



RCE en Splunk Empresa



para analistas de SOC

CVE-2023-46214



vamos a defender.io



LetsDefend

MESA DE CONTENIDOS

01

Alerta

04

Detección

05

Análisis

13

Contención

14

Apéndice

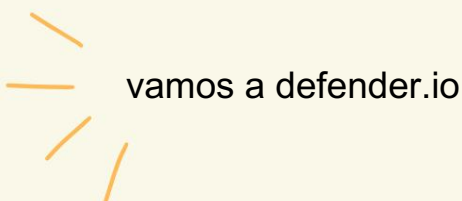
Autor: Muhammet Donmez

Alerta

Al observar el motivo que activó la alerta, se vio que se intentó cargar el archivo XSLT malicioso, que permite que RCE se ejecute en Splunk Enterprise. La alarma violó la regla SOC239: ejecución remota de código detectada en Splunk Enterprise.

★ Splunk App for Lookup File Editing RCE via User XSLT	
EventID :	201
Event Time :	Nov, 21, 2023, 12:24 PM
Rule :	SOC239 - Remote Code Execution Detected in Splunk Enterprise
Level :	Security Analyst
Source IP Address :	180.101.88.240
Destination IP Address :	172.16.20.13
Hostname :	Splunk Enterprise
HTTP Request Method :	POST
Requested URL :	http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xml
Trigger File Path :	/opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xml
Alert Trigger Reason :	Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.
Device Action :	Allowed
File (Password:infected) :	Download

Primero, se debe verificar esta alerta revisando los registros existentes, luego se debe investigar la fuente de este tráfico y se debe confirmar si es tráfico legal.

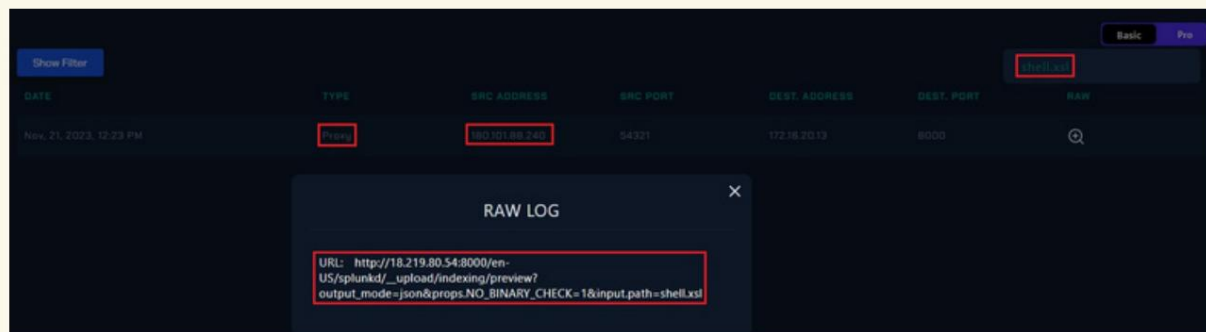


Detección

Verificar

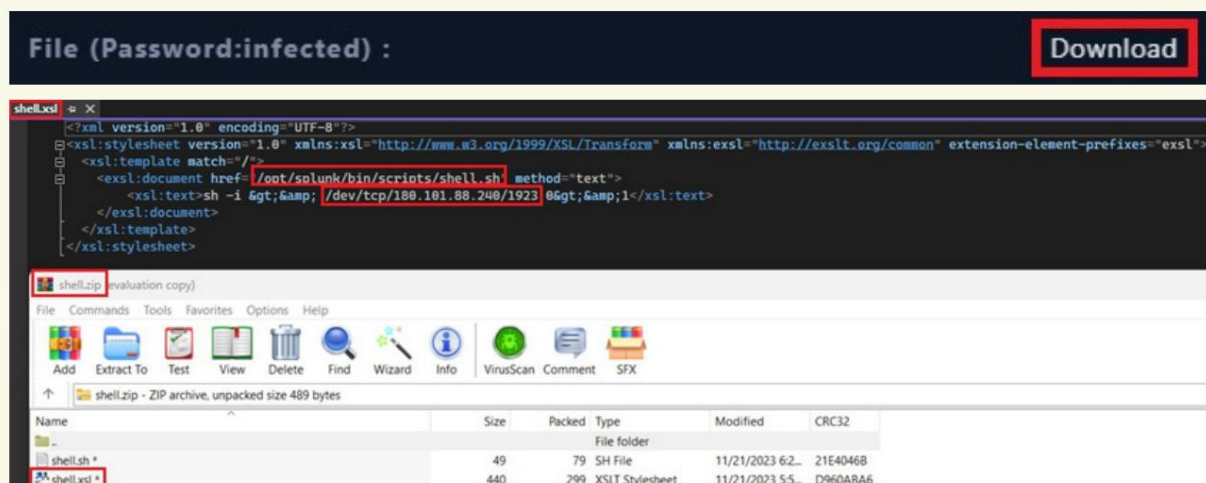
La alarma se activó como resultado de intentar cargar el archivo llamado "shell.xml" en Splunk en la solicitud que llega al sistema. A continuación se muestra la solicitud que activó la alarma. La solicitud relevante se puede buscar y confirmar en Gestión de registros.

