

Nama Team: kopral satu kopral dua minum kopi
Kategori Lomba: Incident response



Case #01: Defender Cache Maintenance

Case #02: Storage Optimization

Task1:

Task2:

Kami menemukan "Task to run" pada file "ScheduledTasks.txt", saat memperhatikan isi file dengan command: `cat ScheduledTasks.txt | grep 'Task To Run'`

Dengan banyaknya line yang memberikan hasil Task To Run, kami coba satu-per-satu, dan menemukan bahwa "%windir%\system32\defrag.exe -c -h -o -\$" merupakan Task to run yang benar:

```
Task To Run: COM handler
Task To Run: %windir%\system32\defrag.exe -c -h -o -$
Task To Run: %windir%\system32\devicecensus.exe SystemCxt
Task To Run: %windir%\system32\devicecensus.exe SystemCxt
Task To Run: %windir%\system32\devicecensus.exe UserCxt
```

Task3:

Kami menemukan "Last Result" pada file "ScheduledTasks.txt", saat memperhatikan isi file dengan command: `cat ScheduledTasks.txt | grep 'Last Result'`

Ditemukan bahwa rata-rata line yang memberikan Final Result, berupa "267011", karena lebih dominan muncul:

```
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
Last Result: 267011
```

Task4:

Kami menemukan "Power Management" pada file "ScheduledTasks.txt", saat memperhatikan jawaban pada isi file dengan command: `cat ScheduledTasks.txt | grep 'Power Management'`

Stop On Battery Mode, No Start On Batteries:

```
Power Management: Stop On Battery Mode, No Start On Batteries
Power Management: Stop On Battery Mode, No Start On Batteries
Power Management: Stop On Battery Mode, No Start On Batteries
```

Task5:

Kami menemukan "Run as user" pada file "ScheduledTasks.txt", saat memperhatikan jawaban pada isi file dengan command: `cat ScheduledTasks.txt | grep 'Run As User'`

```
Run As User: SYSTEM
Run As User: SYSTEM
Run As User: SYSTEM
Run As User: SYSTEM
```

Evidence:

```
removagg@LAPTOP-2NIQFF5:~$
Masukkan Token Tim >> ks4e8a6c
[✓] Token Terverifikasi: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #02: SCHEDULED TASK - STORAGE OPTIMIZATION (100 pts)
Kategori: Easy | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\Defrag\ScheduledDefrag
✓ Benar! Evidence valid.

[Bagian 2/5] Task to run?
Jawaban >> %windir%\system32\defrag.exe -c -h -o -s
✓ Benar! Evidence valid.

[Bagian 3/5] Last result?
Jawaban >> 267011
✓ Benar! Evidence valid.

[Bagian 4/5] Power management?
Jawaban >> Stop On Battery Mode, No Start On Batteries
✓ Benar! Evidence valid.

[Bagian 5/5] Run as user?
Jawaban >> SYSTEM
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{ee6933f4dda0b4ff9e706c13ee1271ea}

Tekan [ENTER] untuk keluar / kembali...
```

Task1:

Ditemukan pada file "ScheduledTasks.txt" dengan command: `cat ScheduledTasks.txt | grep 'Memory'`

```
$ cat ScheduledTasks.txt | grep 'Memory'
Folder: \Microsoft\Windows\MemoryDiagnostic
TaskName: \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents
TaskName: \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents
TaskName: \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents
TaskName: \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic
```

Task2:

Ditemukan pada file "ScheduledTasks.txt" dengan command: `cat ScheduledTasks.txt | grep 'Last Run'`

```
Last Run Time: 8/21/2026 5:52:10 AM
Last Run Time: 8/21/2026 5:52:10 AM
```

