HPS

Dominik Mann

Forensic Tools and Incident Response

Table of contents

1 Introduction to theoretical Incident Response

2 Practical Incident Response

3 Velociraptor

4 References

Outline

1 Introduction to theoretical Incident Response

2 Practical Incident Response

3 Velociraptor

4 References

SANS Incident Response Process

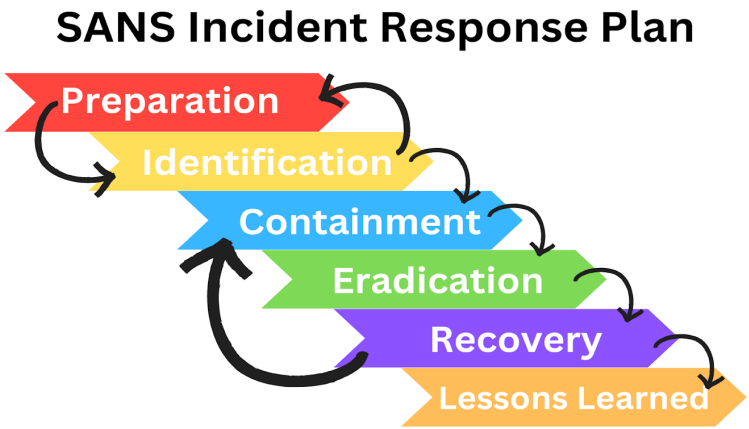
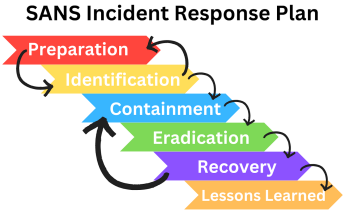


Image source: https://wirexsystems.com/wp-content/uploads/2023/01/unnamed-20.png

Theoretical Incident Response



- Preparation: Ensure timely response to incident
- Identification: Monitor IT-Systems and detect deviations
- Containment: Limit damage from current security incident
- Eradication: Remove malware or other artifacts and fully restore system
- Recovery: Bring system back to full operation
- Lessons Learned: Extract lessons from gathered information

Image source: https://wirexsystems.com/wp-content/uploads/2023/01/unnamed-20.png

Outline

1 Introduction to theoretical Incident Response

2 Practical Incident Response

3 Velociraptor

4 References

Practical Incident Response

- Get forensically sound image of compromised system
  - Raw format
    - Bit by bit copy of raw data on
    - sudo dd if=<*input volume*> of=<*output file*> bs=*block size* conv=noerror,sync
  - E01 or EWF format
    - Physical bitstream with hash values of files
    - Uses compression - not as large as raw image
- Mount the image in read-only mode
  - sudo mount -o ro,noload <*output file*> <*mount point*>
- Where to go from here?

Practical Incident Response

- Check SSH-Log for Logins
- Check running processes
- Check bash history
- Check timestamps of suspicious files or common used binaries
- Check crontab for automatic executions
- ...
  - Use scripts for automatically collecting evidence

Real life example

```
$ ls -la /etc/fonts
drwxr-xr-x.   3 root root    4096 Feb 20 01:31 .
drwxr-xr-x. 128 root root   12288 May 13 18:10 ..
-rwsr-sr-x    1 root root    8616 Feb 24  2017 .fonts
-rwxr-xr-x    1 root 200046 20144 Feb 24  2017 .low
drwxr-xr-x.   2 root root    4096 Feb 20 01:31 conf.d
-rw-r--r--    1 root root    2416 Jun  8  2018 fonts.conf
```

- Notice of partner HPC cluster of compromise and likely indicator of compromise
- Two executables found on few clusters that did not belong there
- Used kernel exploit to gain root access
- Forensic workflow: Iterativley appending timeline and performing extensive search with script
- Ultimately gained access to head node

Image source: https://www.educv.de/blog/post-2021-02-17-analyzing-a-compromised-hpc-cluster/

Chain of infection

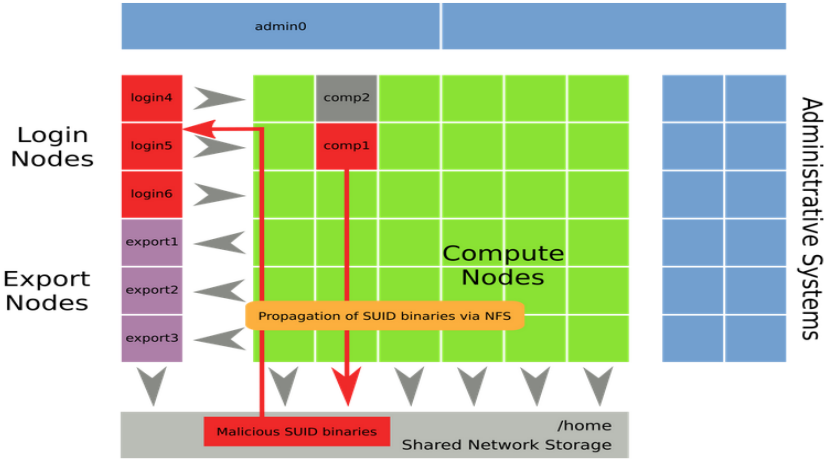


Image source: https://www.educv.de/blog/post-2021-02-17-analyzing-a-compromised-hpc-cluster/

Outline

1 Introduction to theoretical Incident Response

2 Practical Incident Response

3 Velociraptor

4 References

Shift from traditional Incident Response

Velociraptor

- Traditional evidence acquisition consists of bit by bit copy of disk and memory
  - In HPC context not always feasible
- **Use live triage**
- Velociraptor connects clients to central Velociraptor server
- Load for searching and evidence acquisition placed on clients
  - Allows concurrent searches and execution of code on multiple remote clients in real time
- Uses "Artifacts" to "hunt"
- Can use any forensic tool as long as there is interactivity

Image source: https://docs.velociraptor.app/

Summary

- Incident response is not a strict consecutive chain of actions
- Getting forensically sound images of compromised systems is crucial
- Automation is important for Incident Response, however manual acquisition is always needed
  - Need to know normal behavior of system
- Modern Incident Response begins to shift towards live response

References

- Johansen, Gerard. Digital forensics and incident response: Incident response techniques and procedures to respond to modern cyber threats. Packt Publishing Ltd, 2020.
- Kral, Patrick. "The incident handlers handbook." SANS Institute, 2011.
- Brücker, Pascal. "Analyzing a compromised HPC cluster." Technische Universität Dresden, 2021.