RequestURL: http://3.133.116.124:8000/en-US/splunkd/_upload/indexing/preview?
output_mode=json&props.NO_BINARY_CHECK=1&input.path= shell.xml



Como se puede ver arriba, la solicitud correspondiente llegó a las "12:23 p. m.". Se vio que la solicitud correspondiente procedía de la dirección IP "180.101.88.240" ubicada en China. Como resultado de las investigaciones realizadas hasta el momento, se ha confirmado que hubo un intento de subir archivos al sistema. Por lo tanto la alarma correspondiente es Verdadero Positivo. Sin embargo, para tomar una decisión clara, es necesario examinar el contenido del archivo que se intenta cargar.

Se han compartido archivos relevantes para su descarga con detalle de la alarma.



Análisis

Verificación de reputación

Al cargar el archivo, se debe verificar la reputación de "180.101.88.240" que se ve en la IP de origen.

180.101.88.240 was found in our database!

This IP was reported **12,872** times. Confidence of Abuse is **100%**: ?

100%

ISP: ChinaNet Jiangsu Province Network
Usage Type: Data Center/Web Hosting/Transit
Domain Name: chinatelecom.com.cn
Country: China
City: Suzhou, Jiangsu

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

[REPORT 180.101.88.240](#) [WHOIS 180.101.88.240](#)

IP Abuse Reports for 180.101.88.240

This IP address has been reported a total of **12,872** times from 65 distinct sources. 180.101.88.240 was first reported on August 17th 2023, and the most recent report was 3 minutes ago.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
Abuse Reporting	2023-11-22 09:44:33 (3 minutes ago)	Nov 22 09:43:23 Server-Eygelsho sshd[193982]: Failed password for root from 180.101.88.240 port 1402 ... show more	Brute-Force SSH
Valea	2023-11-22 09:41:33 (6 minutes ago)	Nov 22 10:41:27 dockerhost sshd[2255944]: Failed password for root from 180.101.88.240 port 62928 ss ... show more	Brute-Force SSH
SIT	2023-11-22 09:40:43 (6 minutes ago)	Nov 22 10:39:27 cloud01 sshd[3150313]: Failed password for root from 180.101.88.240 port 10441 ssh2< ... show more	Brute-Force SSH
devmoon.de	2023-11-22 09:22:45 (24 minutes ago)	Nov 22 10:21:25 docker-01 sshd[799116]: Failed password for root from 180.101.88.240 port 19079 ssh2 ... show more	Brute-Force SSH
Abuse Reporting	2023-11-22 09:20:23 (27 minutes ago)	Nov 22 09:19:09 Server-Eygelsho sshd[193016]: Failed password for root from 180.101.88.240 port 2131 ... show more	Brute-Force SSH

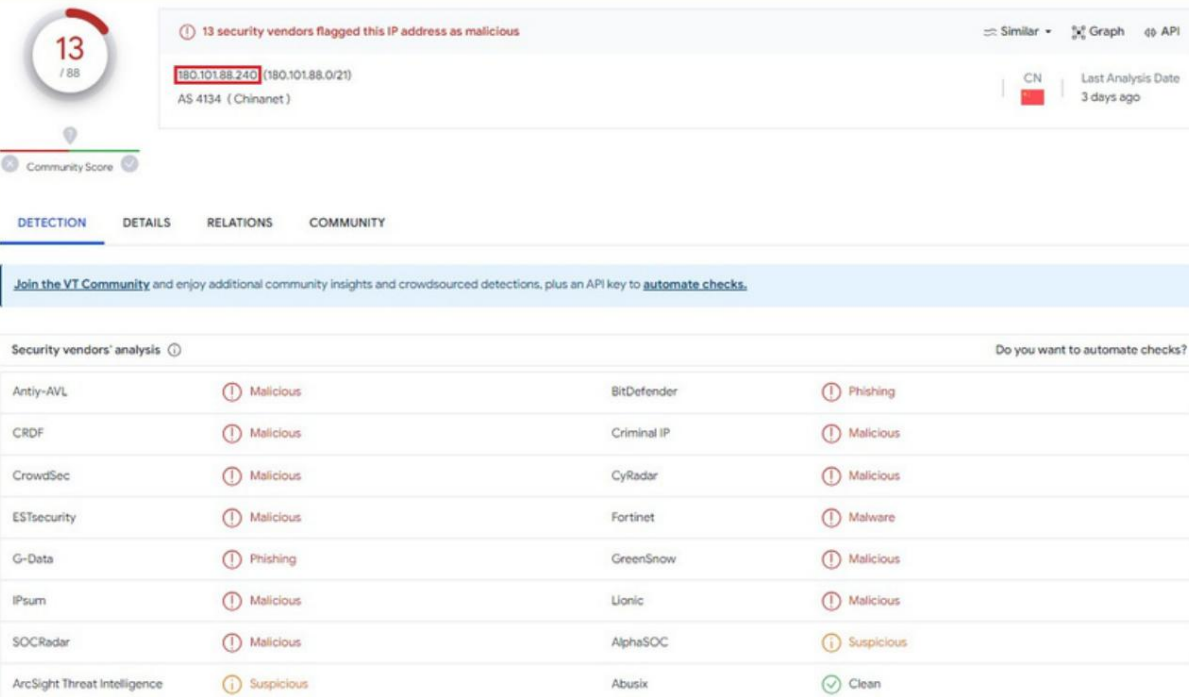
<https://www.abuseipdb.com/check/180.101.88.240>