Taa

Evidence:

```
removeegg@LAPTOP-2NIQFF5 x + v

[✓] Token Terverifikasi: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #03: SCHEDULED TASK - MEMORY DIAGNOSTIC EVENTS (100 pts)
Kategori: Easy | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\MemoryDiagnostic\ProcessMemoryDiagnosticEvents
✓ Benar! Evidence valid.

[Bagian 2/5] Last run time?
Format input: M/D/YYYY H:MM:SS AM/PM
Jawaban >> 8/21/2026 5:52:18 AM
✓ Benar! Evidence valid.

[Bagian 3/5] Last result?
Jawaban >> ~2147020576
✓ Benar! Evidence valid.

[Bagian 4/5] Run as user?
Jawaban >> Administrators
✓ Benar! Evidence valid.

[Bagian 5/5] Schedule type?
Format input: SCHEDULE TYPE
Jawaban >> When an event occurs
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{df242e6a13cde9fd18df8c0bdfbdf5e}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removeegg@LAPTOP-2NIQFF5 x + v

Masukkan Token Tim >> ks4e8a6c

[✓] Token Terverifikasi: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #04: PREFETCH DEFENDER/REMOVAL INVENTORY (100 pts)
Kategori: Easy | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/5] MpCmdRun Prefetch?
Jawaban >> MPCMDRUN.EXE-2C9109F9.pf
✓ Benar! Evidence valid.

[Bagian 2/5] MpSigStub variant 1?
Jawaban >> MPSIGSTUB.EXE-5D0450B3.pf
✓ Benar! Evidence valid.

[Bagian 3/5] MpSigStub variant 2?
Jawaban >> MPSIGSTUB.EXE-E6B2483B.pf
✓ Benar! Evidence valid.

[Bagian 4/5] MRT Prefetch?
Jawaban >> MRT.EXE-46668014.pf
✓ Benar! Evidence valid.

[Bagian 5/5] Antimalware engine Prefetch?
Jawaban >> AM_ENGINE.EXE-F1C956E4.pf
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{24e45010a2d569548dacfd0bc2a7348e}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5 x + v
└─$ ssh n1g5vghj@209.25.142.16 -p 3738 ks4e8a6c
(n1g5vghj@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Kopral Satu Kopral Dua Minum Kopi

=====
CASE #05: PREFETCH ARTIFACT INVENTORY (100 pts)
Kategori: Easy | Tim: Kopral Satu Kopral Dua Minum Kopi
=====

[Bagian 1/5] Prefetch CERTUTIL?
Jawaban >> CERTUTIL.EXE-28F1E0C1.pf
✓ Benar! Evidence valid.

[Bagian 2/5] Prefetch FODHELPER?
Jawaban >> FODHELPER.EXE-7F1ED892.pf
✓ Benar! Evidence valid.

[Bagian 3/5] Prefetch IPCONFIG?
Jawaban >> IPCONFIG.EXE-BFEC2AD0.pf
✓ Benar! Evidence valid.

[Bagian 4/5] Prefetch HOSTNAME?
Jawaban >> HOSTNAME.EXE-03A2F198.pf
✓ Benar! Evidence valid.

[Bagian 5/5] Prefetch FINDSTR?
Jawaban >> FINDSTR.EXE-1BC2295F.pf
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{aeab3039fa2b9281136446fb2ba998e}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5 x + v
└─$ ssh nz23q2dp@209.25.142.16 -p 3738 ks4e8a6c
(nz23q2dp@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Kopral Satu Kopral Dua Minum Kopi

=====
CASE #06: SCHEDULED TASK - FULL MEMORY DIAGNOSTIC (100 pts)
Kategori: Easy | Tim: Kopral Satu Kopral Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\MemoryDiagnostic\RunFullMemoryDiagnostic
✓ Benar! Evidence valid.

[Bagian 2/5] Status?
Jawaban >> Disabled
✓ Benar! Evidence valid.

[Bagian 3/5] Scheduled task state?
Jawaban >> Disabled
✓ Benar! Evidence valid.

[Bagian 4/5] Comment?
Jawaban >> Detects and mitigates problems in physical memory (RAM).
✓ Benar! Evidence valid.

[Bagian 5/5] Run as user?
Jawaban >> Administrators
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{0a94196b09493d5718e0df66453564ef}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5 x + v

=====
CASE #07: SCHEDULED TASK - DEFENDER SCHEDULED SCAN (100 pts)
Kategori: Easy | Tim: Kopral Satu Kopral Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\UpdateOrchestrator\Schedule Scan
