StealthCup 2025: Scoring System & Optimization Cheatsheet

This cheatsheet provides a detailed breakdown of the StealthCup scoring system and strategies to optimize your score. Since the team with the **lowest score wins**, understanding how to minimize alerts is crucial for success.

1. Scoring System Breakdown

The StealthCup scoring system is based on alerts triggered during your attack operations.

Core Scoring Formula

```
Final Score = [Wazuh Alerts + Suricata Alerts] × Reset Multiplier
```

Where:

- **Wazuh Alerts** = (Critical × 50) + (High × 3) + (Medium × 1) + (Low × 0.05)
- **Suricata Alerts** = (Critical × 500) + (High × 30) + (Medium × 20) + (Low × 10)
- **Reset Multiplier** = 1 + (0.1 × Number of Resets)

Alert Severity Weights

Alert Source	Critical	High	Medium	Low
Wazuh (HIDS)	50	3	1	0.05
Suricata (NIDS)	500	30	20	10

Key Insights:

- Suricata alerts are weighted **much more heavily** than Wazuh alerts
- Critical alerts have disproportionately high weights
- A single Suricata Critical alert (500 points) is equivalent to 10 Wazuh Critical alerts (50 points each)

Reset Multiplier

Each time you reset the infrastructure, a multiplier is applied to your subsequent score:

- First attempt (0 resets): 1.0× multiplier
- Second attempt (1 reset): 1.1× multiplier
- Third attempt (2 resets): 1.2× multiplier
- And so on...

Important: Resets cause 10-20 minute downtime, and the multiplier increases the difficulty of achieving a low score on subsequent attempts.

2. Score Calculation Examples

Example 1: Low-Medium Alert Volume

```
Wazuh: 0 Critical, 2 High, 15 Medium, 100 Low
Suricata: 0 Critical, 0 High, 1 Medium, 2 Low
Resets: 0

Wazuh Score = (0 × 50) + (2 × 3) + (15 × 1) + (100 × 0.05) = 6 + 15 + 5 = 26
Suricata Score = (0 × 500) + (0 × 30) + (1 × 20) + (2 × 10) = 0 + 0 + 20 + 20 = 40
Reset Multiplier = 1.0

Final Score = (26 + 40) × 1.0 = 66
```

Example 2: High Alert Volume

```
Wazuh: 2 Critical, 10 High, 934 Medium, 5423 Low
Suricata: 0 Critical, 0 High, 2 Medium, 0 Low
Resets: 2

Wazuh Score = (2 × 50) + (10 × 3) + (934 × 1) + (5423 × 0.05) = 100 + 30 + 934 +
271.15 = 1335.15
Suricata Score = (0 × 500) + (0 × 30) + (2 × 20) + (0 × 10) = 0 + 0 + 40 + 0 = 40
Reset Multiplier = 1.2

Final Score = (1335.15 + 40) × 1.2 = 1650.18
```

Example 3: Critical Alert Impact

```
Wazuh: 0 Critical, 0 High, 100 Medium, 200 Low
Suricata: 1 Critical, 0 High, 0 Medium, 0 Low
Resets: 0

Wazuh Score = (0 × 50) + (0 × 3) + (100 × 1) + (200 × 0.05) = 0 + 0 + 100 + 10 =
110
Suricata Score = (1 × 500) + (0 × 30) + (0 × 20) + (0 × 10) = 500 + 0 + 0 + 0 =
500
Reset Multiplier = 1.0

Final Score = (110 + 500) × 1.0 = 610
```

Key Insight: A single Suricata Critical alert dramatically increases your score, more than hundreds of medium/low alerts combined.

3. Alert Source Analysis

Understanding what triggers alerts from each detection system helps minimize them.

