
Active Connections
Proto Local Address Foreign Address State PID
TCP 172.16.71.152:11339 23.197.86.189:443 ESTABLISHED 9056
BITS
[svchost.exe]
TCP 172.16.71.152:11340 150.171.109.148:443 ESTABLISHED 9056
BITS
[svchost.exe]
TCP 172.16.71.152:11341 23.197.86.189:443 ESTABLISHED 9056
BITS
[svchost.exe]
TCP 172.16.71.152:11354 48.211.71.201:443 ESTABLISHED 3504
Can not obtain ownership information
TCP 172.16.71.152:11361 23.37.17.251:443 ESTABLISHED 2536
Can not obtain ownership information
TCP 172.16.71.152:11362 23.37.17.251:443 ESTABLISHED 2536
Can not obtain ownership information
TCP 172.16.71.152:11363 23.37.17.251:443 ESTABLISHED 2536

RITA (Real Intelligence Threat Analytics)



Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mode	Intvl. Mode Count	Size Mode Count
0.997	10.234.234.100	138.197.117.74	4532	1317.207	8	935	10	544	3921	4453
0.994	10.234.234.100	65.52.108.210	28	633.679	471	2674	1680	197	19	27
0.994	10.234.234.101	65.52.108.211	28	631.393	470	2634	1680	197	23	27
0.992	10.234.234.103	65.52.108.194	28	629.536	470	2582	1680	197	14	27
0.986	10.234.234.102	65.52.108.186	28	629.536	471	2582	1680	197	12	27
0.986	10.234.234.104	131.253.34.232	28	628.393	471	2566	1680	197	12	27
0.984	10.234.234.103	131.253.34.248	26	650.423	30	2566	1683	197	13	25
0.984	10.234.234.105	40.77.224.145	28	630.393	731	2566	1680	197	18	27
0.917	10.233.233.5	74.120.81.219	88	149.409	31	0	533	76	5	88

Table 3.1: Common lateral movement connection ports

PORT	DESCRIPTION
TCP 22	Secure Shell (SSH)
TCP 135	RPC/DCOM (an additional, dynamic high number port may also be involved)
TCP 445	Server Message Block (SMB)
TCP 3389	Remote Desktop Protocol
TCP 5985/5986	WinRM and PowerShell Remoting

Unusual Processes

Process path: malware commonly runs from %TEMP%, %APPDATA%, C:\ProgramData, or C:\Users

Process name masquerading: svchost.exe outside C:\Windows\System32 is malware

Parent-child anomalies: Word or Excel spawning cmd.exe, PowerShell, or wscript.exe

Process hollowing: legitimate image (e.g., svchost.exe) with injected malicious code

Unsigned or poorly-signed executables in unusual locations — check with Get-FileHash

High CPU/memory processes with no obvious function — may indicate crypto mining

Process Explorer (Sysinternals): shows full path, VirusTotal score, parent-child tree

Unusual Services, Ports & Accounts

Services & Ports

Services with binary paths in user-writable locations

Services with Display Name / Description left blank

Services running as LocalSystem with no clear purpose

sc query type=all state=all to list every service

HTTP/HTTPS servers (port 80/443) run by non-IIS processes

High-numbered ports (>49152) in LISTENING state

Rogue Accounts

net localgroup administrators: unexpected members

Accounts created recently with never-expiring passwords

Accounts with $ suffix added to Administrators group

Domain accounts granted local admin on endpoints

Event ID 4720 (account created) + 4732 (added to group) pair

Unusual Files & Autostart Locations

Unusual Files

Recently modified DLLs or EXEs in C:\Windows\System32

Executables in %TEMP%, %APPDATA%\Roaming, or Public\Downloads

Double-extension tricks: invoice.pdf.exe (icon shows PDF)

Get-FileHash: compute SHA256, compare to VirusTotal/known-good

dir /tc /od lists files in creation-time order (oldest first)

Autostart Locations

HKLM/ HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run(Once)

Scheduled tasks: schtasks /query /fo LIST /v | findstr /i "task\|run"

Services (HKLM\SYSTEM\CurrentControlSet\Services)

Startup folders: shell:startup, shell:common startup

Browser extensions, DLL hijacking in application folders

WMI Persistence — Advanced Autostart

WMI event subscriptions survive reboots and are invisible to Autoruns by default

Three-part structure: Event Filter + Event Consumer + Filter-to-Consumer Binding

Event Filter: defines WHEN to trigger (e.g., on process start, logon, or timer)

Event Consumer: defines WHAT to run (CommandLineEventConsumer, ActiveScriptEventConsumer)