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan
✓ Benar! Evidence valid.

[Bagian 2/5] Task to run?
Jawaban >> C:\Program Files\Windows Defender\MpCmdRun.exe Scan -ScheduleJob -ScanTrigger 55
✓ Benar! Evidence valid.

[Bagian 3/5] Comment?
Jawaban >> Periodic scan task.
✓ Benar! Evidence valid.

[Bagian 4/5] Power management?
Jawaban >> No Start On Batteries
✓ Benar! Evidence valid.

[Bagian 5/5] Run as user?
Jawaban >> SYSTEM
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{3e51bc7f8db0f6a91db94bca321deb4}

=====

Tekan [ENTER] untuk keluar / kembali...|
```

```
removegg@LAPTOP-2NIQFF5 x + v

Kategori: Easy | Tim: Kopral Satu Kopral Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \MicrosoftEdgeUpdateTaskMachineCore
✓ Benar! Evidence valid.

[Bagian 2/5] Status?
Jawaban >> Running
✓ Benar! Evidence valid.

[Bagian 3/5] Last result?
Jawaban >> 267009
✓ Benar! Evidence valid.

[Bagian 4/5] Task to run?
Jawaban >> C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe /c
✓ Benar! Evidence valid.

[Bagian 5/5] Schedule type?
Format input: SCHEDULE_TYPE
Jawaban >> Daily
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Schedule type?
Format input: SCHEDULE_TYPE
Jawaban >> Daily
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Schedule type?
Format input: SCHEDULE_TYPE
Jawaban >> daily
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Schedule type?
Format input: SCHEDULE_TYPE
Jawaban >> At logon time
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{c2c36aed9e32eecd8d7da53827546fe3}
```

```
removegg@LAPTOP-2NIQFF5  x  +  v
Tekan [ENTER] untuk keluar / kembali...
Connection to 209.25.142.16 closed.

[removegg@LAPTOP-2NIQFF5]~/mnt/d/ctf/2026_RISETHERANGERFinal
└─$ ssh fwfylv@209.25.142.16 -p 3738 ks4e8a6c
(fwfylv@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #09: PREFETCH EDGE UPDATE INVENTORY (200 pts)
Kategori: Medium | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/s] EdgeUpdate variant 1?
Jawaban >> MICROSOFTEDGEUPDATE.EXE-7A595326.pf
✓ Benar! Evidence valid.

[Bagian 2/s] EdgeUpdate variant 2?
Jawaban >> MICROSOFTEDGEUPDATE.EXE-D9B797EF.pf
✓ Benar! Evidence valid.

[Bagian 3/s] EdgeUpdate COM register?
Jawaban >> MICROSOFTEDGEUPDATECOMREGISTE-6B5F3955.pf
✓ Benar! Evidence valid.

[Bagian 4/s] EdgeUpdate setup?
Jawaban >> MICROSOFTEDGEUPDATESSETUP.EXE-3CACFD4D.pf
✓ Benar! Evidence valid.

[Bagian 5/s] Edge x64 package?
Jawaban >> MICROSOFTEDGE_X64_151.0.4129.-36A6E15F.pf
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG:  RTRTNI26{36f2b95edc119c126098df02e67a14ad}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5  x  +  v
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hxb6dmzz1zh0.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:BackgroundTaskHost.WebAccountProvider
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> C:\Windows\System32\backgroundTaskHost.exe
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hxb6dmzz1zh0.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXw3e32mpkfkfbh0tznppwqfw96t0tfx6.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hxb6dmzz1zh0.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> taskhostw.exe Logon
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/s] Taskhost command?
Jawaban >> taskhostw.exe
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG:  RTRTNI26{8bc1f5e03dbb7aa7b3691e957b00ab5c}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5 > (removegg@LAPTOP-2NIQFF5)~[/mnt/d/ctf/2026_RISETHERANGERFinal]