vamos a defender.io



LetsDefend



The screenshot shows the VirusTotal interface for the IP address 180.101.88.240. At the top, a red circle indicates a score of 13/88. A warning message states: "13 security vendors flagged this IP address as malicious". The IP is listed as 180.101.88.240 (180.101.88.0/21) and is associated with AS 4134 (Chinanet) in China (CN). The last analysis date was 3 days ago. Below the header, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A banner encourages joining the VT Community. The main section, "Security vendors' analysis", shows a table of results from 13 vendors. A link "Do you want to automate checks?" is present on the right.

Security Vendor	Analysis Result
Anti-AVL	Malicious
BitDefender	Phishing
CRDF	Malicious
Criminal IP	Malicious
CrowdSec	Malicious
CyRadar	Malicious
ESTsecurity	Malicious
Fortinet	Malware
G-Data	Phishing
GreenSnow	Malicious
IPsum	Malicious
Lionic	Malicious
SOCradar	Malicious
AlphaSOC	Suspicious
ArcSight Threat Intelligence	Suspicious
Abusix	Clean

<https://www.virustotal.com/gui/ip-address/180.101.88.240>

La IP correspondiente se encuentra en China y pertenece a las empresas de hosting. Cuando se realizan comprobaciones tanto en AbuseIPDB como en Virus Total para la IP 180.101.88.240, se ve que la IP relevante es reportada por diferentes fuentes en categorías como fuerza bruta, phishing y piratería.

Acceso inicial

Antes de iniciar el análisis se deben investigar los detalles del RCE que el atacante probó en el sistema. ¿De qué vulnerabilidad del sistema debería surgir el RCE correspondiente? Si se comprende esta cuestión, las investigaciones serán más fáciles.

Hay un detalle compartido como ejemplo del mundo real en los detalles de la alerta.

★ Splunk App for Lookup File Editing RCE via User XSLT	
EventID :	201
Event Time :	Nov. 21, 2023, 12:24 PM
Rule :	SOC239 - Remote Code Execution Detected in Splunk Enterprise
Level :	Security Analyst
Source IP Address :	180.101.88.240
Destination IP Address :	172.16.20.13
Hostname :	Splunk Enterprise
HTTP Request Method :	POST
Requested URL :	http://18.219.80.54:8000/en-US/splunkd/_upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xsl
Trigger File Path :	/opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xsl
Alert Trigger Reason :	Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.
Device Action :	Allowed
File (Password:infected) :	Download

Cuando buscamos "Aplicación Splunk para edición de archivos de búsqueda RCE mediante usuario XSLT" en Google, nos encontramos con la vulnerabilidad CVE-2023-46214. En los detalles de la vulnerabilidad relevante, se compartió que en las versiones vulnerables, los atacantes pueden cargar el archivo malicioso "XSLT" en los sistemas de destino, lo que permitirá la ejecución remota de código (RCE) en el sistema de destino.

Product	Version	component	Affected Version	FixVersion
Splunk Enterprise	9.0	Splunk Web	9.0.0 to 9.0.6	9.0.7
Splunk Enterprise	9.1	Splunk Web	9.1.0 to 9.1.1	9.1.2
Splunk Cloud	-	Splunk Web	Versions below 9.1.2308	9.1.2308

