The "First Responder" Shell Cheatsheet

FIRST 5 MINUTES: TRIAGE & ISOLATE

QUICK SYSTEM SNAPSHOT

LINUX

```
whoami; id; hostname; uptime
w | head -15 # Active users/sessions
last -n 10 # Recent logins
ps aux | wc -l # Running processes count
netstat -tlnp | grep LISTEN # Listening ports
```

WINDOWS (PowerShell)

```
whoami; hostname; systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
quser # Active sessions
qwinsta # Console sessions
Get-Process | Measure # Process count
netstat -ano | findstr LISTENING # Listening ports
```

IMMEDIATE ISOLATION

LINUX - Disconnect network (KEEP SSH)

```
ip link set eth0 down # Replace eth0 with active interface
iptables -P INPUT DROP; iptables -P OUTPUT DROP; iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT # Allow localhost
iptables -A OUTPUT -o lo -j ACCEPT # Allow localhost
```

WINDOWS - Disable network adapters

```
Disable-NetAdapter -Name "Ethernet*" -Confirm:$false
netsh advfirewall set allprofiles state on # Enable Windows Firewall
New-NetFirewallRule -DisplayName "BlockAllInbound" -Direction Inbound -Action Block
```

MINUTES 5-15: EVIDENCE COLLECTION

MEMORY & PROCESS DUMP

LINUX

```
ps aux --forest > /tmp/process_tree.txt
cat /proc/[PID]/cmdline # For suspicious PID
volatility3 -f memory.dump linux.pslist # Memory forensics
```

WINDOWS

```
procdump -accepteula -ma [PID] C:\temp\dumps
tasklist /svc > C:\temp\processes.txt
Get-WmiObject Win32_Process | Select Name,ProcessId,ParentProcessId | Export-Csv
processes.csv
```

NETWORK INVESTIGATION

LINUX - Active connections + C2 check

```
netstat -tlnp | grep ESTABLISHED
ss -tulp | grep :[suspicious_port]
lsof -i :[port] -iTCP -iUDP
curl -s ipinfo.io/[suspicious_ip] | jq # IP geolocation
```

WINDOWS

```
netstat -ano | findstr ESTABLISHED
Get-NetTCPConnection | Where-Object {$_.State -eq "Established"} | Select
Local*,Remote*,OwningProcess
Get-NetUDPEndpoint | Select Local*,OwningProcess
Resolve-DnsName suspicious.domain.com # DNS lookup
```


DISK & TIMELINE

LINUX

```
df -h; mount | grep noexec # Mounted filesystems
ls -la /tmp /var/tmp /dev/shm # Common drop locations
find / -type f -newer /proc/version -ls 2>/dev/null | head -20 # Recent files
ls -la ~/*/.ssh/ # Check authorized_keys
```

WINDOWS

```
Get-PSDrive # Mounted drives
Get-ChildItem C:\Windows\Temp,C:\Users*\AppData\Local\Temp -Recurse | Where-Object
{$_.CreationTime -gt (Get-Date).AddHours(-1)}
Get-ChildItem "C:\Users*\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup" -Recurse
Get-WinEvent -FilterHashtable @{LogName='Security';ID=4624,4625,4672} -MaxEvents 50 |
Select TimeCreated,Id,Message
```

MINUTES 15-30: PERSISTENCE & FORENSICS

PERSISTENCE CHECK

LINUX - Cron, Services, Startup

```
crontab -l; cat /etc/crontab; ls /etc/cron.*
systemctl list-unit-files --state=enabled | grep -v static
ls -la /etc/systemd/system/*.service /etc/init.d/
cat /etc/rc.local; ls ~/.bashrc ~/.profile /etc/profile
```

WINDOWS - Registry & Scheduled Tasks

```
schtasks /query /fo LIST /v | findstr /i "taskname"
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Get-CimInstance Win32_StartupCommand | Select Name,Command,Location,User
```

MALWARE HUNTING

LINUX

```
rkhunter --check --skip-keypress
chkrootkit | grep INFECTED
ldd /usr/bin/* 2>/dev/null | grep "not found"
strings /usr/bin/suspicious_binary | grep -i "eval|base64|curl|wget"
```

WINDOWS

```
Get-MpComputerStatus # Windows Defender status
Get-MpThreatDetection # Recent detections
sigcheck -u -e C:\Windows\System32\ # Unsigned binaries
Get-AuthenticodeSignature -FilePath suspicious.exe | fl
```