$ ssh wc@r1n7a@209.25.142.16 -p 3738 ks4e8a6c
(wc@r1n7a@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Kopral Satu Kopral Dua Minum Kopi

=====
CASE #10: PUSHTOINSTALL REGISTRATION SEQUENCE (200 pts)
Kategori: Medium | Tim: Kopral Satu Kopral Dua Minum Kopi
=====

[Bagian 1/5] PushToInstall service-host command?
Jawaban >> C:\Windows\System32\svchost.exe -k netsvcs -p -s PushToInstall
✓ Benar! Evidence valid.

[Bagian 2/5] SC registration command?
Jawaban >> "C:\Windows\system32\sc.exe" start pushtoinstall registration
✓ Benar! Evidence valid.

[Bagian 3/5] WERMGCR command?
Jawaban >> "C:\Windows\system32\wermgr.exe" -upload
✓ Benar! Evidence valid.

[Bagian 4/5] Scheduler parent command?
Jawaban >> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
✓ Benar! Evidence valid.

[Bagian 5/5] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName Global.RulesEngine.AppXgphnekvm0vv49drvfehhb6kyf6ckafp.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.IrisService.AppXwt29n3t7x7q6fgyrbbqxwzkqjffjaw4y.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:WindowsBackup.AppXg20mfg639r98zjt11v82s19ze9v9t09.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Taskhost command?
Jawaban >> "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:Global.Accounts.AppXqe94epy97qwa6w3j6w132e8zvcsl17nd.mca
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 5/5] Taskhost command?
```

```
removegg@LAPTOP-2NIQFF5 > [Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files\RUXIM\PLUGSscheduler.exe"
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> C:\Windows\System32\sc.exe
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files\RUXIM\PLUGSscheduler.exe"
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /ua /installsource scheduler
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files\RUXIM\PLUGSscheduler.exe"
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /ua /installsource scheduler
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Program Files\RUXIM\PLUGSscheduler.exe"
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
✓ Benar! Evidence valid.

[Bagian 5/5] Taskhost logon command?
Jawaban >> taskhostw.exe logon
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{e23f096a08662c5f8bc9beeb60fe7393}

=====
```

```
removegg@LAPTOP-2NIQFF5 x + v
Tekan [ENTER] untuk keluar / kembali...

(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_RISETHERANGERFinal]
$ ssh ehhgocni@209.25.142.16 -p 3738 ks4e8adc
ehhgocni@209.25.142.16) Password:

[V] Token Terverifikasi dari Argumen SSH: Koprал Satu Koprал Dua Minum Kopi

=====
CASE #11: PUSHTOINSTALL LOGIN SEQUENCE (200 pts)
Kategori: Medium | Tim: Koprал Satu Koprал Dua Minum Kopi
=====

[Bagian 1/5] PushToInstall service-host command?
Jawaban >> C:\Windows\System32\svchost.exe -k netsvcs -p -s PushToInstall
✓ Benar! Evidence valid.

[Bagian 2/5] SC command?
Jawaban >> "C:\Windows\system32\sc.exe" start pushtoinstall registration
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 2/5] SC command?
Jawaban >> sc.exe
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 2/5] SC command?
Jawaban >> "C:\Windows\system32\sc.exe" start pushtoinstall logi
✓ Benar! Evidence valid.

[Bagian 3/5] SC image?
Jawaban >> C:\Windows\System32\sc.exe
✓ Benar! Evidence valid.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> "C:\Windows\system32\sc.exe" start pushtoinstall registration
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> C:\Windows\SysWOW64\schtasks.exe -create -tn Microsoft\Windows\WindowsUpdate\RUXIM\PLUGScheduler -xml plugscheduler.xml -F