Fuente: <https://advisory.splunk.com/advisories/SVD-2023-1104>

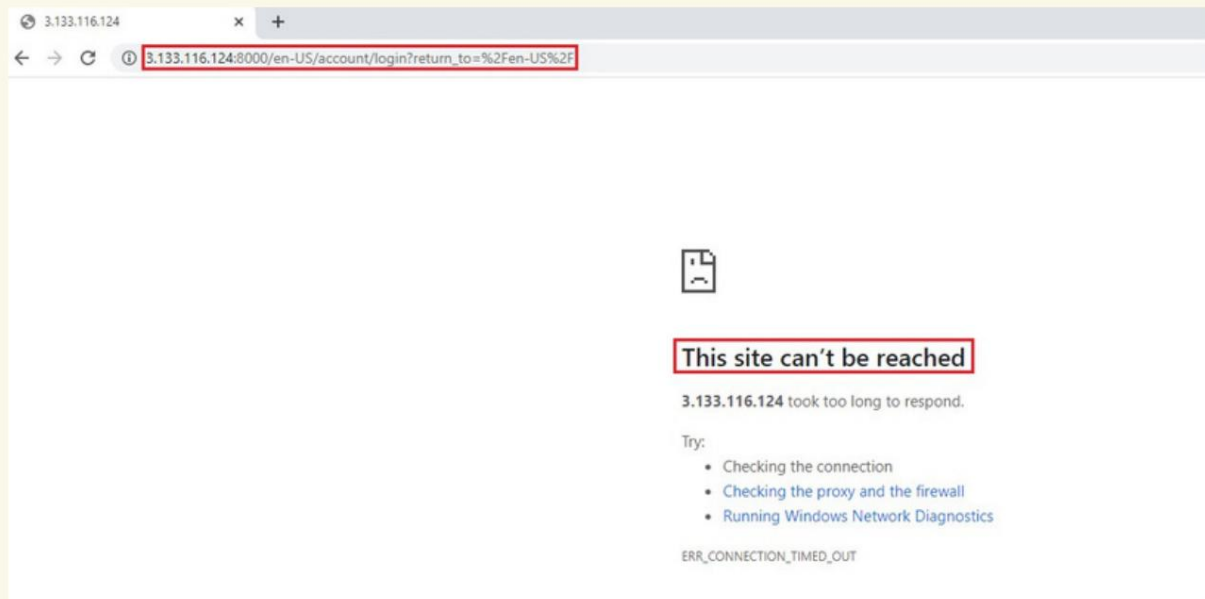
Cuando se realizó un examen POC detallado de la vulnerabilidad relevante, se vio que el atacante necesitaba algunos requisitos previos para explotar la vulnerabilidad relevante en el sistema objetivo. El primer e importante requisito previo es la accesibilidad al sistema de destino. Entonces, como aquí, el sistema de destino debe tener acceso a 3.133.116.124 (Splunk IP) Remote o la información debe haber sido comprometida por alguien que haya accedido a ella. Por ejemplo, permita que el acceso remoto a Splunk esté deshabilitado. Sin embargo, el acceso remoto al sistema debería ser posible con VPN. La información VPN de las personas que acceden aquí debe filtrarse. Por lo tanto, aquí es menos probable que el sistema de destino esté abierto a control remoto. Para probar esto, se puede intentar el acceso a través del puerto 8000 de la IP correspondiente. Como consecuencia del correspondiente control no se pudo conseguir el acceso a Splunk, como se puede comprobar a continuación.



vamos a defender.io

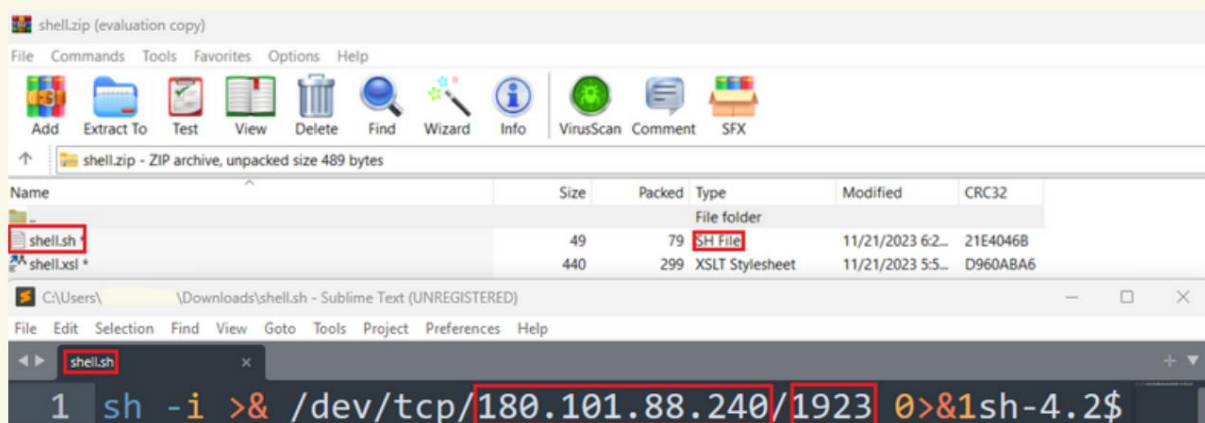


LetsDefend



De aquí se entiende que el acceso al sistema objetivo se logró por otros medios. Se accedió al sistema con las credenciales de otros (empleados de empresas externas), que es uno de los métodos más utilizados por los atacantes. Por lo tanto, se puede decir "Relación de confianza (T1199)" para el acceso inicial. Además, una segunda técnica de acceso inicial puede denominarse "Explotar aplicaciones públicas". Porque el atacante aprovechó la vulnerabilidad de Splunk para obtener acceso al sistema.

El segundo punto importante para explotar la vulnerabilidad es la información de las credenciales del usuario autorizado para iniciar sesión en el sistema de destino. Después de que el atacante inicia sesión en el sistema de destino con el código Python que ejecutará, deja "shell.sh" en la ruta del archivo "/opt/splunk/bin/scripts/". El contenido del archivo relevante se encuentra entre los archivos compartidos en los detalles de la alerta y se puede ver desde allí.

