Linux Restricted Shell Breakout via Linux Binary(s)

Identifies the abuse of a Linux binary to break out of a restricted shell or environment by spawning an interactive system shell. The activity of spawning a shell from a binary is not common behavior for a user or system administrator, and may indicate an attempt to evade detection, increase capabilities or enhance the stability of an adversary.

Rule type: eql

Rule indices:

- logs-endpoint.events.*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

- https://gtfobins.github.io/gtfobins/gawk/
- https://gtfobins.github.io/gtfobins/busybox/
- https://gtfobins.github.io/gtfobins/c89/
- https://gtfobins.github.io/gtfobins/c99/
- https://gtfobins.github.io/gtfobins/cpulimit/
- https://gtfobins.github.io/gtfobins/crash/
- https://gtfobins.github.io/gtfobins/env/
- https://gtfobins.github.io/gtfobins/expect/
- https://gtfobins.github.io/gtfobins/find/
- https://gtfobins.github.io/gtfobins/flock/
- https://gtfobins.github.io/gtfobins/gcc/
- https://gtfobins.github.io/gtfobins/mysql/
- https://gtfobins.github.io/gtfobins/nice/
- https://gtfobins.github.io/gtfobins/ssh/
- https://gtfobins.github.io/gtfobins/vi/
- https://gtfobins.github.io/gtfobins/vim/
- https://gtfobins.github.io/gtfobins/capsh/
- https://gtfobins.github.io/gtfobins/byebug/
- https://gtfobins.github.io/gtfobins/git/
- https://gtfobins.github.io/gtfobins/ftp/
- https://www.elastic.co/security-labs/sequel-on-persistence-mechanisms

Tags:

- Domain: Endpoint

Rule authors:

- Elastic

Rule license: Elastic License v2

Investigation guide

edit

Triage and analysis

Investigating Shell Evasion via Linux Utilities

Detection alerts from this rule indicate that a Linux utility has been abused to breakout of restricted shells or environments by spawning an interactive system shell. Here are some possible avenues of investigation: - Examine the entry point to the host and user in action via the Analyse View. - Identify the session entry leader and session user - Examine the contents of session leading to the abuse via the Session View. - Examine the command execution pattern in the session, which may lead to suspricous activities - Examine the execution of commands in the spawned shell. - Identify imment threat to the system from the executed commands - Take necessary incident response actions to contain any malicious behviour caused via this execution.

Related rules

- A malicious spawned shell can execute any of the possible MITTRE ATT&CK vectors mainly to impair defences.

malicious spawned shell,

- Isolate the involved host to prevent further post-compromise behavior.
- If the triage identified malware execution via the maliciously spawned shell,
- Search the environment for additional compromised hosts.
- Implement temporary network rules, procedures, and segmentation to contain the malware.
- Stop suspicious processes.
- Immediately block the identified indicators of compromise (IoCs).
- Inspect the affected systems for additional malware backdoors like reverse shells, reverse proxies, or droppers that attackers could use to reinfect the system.
- If the triage revelaed defence evasion for imparing defenses
- Isolate the involved host to prevent further post-compromise behavior.
- Identified the disabled security guard components on the host and take necessary steps in renebaling the same.
- If any tools have been disbaled / uninstalled or config tampered work towards reenabling the same.
- If the triage revelaed addition of persistence mechanism exploit like auto start scripts
- Isolate further login to the systems that can initae auto start scripts.

rotation process for all exposed crednetials.

- Investiagte if any IPR data was accessed during the data crawling and take appropriate actions.
- Determine the initial vector abused by the attacker and take action to prevent reinfection through the same vector.
- Using the incident response data, update logging and audit policies to improve the mean time to detect (MTTD) and the mean time to respond (MTTR).

Setup

edit

Setup

This rule requires data coming in from Elastic Defend.

Elastic Defend Integration Setup

Elastic Defend is integrated into the Elastic Agent using Fleet. Upon configuration, the integration allows the Elastic Agent to monitor events on your host and send data to the Elastic Security app.

Prerequisite Requirements:

- Fleet is required for Elastic Defend.
- To configure Fleet Server refer to the documentation.

The following steps should be executed in order to add the Elastic Defend integration on a Linux System:

"Traditional Endpoints" or "Cloud Workloads".

- Select a configuration preset. Each preset comes with different default settings for Elastic Agent, you can further customize these later by configuring the Elastic Defend integration policy. Helper guide.
- We suggest selecting "Complete EDR (Endpoint Detection and Response)" as a configuration setting, that provides "All events; all preventions"
- Enter a name for the agent policy in "New agent policy name". If other agent policies already exist, you can click the "Existing hosts" tab and select an existing policy instead. For more details on Elastic Agent configuration settings, refer to the helper guide.
- Click "Save and Continue".
- To complete the integration, select "Add Elastic Agent to your hosts" and continue to the next section to install the Elastic Agent on your hosts. For more details on Elastic Defend refer to the helper guide.

Session View uses process data collected by the Elastic Defend integration, but this data is not always collected by default. Session View is available on enterprise subscription for versions 8.3 and above.

To confirm that Session View data is enabled:

- Go to “Manage → Policies”, and edit one or more of your Elastic Defend integration policies.

“Capture terminal output” toggle. For more information about the additional fields collected when this setting is enabled and the usage of Session View for Analysis refer to the helper guide.

Rule query

edit

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy.
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

```
    (process.parent.name : "*awk" and process.parent
    (process.parent.name == "git" and process.parent
     process.args : ("*PAGER*", "!*sh", "exec *sh")
    (process.parent.name : ("byebug", "ftp", "strace
    (
      process.parent.args : "BEGIN {system(*)}" or
      (process.parent.args : ("*PAGER*", "!*sh", "ex
      (
        (process.parent.args : "exec=*sh" or (proces
        (process.args : "exec=*sh" or (process.args
        )
      )
    ) or

    /* shells specified in parent args */
    /* nice rule is broken in 8.2 */
    (process.parent.args : "*sh" and
      (
        (process.parent.name == "nice") or
        (process.parent.name == "cpulimit" and proce
        (process.parent.name == "find" and process.p
         process.parent.args == ";" and process.pare
        (process.parent.name == "flock" and process.
      )
    )
  )) or

  /* shells specified in args */
  (process.args : "*sh" and (
    (process.parent.name == "crash" and process.pare
  (process.parent.name in ("vi", "vim") and process.
  (process.parent.name in ("c89", "c99", "gcc") and 
  (process.parent.name == "expect" and process.paren
  (process.parent.name == "mysql" and process.parent
  (process.parent.name == "ssh" and process.parent.a
)
```

Framework: MITRE ATT&CK^{TM}

- Tactic:
    - Name: Execution
    - Reference URL: https://attack.mitre.org/tactics/TA0002/
- Technique:
    - Name: Command and Scripting Interpreter
    - ID: T1059
    - Reference URL: https://attack.mitre.org/techniques/T1059/
- Sub-technique:
    - Name: Unix Shell
    - ID: T1059.004
    - Reference URL: https://attack.mitre.org/techniques/T1059/004/

Follow us

About us

- About Elastic
- Leadership
- DE&I
- Blog
- Newsroom

Join us

- Careers
- Career portal

Partners

- Find a partner
- Partner login
- Request access
- Become a partner

Trust & Security

- Trust center
- EthicsPoint portal
- ECCN report
- Ethics email

Investor relations