X Evidence tidak cocok. Silakan coba lagi.

[Bagian 4/5] SC parent scheduler command?
Jawaban >> C:\Windows\SysWOW64\schtasks.exe -create -tn Microsoft\Windows\WindowsUpdate\RUXIM\PLUGScheduler -xml plugscheduler.xml -F
X Evidence tidak cocok. Silakan coba lagi.
```

```
removegg@LAPTOP-2NIQFF5 x + v

=====
CASE #01: SCHEDULED TASK - DEFENDER CACHE MAINTENANCE (100 pts)
Kategori: Easy | Tim: Koprал Satu Koprал Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> Microsoft\Windows Defender\Windows Defender Cache Maintenance
✓ Benar! Evidence valid.

[Bagian 2/5] Task to run?
Jawaban >> C:\Program Files\Windows Defender\MpCmdRun.exe -IdleTask -TaskName WdCacheMaintenance
✓ Benar! Evidence valid.

[Bagian 3/5] Comment?
Jawaban >> Periodic maintenance task.
✓ Benar! Evidence valid.

[Bagian 4/5] Schedule type?
Format input: SCHEDULE_TYPE
Jawaban >> On demand only
✓ Benar! Evidence valid.

[Bagian 5/5] Stop-after duration?
Format input: HH:MM:SS
Jawaban >> 72:00:00
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{44dd987bed542c52ec45bfe336cbbf93}

=====

Tekan [ENTER] untuk keluar / kembali...
Connection to 209.25.142.16 closed.

(removegg@LAPTOP-2NIQFF5J) [/mnt/d/ctf/2026_RISETHERANGERFinal]
```

```
removegg@LAPTOP-2NIQFF5 X + v
[Bagian 5/s] Associated service-host command?
Jawaban >> Connection to 209.25.142.16 closed by remote host.

[removegg@LAPTOP-2NIQFF5]~/mnt/d/ctf/2026_RISETHERANGERFinal
$ ssh lzw6bpou@209.25.142.16 -p 3738 ks4e8a6c
(lzw6bpou@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #14: PROCESS INVENTORY - DEFRAK CONTEXT A (200 pts)
Kategori: Medium | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/s] Defrag image?
Jawaban >> C:\Windows\System32\Defrag.exe
✓ Benar! Evidence valid.

[Bagian 2/s] Defrag command?
Jawaban >> "C:\Windows\system32\defrag.exe" -p 648 -s 000000000000398 -b -OnlyPreferred C:
✓ Benar! Evidence valid.

[Bagian 3/s] Defrag parent image?
Jawaban >> C:\Windows\System32\svchost.exe
✓ Benar! Evidence valid.

[Bagian 4/s] Defrag parent command?
Jawaban >> C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
✓ Benar! Evidence valid.

[Bagian 5/s] Associated service-host command?
Jawaban >> C:\Windows\system32\svchost.exe -k defragsvc
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{465234b3b1bb62a7f4ccd5bc5c42723b}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQFF5 X + v
Jawaban >> "C:\Windows\system32\defrag.exe" -p 648 -s 000000000000398 -b -OnlyPreferred C:
X Evidence tidak cocok.
(Percobaan salah: 4/5. Sisa 1x sebelum jeda cooldown 15 detik)

[Bagian 2/s] Defrag command?
Jawaban >> "C:\Windows\system32\defrag.exe" -p 654 -s 00000000000015C -b -OnlyPreferred C:
X Evidence tidak cocok.

[⚠ PERINGATAN RATE LIMIT] Terlalu banyak jawaban salah (5x percobaan berturut-turut).
Sistem menjeda input selama 15 detik untuk mencegah spam submission...
[✓] Waktu cooldown selesai! Silakan periksa kembali artefak dan masukkan jawaban.

[Bagian 2/s] Defrag command?
Jawaban >> "C:\Windows\system32\defrag.exe" -p 688 -s 0000000000003B4 -b -OnlyPreferred C:
✓ Benar! Evidence valid.

[Bagian 3/s] Defrag parent image?
Jawaban >> C:\Windows\System32\Defrag.exe
X Evidence tidak cocok.
(Percobaan salah: 1/5. Sisa 4x sebelum jeda cooldown 15 detik)

[Bagian 3/s] Defrag parent image?
Jawaban >> C:\Windows\System32\Defrag.exe
X Evidence tidak cocok.
(Percobaan salah: 2/5. Sisa 3x sebelum jeda cooldown 15 detik)

[Bagian 3/s] Defrag parent image?