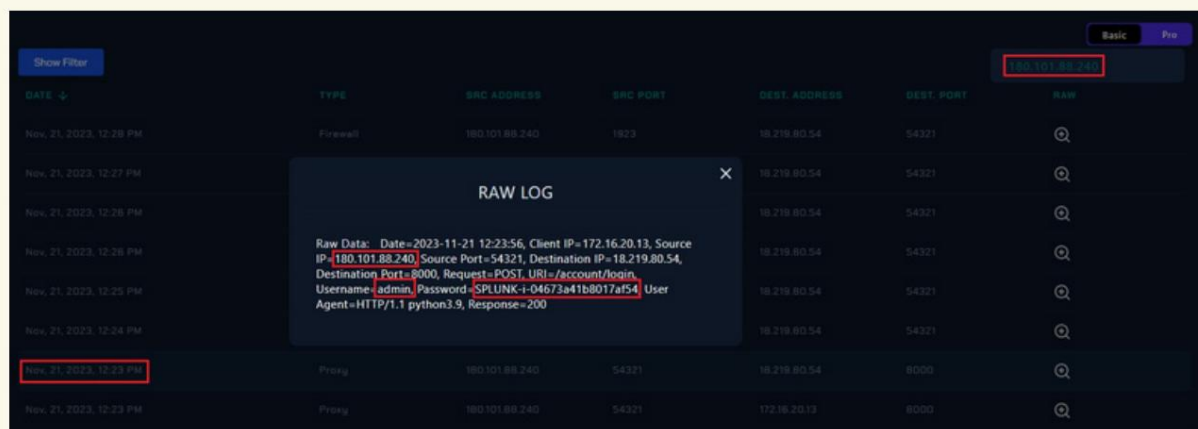


El archivo anterior es aparentemente un comando de shell inverso de Bash. Este comando se utiliza para crear un shell en un sistema de destino y dirigir ese shell como una conexión inversa a la dirección IP y el número de puerto especificados. Crea una conexión TCP usando Bash

Característica /dev/tcp. Crea una conexión inversa con la dirección IP especificada (180[.]101.88.240) y el número de puerto (1923).

El análisis hasta el momento se ha centrado en los archivos compartidos en alerta. De estos archivos se desprende que el atacante tenía la intención de recibir un shell inverso en el sistema de destino. Estas actividades deben confirmarse comprobando los registros en Gestión de registros.

Se debe examinar todo el tráfico de IP "180[.]101.88.240" que intenta cargar "shell.xsl" en Splunk. Como resultado de la búsqueda relevante, los registros de proxy y firewall se ven en Log Management. Los registros deben clasificarse por tiempo y examinarse en detalle. El primer registro de proxy es el registro de carga de archivos al sistema. Los detalles se pueden ver a continuación en el segundo registro de proxy. Se ve que el atacante envió una solicitud de autenticación al sistema a través del puerto 8000, como se puede ver en el registro de nombre de usuario y contraseña.

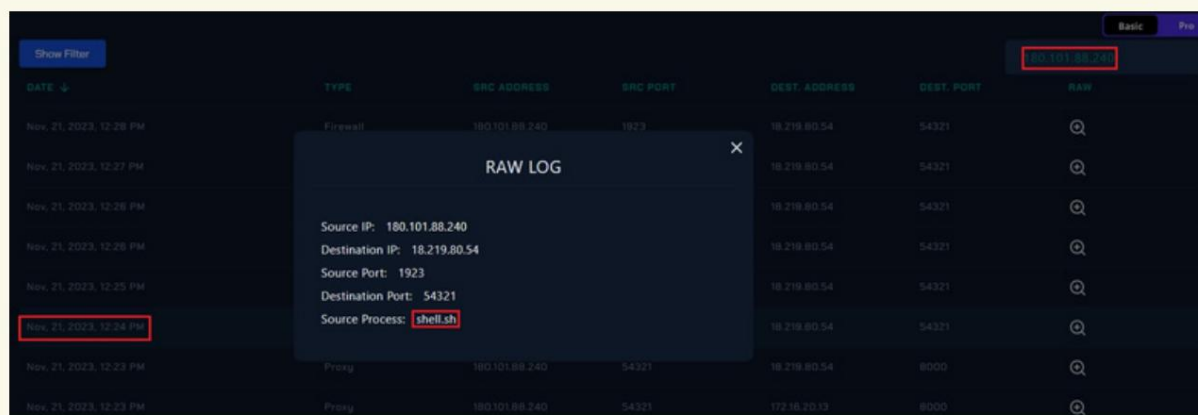


DATE	TYPE	SRC ADDRESS	SRC PORT	DEST ADDRESS	DEST PORT	RAW
Nov 21, 2023, 12:28 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov 21, 2023, 12:27 PM				18.219.80.54	54321	
Nov 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov 21, 2023, 12:25 PM				18.219.80.54	54321	
Nov 21, 2023, 12:24 PM				18.219.80.54	54321	
Nov 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG
Raw Data: Date=2023-11-21 12:23:56, Client IP=172.16.20.13, Source IP=180.101.88.240, Source Port=54321, Destination IP=18.219.80.54, Destination Port=8000, Request=POST, URI=/account/login, Username=admin, Password=SPLUNK-i-04673a41b8017af54, User Agent=HTTP/1.1 python3.9, Response=200

Los detalles del registro de proxy muestran la información de usuario y contraseña utilizada por el atacante para iniciar sesión en el sistema de destino.

Cuando se examinan todos los registros de la IP del atacante en la administración de registros, se cree que se estableció una conexión de shell inversa a las 12:24 p.m. Porque se ve una gran cantidad de tráfico de Firewall, siendo la IP de origen "180.101.88.240", el puerto de origen "1923" y la IP de destino "18.219.80.54 (IP de Splunk)".