Wazuh (HIDS) Alert Sources

Wazuh primarily monitors host-based activities:

Alert Type	Severity	Common Triggers	Avoidance Strategy
File Integrity	Medium-High	Creating/modifying system files	Use memory-only techniques, avoid writing to monitored directories
Command Execution	Medium-High	Running suspicious commands	Use command obfuscation, living off the land techniques
Authentication	Medium	Failed logins, credential brute forcing	Use valid credentials, limit authentication attempts
Privilege Escalation	Critical	UAC bypass, token manipulation	Use minimal privilege escalation, legitimate admin channels
Process Creation	Medium	Creating suspicious processes	Use legitimate processes, avoid known malicious process names
Registry Changes	Medium	Modifying startup keys, services	Limit registry modifications, use temporary changes
Script Execution	Medium-High	PowerShell, VBScript, batch files	Use script obfuscation, avoid suspicious parameters

Suricata (NIDS) Alert Sources

Suricata primarily monitors network-based activities:

Alert Type	Severity	Common Triggers	Avoidance Strategy
Exploit Attempts	Critical	Known exploit signatures	Modify exploits to avoid signatures, use custom exploits
Protocol Violations	High	Non-standard protocol usage	Ensure protocol compliance, avoid protocol abuse
Scanning Activity	Medium-High	Port scanning, network enumeration	Use slow, targeted scanning, passive reconnaissance
Malware Traffic	Critical	Known C2 patterns, malware signatures	Use custom C2 channels, encrypt/obfuscate traffic
Data Exfiltration	High	Large outbound transfers	Limit transfer size, use covert channels
Suspicious Connections	Medium	Connections to unusual ports/hosts	Use common ports (80, 443), legitimate connection patterns
DoS Patterns	High	High-volume traffic	Avoid rapid connection attempts, rate limit activities

4. Score Optimization Strategies

Pre-Attack Planning

- **Reconnaissance Strategy**: Prioritize passive reconnaissance over active scanning.
    - **Example**: Analyze network traffic captured from your initial foothold before active scanning.
    - **Potential Alert Savings**: 5-10 Medium Suricata alerts (100-200 points)
- **Attack Path Planning**: Map multiple attack paths and prioritize the stealthiest.
    - **Example**: Compare direct Domain Admin compromise vs. gradual privilege escalation.
    - **Potential Alert Savings**: 1-2 Critical alerts (50-1000 points)

During Attack Execution

- **Incremental Approach**: Start with minimal, low-noise techniques before escalating.
    - **Example**: Try known credentials before attempting password spraying.
    - **Potential Alert Savings**: 3-5 High alerts (9-150 points)
- **Cooling Periods**: Space out high-risk activities to avoid correlation alerts.
    - **Example**: Wait 30-60 minutes between major attack phases.
    - **Potential Alert Savings**: 2-3 High correlation alerts (6-90 points)
- **Technique Selection**: Choose techniques based on their alert profile.
    - **Example**: Use WinRM (administrative tool) instead of PsExec (often flagged).
    - **Potential Alert Savings**: 1-2 High alerts per lateral movement (3-60 points)

Reset Strategy Optimization

- **First Attempt Strategy**: Focus on reconnaissance and minimal interaction.
    - **Goal**: Understand the environment without triggering many alerts.
    - **Benefit**: No reset multiplier applied (1.0×).
- **When to Reset**:
    - If you've triggered Critical Suricata alerts (500+ points each)
    - If you've triggered multiple High alerts early in your attack
    - If you've discovered a much stealthier attack path
- **When Not to Reset**:
    - If you've only triggered Low/Medium alerts
    - If you're close to achieving an objective
    - If you've already reset multiple times (high multiplier)
- **Timing Considerations**:
    - Resets take 10-20 minutes

- Last reset should be at least 60 minutes before the end of the event
- Resets happen in 15-minute batches

5. Alert-to-Action Mapping

This section maps common actions to their likely alert levels to help you make informed decisions.