Jawaban >> C:\Windows\System32\svchost.exe
✓ Benar! Evidence valid.

[Bagian 4/s] Parent service command?
Jawaban >> C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
✓ Benar! Evidence valid.

[Bagian 5/s] Console host command?
Jawaban >> \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG: RTRTNI26{e414f7b5c7e0a57d8319d3ee956414b1}
```

```
removegg@LAPTOP-2NIQFF5  +  -  
  
=====   
CASE #15: PROCESS INVENTORY - DEFRAG CONTEXT B (200 pts)   
Kategori: Medium | Tim: Kopral Satu Kopral Dua Minum Kopi   
=====   
  
[Bagian 1/5] Service host command?   
Jawaban >> C:\Windows\system32\svchost.exe -k defragsvc   
✓ Benar! Evidence valid.   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 654 -s 000000000000015C -b -OnlyPreferred C:   
X Evidence tidak cocok.   
(Percobaan salah: 1/5. Sisa 4x sebelum jeda cooldown 15 detik)   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 654 -s 000000000000015C -b -OnlyPreferred C:   
X Evidence tidak cocok.   
(Percobaan salah: 2/5. Sisa 3x sebelum jeda cooldown 15 detik)   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 648 -s 0000000000000398 -b -OnlyPreferred C:   
X Evidence tidak cocok.   
(Percobaan salah: 3/5. Sisa 2x sebelum jeda cooldown 15 detik)   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 648 -s 0000000000000398 -b -OnlyPreferred C:   
X Evidence tidak cocok.   
(Percobaan salah: 4/5. Sisa 1x sebelum jeda cooldown 15 detik)   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 654 -s 000000000000015C -b -OnlyPreferred C:   
X Evidence tidak cocok.   
  
[⚠ PERINGATAN RATE LIMIT] Terlalu banyak jawaban salah (5x percobaan berturut-turut).   
Sistem menjeda input selama 15 detik untuk mencegah spam submission...   
[✓] Waktu cooldown selesai! Silakan periksa kembali artefak dan masukkan jawaban.   
  
[Bagian 2/5] Defrag command?   
Jawaban >> "C:\Windows\system32\defrag.exe" -p 688 -s 00000000000003B4 -b -OnlyPreferred C:   
✓ Benar! Evidence valid.   
  
[Bagian 3/5] Defrag parent image?   
Jawaban >> C:\Windows\System32\Defrag.exe   
  
08:59 24/08/2026
```

```
removegg@LAPTOP-2NIQFF5  +  -  
  
Wajib memasukkan Token Tim unik (8 karakter hash) untuk mengakses arena.   
  
Masukkan Token Tim >> ks4e8a6c   
  
[✓] Token Terverifikasi: Kopral Satu Kopral Dua Minum Kopi   
  
=====   
CASE #13: SCHEDULED TASK - EDGE UA (200 pts)   
Kategori: Medium | Tim: Kopral Satu Kopral Dua Minum Kopi   
=====   
  
[Bagian 1/5] Task name?   
Jawaban >> \MicrosoftEdgeUpdateTaskMachineUA   
✓ Benar! Evidence valid.   
  
[Bagian 2/5] Next run time?   
Format input: M/D/YYYY H:MM:SS AM/PM   
Jawaban >> 8/21/2026 6:44:39 AM   
✓ Benar! Evidence valid.   
  
[Bagian 3/5] Last run time?   
Format input: M/D/YYYY H:MM:SS AM/PM   
Jawaban >> 8/21/2026 5:44:40 AM   
✓ Benar! Evidence valid.   
  
[Bagian 4/5] Start time?   
Format input: M/D/YYYY H:MM:SS AM/PM   
Jawaban >> 7:44:39 AM   
✓ Benar! Evidence valid.   
  
[Bagian 5/5] Task repeat interval (Contoh format: 1 Hour(s), 0 Minute(s))?   
Jawaban >> 1 Hour(s), 0 Minute(s)   
✓ Benar! Evidence valid.   
  
=====   
✓ SEMUA EVIDENCE VALID! CASE SOLVED!   
=====   
  
FLAG: RTRTNI26{99405e3b32ad75b92836dafdd25cbaf3}   
  
=====   
  
Tekan [ENTER] untuk keluar / kembali...]
```

```
removegg@LAPTOP-2NIQF5  x  +  v

[✓] Token Terverifikasi dari Argumen SSH: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #16: SCHEDULED TASK - MRT HEARTBEAT (200 pts)
Kategori: Medium | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/5] Task name?
Jawaban >> \Microsoft\Windows\RemovalTools\MRT_ERROR_HB