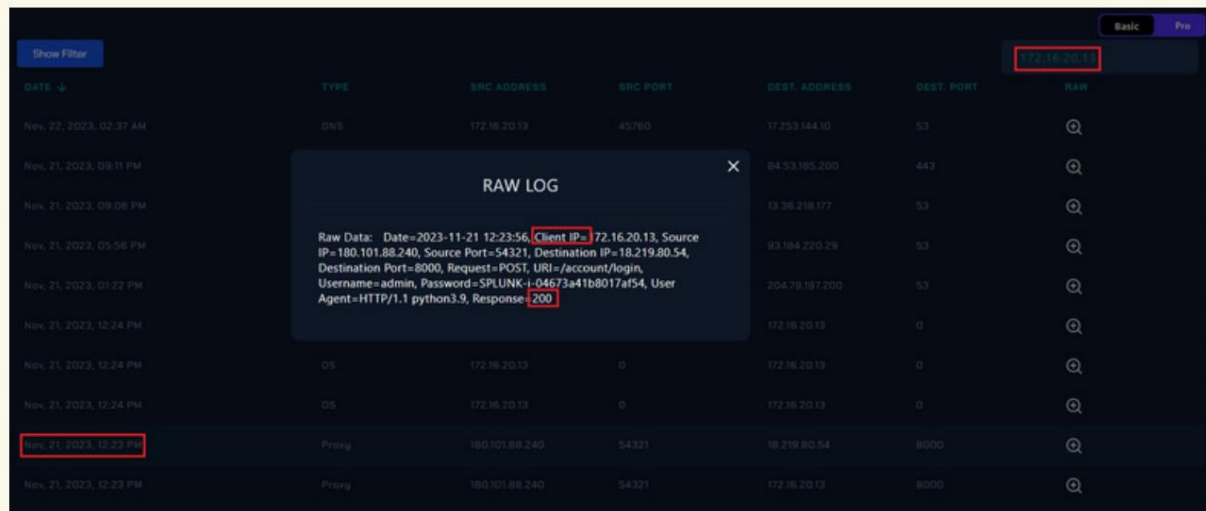


DATE	TYPE	SRC ADDRESS	SRC PORT	DEST ADDRESS	DEST PORT	RAW
Nov 21, 2023, 12:28 PM	Firewall	180.101.88.240	1923	18.219.80.54	54321	
Nov 21, 2023, 12:27 PM				18.219.80.54	54321	
Nov 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov 21, 2023, 12:26 PM				18.219.80.54	54321	
Nov 21, 2023, 12:25 PM				18.219.80.54	54321	
Nov 21, 2023, 12:24 PM				18.219.80.54	54321	
Nov 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG
Source IP: 180.101.88.240
Destination IP: 18.219.80.54
Source Port: 1923
Destination Port: 54321
Source Process: shell.sh



En los detalles de la alarma, se ve "172.16.20.13" como la IP de destino. Si la IP 18.219.80.54 pertenece a Splunk, ¿cuál es esta IP? Esta IP es la IP local de Splunk. En los detalles de los registros del proxy, se lo ve como el cliente de esta IP.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.30	53	
Nov. 21, 2023, 09:11 PM				84.53.185.200	443	
Nov. 21, 2023, 09:08 PM				13.36.218.177	53	
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG

Raw Data: Date=2023-11-21 12:23:56, Client IP=172.16.20.13, Source IP=180.101.88.240, Source Port=54321, Destination IP=18.219.80.54, Destination Port=8000, Request=POST, URI=/account/login, Username=admin, Password=SPLUNK-i-04673a41b8017af54, User Agent=HTTP/1.1 python3.9, Response=200

La IP relevante se puede buscar en Endpoint Security para confirmar. Como resultado, parece que la IP relevante pertenece al host "Splunk Enterprise".



Al examinar la gestión de registros, es necesario buscar según la IP local relevante. Porque también se debe examinar el comportamiento del atacante después de recibir un Shell inverso en el sistema de destino. Por este motivo, se espera que los registros relevantes aparezcan en la IP local.

Show Filter

172.16.20.13

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG

Source IP: 172.16.20.13
Destination IP: 172.16.20.13
Destination Port: 0
Message: session opened for user admin(uid=0) by (uid=0)

Como se puede ver arriba, cuando se busca IP 172.16.20.13, hay registros del sistema operativo, DNS y firewall después de los registros del proxy. Continuando con el análisis por tiempo, se ve que el atacante inició sesión con "admin" a las 12:24 p.m. En el siguiente registro del sistema operativo, se ve que el atacante agregó usuarios para ganar permanencia en el sistema.

Show Filter

172.16.20.13

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG

Username: admin
Source Process Name: bash
Target Process Name: useradd
Target Process Command Line: useradd -m analyst

Agregar usuario

Show Filter

172.16.20.13

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Nov. 22, 2023, 02:37 AM	DNS	172.16.20.13	45760	17.253.144.10	53	
Nov. 21, 2023, 09:11 PM	Firewall	172.16.20.13	64775	84.53.185.200	443	
Nov. 21, 2023, 09:06 PM				13.36.218.177	53	
Nov. 21, 2023, 05:56 PM				93.184.220.29	53	
Nov. 21, 2023, 01:22 PM				204.79.197.200	53	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM				172.16.20.13	0	
Nov. 21, 2023, 12:24 PM	OS	172.16.20.13	0	172.16.20.13	0	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	18.219.80.54	8000	
Nov. 21, 2023, 12:23 PM	Proxy	180.101.88.240	54321	172.16.20.13	8000	