LOGGING & ALERTING

SECURE DATA EXFILTRATION

LINUX - Compress + Base64 for secure transfer

```
tar czf /tmp/incident_evidence.tar.gz /tmp/*.txt /var/log/auth.log
base64 /tmp/incident_evidence.tar.gz > /tmp/evidence.b64
scp /tmp/evidence.b64 analyst@secure-server:/incident/(hostname)−(date +%Y%m%d-%H%M).b64
```

WINDOWS - PowerShell to secure server

```
Compress-Archive -Path C:\temp* -DestinationPath C:\temp\evidence.zip
$cred = Get-Credential; Invoke-Command -ComputerName secure-server -Credential
\temp\evidence.zip C:\incidents}
```

ALERT FORMAT

```
ALERT: [CRITICAL/HIGH/MEDIUM] - [Hostname] - [Timestamp]
IP: [suspicious_ip] | PORT: [port] | USER: [username]
IOC: [hash/domain/filename]
IMPACT: [description]
CONTAINMENT: [actions taken]
NEXT: [escalation plan]
EVIDENCE: [attached files]
ANALYST: [your_name]
```


ONE-LINERS EVERY ANALYST MUST KNOW

Kill suspicious process + children (Linux)

```
pkill -f suspicious_binary; ps aux | grep suspicious | awk '{print $2}' | xargs kill -9
```

Block IP everywhere (Linux)

```
iptables -I INPUT -s BAD_IP -j DROP; iptables -I OUTPUT -d BAD_IP -j DROP
```

Windows - Kill process tree

```
Get-Process suspicious | Stop-Process -Force; wmic process where "name='suspicious.exe'" delete
```

Check for RDP brute force (Windows)

```
Get-WinEvent Security | where {_.Message -match "33809"} | group SourceAddress | sort Count -Descending
```

Recent logins last 24h (Linux)

```
last -F | awk '$6=="today" || $7=="today"' | head -20
```

DECISION MATRIX: ESCALATE WHEN...

CRITERIA	ESCALATE TO T2
Domain/IP in blocklist	IMMEDIATE
Lateral movement detected	IMMEDIATE
Privilege escalation	IMMEDIATE
Data exfiltration (>1MB)	IMMEDIATE
Ransomware indicators	IMMEDIATE
>10 failed logins/min	T2 in 15min
Unknown listening port	T2 in 30min
Suspicious process (ps aux)	T2 in 30min

CONTAINMENT CHECKLIST: DID YOU...

- [ ] Take screenshot of screen
- [ ] Document running processes/connections
- [ ] Check persistence mechanisms
- [ ] Isolate network (but keep evidence path)
- [ ] Hash suspicious files (sha256sum / sha256.exe)
- [ ] Document timeline of events
- [ ] Notify chain of command
- [ ] Secure evidence chain of custody

KEY PRINCIPLES FOR FIRST RESPONDERS

1. Preserve Evidence
Never run destructive commands without documenting first. Evidence integrity is critical.

2. Isolate Carefully
Network isolation prevents spread but document connection details before cutting off.

3. Document Everything
Timestamps, commands run, outputs generated. This is your incident report.

4. Know Your Tools
Each command has specific output. Practice before you need it.

5. Escalate Early
When in doubt, escalate to T2/T3. False positives are better than missed breaches.

RELATED RESOURCES

- **MITRE ATT&CK Framework:** Map findings to attack techniques
- **NIST Incident Response:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- **Incident Handler's Handbook:** https://www.sans.org/white-papers/
- **Linux Forensics:** https://linux-forensics.sans.org/
- **Windows Forensics:** Reference Windows Event Log IDs for investigation

CRITICAL REMINDERS

DO:

- Preserve original evidence
- Document all commands
- Isolate before spreading
- Hash files for integrity
- Escalate when uncertain
- Follow your organization's incident response plan

DON'T:

- Modify files before hashing

- Disconnect evidence paths
- Run untrusted tools
- Reboot without capturing memory
- Delete logs
- Work alone on critical incidents

PRINT THIS. LAMINATE IT. KEEP IT NEXT TO YOUR TERMINAL.

Your fastest response in the first 30 minutes can mean the difference between contained incident and full breach.

Good luck, First Responder. You've got this.