✓ Benar! Evidence valid.

[Bagian 2/5] Next run time?
Format input: R/D/YYYY H:MM:SS AM/PM
Jawaban >> 8/21/2026 7:36:24 AM
✓ Benar! Evidence valid.

[Bagian 3/5] Last result?
Jawaban >> -2147828576
✓ Benar! Evidence valid.

[Bagian 4/5] Task to run?
Jawaban >> C:\Windows\system32\MRT.exe /EHB /HeartbeatFailure "SubmitHeartbeatReportData" /HeartbeatError
X Evidence tidak cocok.
(Percobaan salah: 1/5. Sisa 4x sebelum jeda cooldown 15 detik)

[Bagian 4/5] Task to run?
Jawaban >> C:\Windows\system32\MRT.exe /EHB /HeartbeatFailure "SubmitHeartbeatReportData" /HeartbeatError "0x88072ee7"
✓ Benar! Evidence valid.

[Bagian 5/5] Task repeat interval (Contoh format: 5 Hour(s), 0 Minute(s))?
Jawaban >> 5 Hour(s), 0 Minute(s)
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG:  RTRTNI26{6e3acd016a2e1eab6ccbd43377255bca}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQF5  x  +  v

Tekan [ENTER] untuk keluar / kembali...

[removegg@LAPTOP-2NIQF5J] [/mnt/d/ctf/2026_RISETHERANGERFinal]
$ seh h9w19vc6@209.25.142.16 -p 3738 ks4e8a6c
(h9w19vc6@209.25.142.16) Password:

[✓] Token Terverifikasi dari Argumen SSH: Koprak Satu Koprak Dua Minum Kopi

=====
CASE #17: PREFETCH DLLHOST SET (200 pts)
Kategori: Medium | Tim: Koprak Satu Koprak Dua Minum Kopi
=====

[Bagian 1/5] Jumlah DLLHOST Prefetch?
Jawaban >> 13
✓ Benar! Evidence valid.

[Bagian 2/5] Variant 15CDDA9C?
Jawaban >> DLLHOST.EXE-15CDDA9C.pf
✓ Benar! Evidence valid.

[Bagian 3/5] Variant 6389524F?
Jawaban >> DLLHOST.EXE-6389524F.pf
✓ Benar! Evidence valid.

[Bagian 4/5] Variant A018D183?
Jawaban >> DLLHOST.EXE-A018D183.pf
✓ Benar! Evidence valid.

[Bagian 5/5] Variant E9BDD97B?
Jawaban >> DLLHOST.EXE-E9BDD97B.pf
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG:  RTRTNI26{916bc2b7ec227c18756031bb0aeb3b2}

=====
Tekan [ENTER] untuk keluar / kembali...
```

```
removegg@LAPTOP-2NIQF5  x  +  v

[Bagian 1/5] Variant 1?
Jawaban >> BACKGROUNDTRANSFERHOST.EXE-052CB2AA.pf
X Evidence tidak cocok.
(Percobaan salah: 3/5. Sisa 2x sebelum jeda cooldown 15 detik)

[Bagian 1/5] Variant 1?
Jawaban >> BACKGROUNDTASKHOST.EXE-073D0F2B.pf
✓ Benar! Evidence valid.

[Bagian 2/5] Variant 2?
Jawaban >> BACKGROUNDTASKHOST.EXE-180BAA32.pf
✓ Benar! Evidence valid.

[Bagian 3/5] Variant 3?
Jawaban >> BACKGROUNDTASKHOST.EXE-6EA81700.pf
X Evidence tidak cocok.
(Percobaan salah: 1/5. Sisa 4x sebelum jeda cooldown 15 detik)

[Bagian 3/5] Variant 3?
Jawaban >> BACKGROUNDTASKHOST.EXE-F8B2D001.pf
X Evidence tidak cocok.
(Percobaan salah: 2/5. Sisa 3x sebelum jeda cooldown 15 detik)

[Bagian 3/5] Variant 3?
Jawaban >> BACKGROUNDTASKHOST.EXE-332B0729.pf
✓ Benar! Evidence valid.

[Bagian 4/5] Variant 4?
Jawaban >> BACKGROUNDTASKHOST.EXE-F8B2D001.pf
X Evidence tidak cocok.
(Percobaan salah: 1/5. Sisa 4x sebelum jeda cooldown 15 detik)

[Bagian 4/5] Variant 4?
Jawaban >> BACKGROUNDTASKHOST.EXE-6EA81700.pf
✓ Benar! Evidence valid.

[Bagian 5/5] Variant 5?
Jawaban >> BACKGROUNDTASKHOST.EXE-F8B2D001.pf
✓ Benar! Evidence valid.

=====
✓ SEMUA EVIDENCE VALID! CASE SOLVED!
=====

FLAG:  RTRTNI26{06210936f2886ea14cfdd01db885134e}
=====
```

[Bagian 1/5] Earlier-run customer-data rename timestamp?

Format input: YYYY-MM-DD HH:MM:SS

Jawaban >> 2026-08-21 07:18:11

✓ Benar! Evidence valid.

[Bagian 2/5] Earlier-run new filename?

Jawaban >> customer-data.locked

✓ Benar! Evidence valid.

[Bagian 3/5] Final-run customer-data rename timestamp?

Format input: YYYY-MM-DD HH:MM:SS

Jawaban >> 2026-08-21 21:17:12

✓ Benar! Evidence valid.