RAW LOG

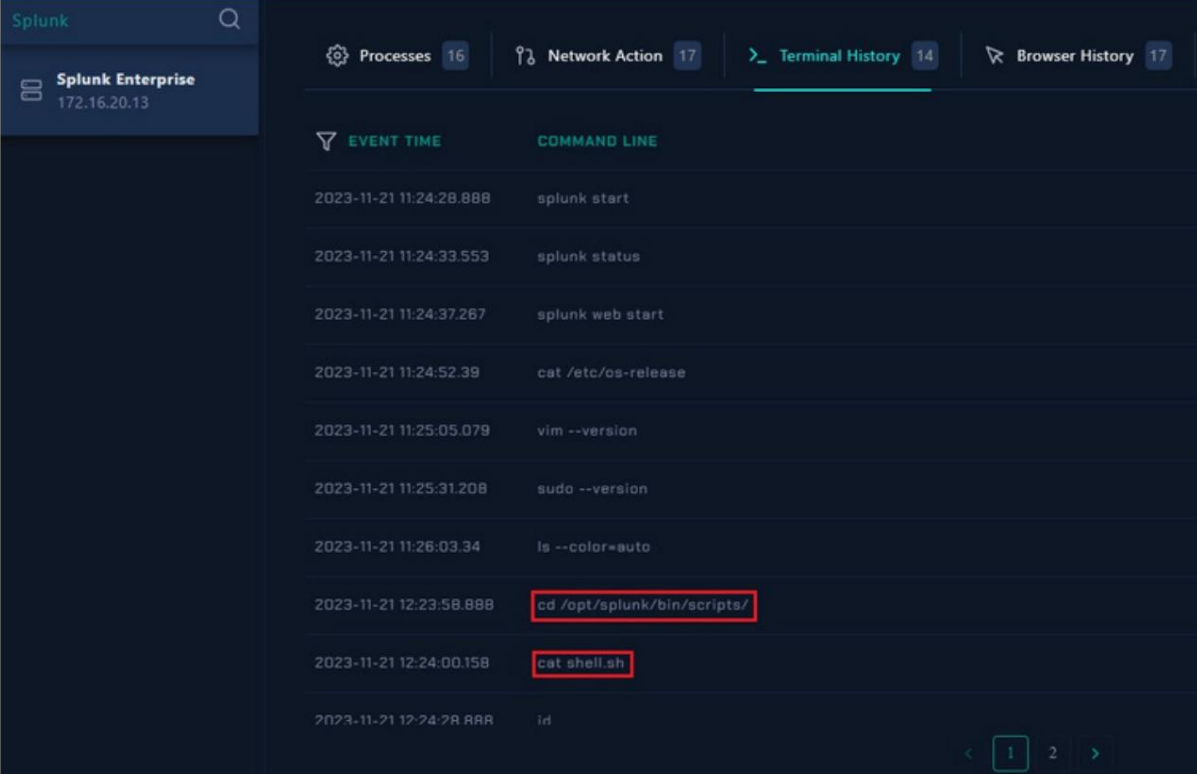
Username: admin
Source Process Name: bash
Target Process Name: passwd
Target Process Command Line: passwd analyst