Detection: wmic /namespace:\\root\subscription PATH __EventFilter get Name,Query

Detection: wmic /namespace:\\root\subscription PATH CommandLineEventConsumer get Name,CommandLineTemplate

Autoruns.exe (Sysinternals): WMI tab shows all subscriptions with VirusTotal lookup

Triage Toolkit

The responder's essential tools

Sysinternals Suite for Live Triage

Process Explorer: full process tree, DLL view, VirusTotal integration, strings

TCPView: live view of TCP/UDP connections mapped to processes

Autoruns: every autostart location — Run keys, tasks, services, WMI, drivers

Process Monitor: real-time file, registry, and network activity per process

PsExec: run commands on remote systems over SMB (also used by attackers — log it)

Handle: find which processes have a file or registry key open

Sigcheck: verify digital signatures and check hashes against VirusTotal

Live Response Methodology

Before touching the system: note time, document your presence in the case log

Step 1 — Connections: netstat -naob > c:\ir\connections.txt

Step 2 — Processes: tasklist /v /fo csv > c:\ir\processes.txt

Step 3 — Services: sc query type= all state= all > c:\ir\services.txt

Step 4 — Accounts: net localgroup administrators > c:\ir\admins.txt

Step 5 — Autoruns: autorunsc -a * -c > c:\ir\autoruns.csv

Step 6 — Scheduled tasks: schtasks /query /fo CSV /v > c:\ir\tasks.csv

Always write to removable media — never to the suspect system's local disk

Guarding Your Credentials

Don't become the attacker's next pivot

Understanding Interactive Logon Types

Type 2 — Interactive: keyboard logon, credentials cached in LSASS memory

Type 3 — Network: SMB/WMI access, credentials NOT cached on remote system

Type 4 — Batch: scheduled tasks, credentials may be stored as LSA secret

Type 5 — Service: service account logon, password stored as LSA secret

Type 7 — Unlock: workstation unlock — same caching risk as Type 2

Type 10 — Remote Interactive (RDP): credentials cached unless Restricted Admin Mode

IR rule: use Type 3 (network) logons for remote access; avoid Type 2 and 10

Credential Attacks to Recognize During Triage

Pass-the-Hash: Event 4624 Type 3 with NTLM from unexpected source IP

Pass-the-Ticket: Kerberos logon (4768/4769) from wrong workstation

Overpass-the-Hash: 4768 (TGT request) from a machine that never contacts that DC

Credential dumping: lsass.exe accessed by non-system process (4663 on lsass)

LSASS memory access: Sysmon Event ID 10 (ProcessAccess) targeting lsass.exe

Mimikatz artifacts: strings 'sekurlsa', 'privilege::debug' in PowerShell logs (4104)

Temporary admin accounts: 4720 + 4732 pair created and deleted within hours

Kerberoasting — Detection & Response

Kerberoasting: any domain user requests TGS for a service account SPN

TGS is encrypted with the service account's NTLM hash — taken offline for cracking

No admin rights needed — low-privilege attacker can perform this attack

Detection: Event 4769 (Kerberos Service Ticket Request) with EncryptionType 0x17 (RC4)

RC4 is weaker and faster to crack — legitimate Kerberos uses AES (0x12/0x11)

Baseline: identify all accounts with SPNs — wmic /domain service where 'StartMode!='Disabled''

Mitigation: use Group Managed Service Accounts (gMSA) with 240-char random passwords

Also look for: bulk 4769 events from a single source in a short window

RDP Restricted Admin Mode & Remote Credential Guard

Restricted Admin Mode

Allows login through RDP without passing the plaintext password to the remote system

Enabled on the RDP server: reg add HKLM\System\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d 0

Connect from client: mstsc /restrictedAdmin

Result: admin rights on remote host but credentials NOT sent to remote LSASS

Downside: Pass-the-Hash can be used to connect (double-edged)

Best for: connecting to potentially compromised systems

Remote Credential Guard

Requires: Windows 10/Server 2016+, Kerberos available, HVCI/Credential Guard on client

Connect: mstsc /remoteGuard

Credentials stay on local machine — Kerberos tickets proxied, never land on remote

Prevents PtH abuse (unlike Restricted Admin Mode)

Best for: permanent operational use on known-clean systems

Conclusion

Systematic triage catches attackers — skip a category and miss the intrusion

WMI subscriptions are invisible to casual inspection; always check them explicitly

Know your logon types: Type 10 (RDP) caches credentials; Type 3 (network) does not

Kerberoasting leaves a clear Event 4769 fingerprint — look for RC4 encryption type

Use Restricted Admin Mode or Remote Credential Guard to protect your IR accounts

Document every command you run — chain of custody starts at first response

Knowledge Check