Reconnaissance Actions

Action	Likely Wazuh Alert	Likely Suricata Alert	Total Score Impact
Passive network sniffing	None	None	0
Slow, targeted port scan	None	Low (1-2)	10-20
Aggressive port scan	None	Medium-High (2-3)	40-90
Service enumeration (banner grabbing)	None	Low (1-2)	10-20
Vulnerability scanning	None	High-Critical (1-2)	30-500+

Active Directory Actions

Action	Likely Wazuh Alert	Likely Suricata Alert	Total Score Impact
LDAP queries (authenticated)	Low (1-2)	None	0.1-0.1
PowerView enumeration	Medium (2-3)	None	2-3
BloodHound collection	Medium-High (3-5)	Low (1)	3-15 + 10
Kerberoasting (small scale)	Medium (1-2)	Low (1)	1-2 + 10
DCSync attack	High-Critical (1)	Medium (1)	3-50 + 20
Creating domain user	Medium (1)	None	1
Adding user to Domain Admins	High (1)	None	3

OT/SCADA Actions

Action	Likely Wazuh Alert	Likely Suricata Alert	Total Score Impact
Modbus TCP reading	None	Low (1)	10
HMI web interface access	Low (1)	None	0.05
PLC parameter reading	None	Low-Medium (1)	10-20
PLC parameter writing	None	Medium (1-2)	20-40
Safety system manipulation	Medium (1)	High (1)	1 + 30
Triggering PORV flag	Medium-High (1-2)	Medium-High (1-2)	1-6 + 20-60

Lateral Movement Actions

Action	Likely Wazuh Alert	Likely Suricata Alert	Total Score Impact
WinRM (authenticated)	Low-Medium (1)	Low (1)	0.05-1 + 10
SSH (authenticated)	Low (1)	Low (1)	0.05 + 10
SMB file transfer	Low (1)	Low-Medium (1)	0.05 + 10-20
PsExec	Medium-High (1)	Medium (1)	1-3 + 20
Pass-the-Hash	High (1)	Medium (1)	3 + 20
WMI execution	Medium (1)	Low (1)	1 + 10

6. Write-up Optimization

The rules state that scores must be validated with a write-up explaining how you bypassed the IDS. Optimize your write-up for maximum score validation:

- **Document Evasion Techniques**: Clearly explain which evasion techniques you used.
- **Highlight Stealth Measures**: Emphasize deliberate steps taken to minimize alerts.
- **Explain Tool Modifications**: If you modified tools to avoid detection, document how.
- **Timing Strategies**: Note if you used timing to avoid correlation alerts.
- **Command Obfuscation**: Detail any obfuscation techniques used.

7. Score Tracking and Analysis

During the competition, you'll have access to a dashboard showing triggered alerts. Use this information strategically:

- **Real-time Adjustment**: Modify techniques based on which alerts you're triggering.
- **Alert Pattern Analysis**: Look for patterns in what actions trigger which alerts.
- **Comparative Analysis**: If working in teams, compare different approaches and their alert profiles.

8. Decision Framework for Score Optimization

Use this decision framework when planning actions:

1. **Is passive reconnaissance sufficient?**
    - If yes: Use passive techniques
    - If no: Proceed to #2
2. **Is the action necessary for the objective?**
    - If no: Skip it
    - If yes: Proceed to #3
3. **Are there multiple ways to accomplish this action?**
    - If yes: Compare alert profiles and choose the stealthiest

- If no: Proceed to #4

4. **Can the action be modified to reduce alerts?**
    - If yes: Apply obfuscation, timing adjustments, etc.
    - If no: Proceed to #5

5. **Is the alert cost worth the progress?**
    - If yes: Execute with caution
    - If no: Find an alternative approach

9. Score Optimization Checklist

Use this checklist before executing any significant action:

- ☐ Have I exhausted passive information gathering?
- ☐ Is this the stealthiest way to accomplish this goal?
- ☐ Have I applied appropriate obfuscation techniques?
- ☐ Am I executing this at an optimal time (business hours, spaced from other actions)?
- ☐ Have I tested/practiced this technique to ensure minimal mistakes?
- ☐ Do I have a fallback plan if this triggers unexpected alerts?
- ☐ Is the potential alert cost worth the progress toward the objective?

Remember: The team with the lowest score wins, not necessarily the team that completes objectives fastest. Patience and stealth are more valuable than speed.