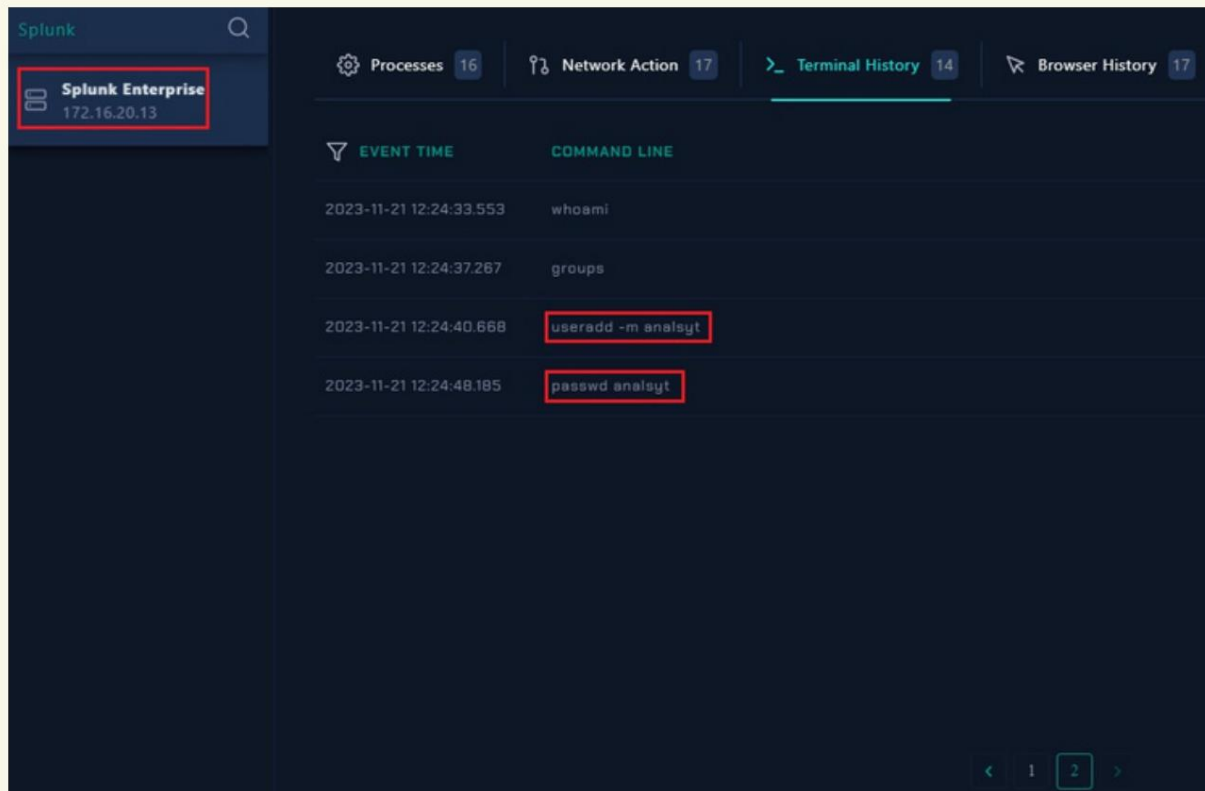
Asignación de contraseña

No hay ninguna situación sospechosa en los registros posteriores de DNS y Firewall de la IP correspondiente.

Lo último que hay que comprobar es el historial del terminal del host correspondiente. El propósito aquí es detectar las actividades del atacante en el sistema objetivo después de obtener acceso al sistema. Para esto, debes dirigirte a Endpoint Security.

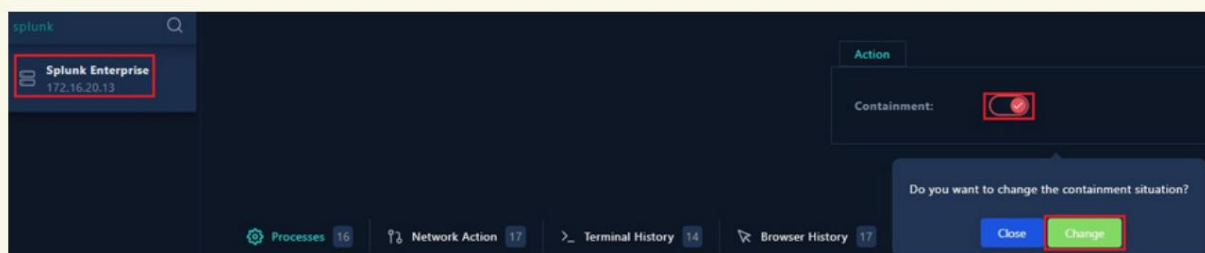


EVENT TIME	COMMAND LINE
2023-11-21 11:24:28.888	splunk start
2023-11-21 11:24:33.553	splunk status
2023-11-21 11:24:37.267	splunk web start
2023-11-21 11:24:52.39	cat /etc/os-release
2023-11-21 11:25:05.079	vim --version
2023-11-21 11:25:31.208	sudo --version
2023-11-21 11:26:03.34	ls --color=auto
2023-11-21 12:23:58.888	cd /opt/splunk/bin/scripts/
2023-11-21 12:24:00.158	cat shell.sh
2023-11-21 12:24:28.888	id



Contención

En los registros del proxy se detectó el intento del atacante de cargar "shell.xsl" en el sistema para explotar la vulnerabilidad "CVE-2023-46214" en Splunk. Posteriormente se pudo observar que el atacante recibió un proyectil inverso. Por tanto, se recomienda aislar el sistema de la red. La operación relevante se puede realizar en Endpoint Security de la siguiente manera.

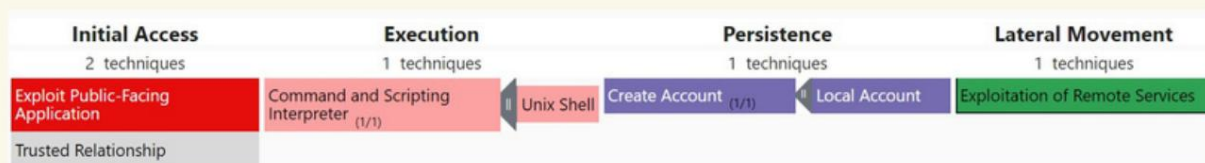


Lección aprendida

- Los productos deben mantenerse actualizados para evitar verse afectados por vulnerabilidades.
- Se recomienda no abrir Splunk to Remote para evitar verse afectado por vulnerabilidades.
- El acceso a empresas de terceros debe estar restringido.
- Se debe brindar capacitación periódicamente para aumentar la conciencia sobre la seguridad de la información entre los usuarios.
- Se pueden escribir reglas de detección en productos de seguridad para IOC reportadas con vulnerabilidades relevantes.

Apéndice

INGLETE



Artefactos

field	value
IPs	<ul style="list-style-type: none">• 180[.]101.88.240
files	<ul style="list-style-type: none">• shell.xsl• shell.sh
users	<ul style="list-style-type: none">• analysyt• admin
Host/IPs	<ul style="list-style-type: none">• Splunk Enterprise• 172.16.20.12• 3[.]133.116.124