KringleCon 2

The 12 Noobian Nights of Christmas

Holiday Hack 2019

OVERVIEW

Young cms19 had never heard of the KringleCon or Elf University that resides at the North Pole. But as she traveled to the land of snow and mystery she found herself entranced by such wonder at the sight of a land full of fun and intrigue. Her deductive skills were honed while memories of math and logic came flooding back. She fought a great campaign till the end when she froze on the hills of Mount Splunk. Luckily, before her final breath of the season she vowed to use the revival of the thaw of winter and the off-season to regroup and train, to build her skills, and return once again to the North Pole to help conquer any mysteries of the tundra.

GOALS

1. Have fun.
2. Solve some puzzles.

Outcome

Young cms19 learned so many new technologies, solved many puzzles, and unlocked key skills that will be essential in her off-season journey towards becoming a cybersecurity professional. Her knowledge of real world information security vulnerabilities deepened and new threat research topics were discovered. A valiant opening season with much anticipation for the new year and upcoming successes.

MILESTONES

Here are cms19's steps and observations along her journey.

Night 0 (exploration)

- Explored the quad, dormitory, and student union.

- Played the Frosty Keypad game by researching the first 1000 prime numbers and matching the hint values of:1,3,7 and one repeated number to several attempts before success.
    - Tried a few random attempts at the Key Generator without success before seeing hint
    - Researched first 100 prime numbers and realized starting in the 7000s was a better use of brute force
    - Resource: https://www.calculatorsoup.com/calculators/math/prime-numbers.php
- Then exited the game for the day while standing next to the fireplace in the student union.

Night 1 ("Challenge 1")

- Find the Turtle Doves - Find the missing turtle doves.
    a. Upon re-entering the game next day, standing next to the fireplace, immediately noticed the two Turtle Doves sitting by the Fireplace. I couldn't believe that was all to finding the Turtle Doves and wondered if they had been there when I exited the previous day.

Night 2 ("Challenge 2")

- Unredact Threatening Document - unredact a pdf file
    a. Noticed a letter image in quad.
    b. A Pdf document opened when image was clicked.
    c. Researched how to unredact a pdf and realized the tools recommended I didn't have access to.
    d. I downloaded the letter and tried to open it with Word and viewed random characters.
    e. Decided to upload pdf to Google drive to see if could use an add-on to unredact.
    f. Clicked on LetterToElfUPersonnel pdf in Google Drive and clicked open with Google Docs
    g. Resulting Google Doc document surprisingly showed the unredacted text of the pdf.
    h. Copied and submitted the requested info "What is the first word in ALL CAPS in the subject line of the letter?": DEMAND

Night 3 ("Challenge 3")

- Windows Log Analysis: Evaluate Attack - Using the event log data, identify the user account that the attacker compromised using a password spray attack.
    a. Download event log data Security.evtx file
    b. From hint suggestion of use gedit, performed download gedit
    c. Use gedit to open Security.evtx file - Failed to open, killed process.
    d. Researched other techniques to read evtx file and found python-evtx possibility
    e. Verified had python 2 installed using: python --version
    f. Tried to run pip install python-evtx unsuccessfully
    g. Downloaded source files for python-evtx directly
    h. Tried pip install python-evtx again unsuccessfully
    i. Researched how to install the files since there was no .exe or wizard for install
    j. Found that python-evtx required python 3

k. Installed python 3
l. Tried to run pip install python-evtx again unsuccessfully
m. Researched why pip wasn't working and had to install pip
n. Tried pip install python-evtx again unsuccessfully due to python3 error
o. Tried pip install python3-evtx again unsuccessfully
p. Researched why linux wasn't using python3 when installed
q. Ran alias python=python3
r. Installed python-evtx successfully using pip install python-evtx
s. Tried unsuccessfully to use evtx_dump.py to convert Security.evtx to Security.xml file using: python3 evtx_dump.py Security.evtx > Security.xml
t. Moved Security.evtx into same directory as evtx_dump.py
u. Ran evtx_dump.py successfully
v. Opened Security.xml file in gedit
w. Searched for compromised user account
x. Found TargetUserName value and entered first and several others usernames unsuccessfully
y. Searched for final log under TargetUserName and entered username successfully: supatree; realized that a password spray log might end when successful and thus be the last entry

Night 4 ("Challenge 4")

- Windows Log Analysis: Determine Attacker Technique - Using these normalized Sysmon logs, identify the tool the attacker used to retrieve domain password hashes from the lsass.exe process.
  a. Download sysmon-data.json file
  b. Use gedit to open sysmon-data.json
  c. Search for "lsass.exe" process in file

Night 5 ("Challenge 5")

- Network Log Analysis: Determine Compromised System - Can you help identify the IP address of the malware-infected system using these Zeek logs?
  a. Download and expand Zeek logs
  b. Looked through the zeek logs folder and noticed several types of files
  c. Researched zeek logs and read that a sha1 use is possible indication of malicious malware
  d. Using a linux grep through all zeek logs inspected files data for related IPs that proved unsuccessful
  e. Spend an enormous amount of time trying to solve the Xmas Cheer Laser to try to get the hint on how to read zeek logs
     i. Researched PowerShell
     ii. Use Get-History to see clue for how to set laser angle: (Invoke-WebRequest http://127.0.0.1:1225/api/angle?val=65.5).RawContent

iii. Use Get-Content to find Christmas Cheer Laser Project Web API info on how to set all laser options:

```
Christmas Cheer Laser Project Web API
-----------------------------------------------------
Turn the laser on/off:
GET http://localhost:1225/api/on
GET http://localhost:1225/api/off
Check the current Mega-Jollies of laser output
GET http://localhost:1225/api/output
Change the lense refraction value (1.0 - 2.0):
GET http://localhost:1225/api/refraction?val=1.0
Change laser temperature in degrees Celsius:
GET http://localhost:1225/api/temperature?val=-10
Change the mirror angle value (0 - 359):
GET http://localhost:1225/api/angle?val=45.1
Change gaseous elements mixture:
POST http://localhost:1225/api/gas
POST BODY EXAMPLE (gas mixture percentages):
O=5&H=5&He=5&N=5&Ne=20&Ar=10&Xe=10&F=20&Kr=10&Rn=10
```

iv. Easily perform the on, off, refraction, temperature, and angle commands and check output but never get correct result

v. Keep failing at gas POST multiple times and at correct search term to get successful attempt

vi. Finally search “powershell post to url” and get correct example to form POST:

```
$postParams = @{O=5;H=5;He=5;N=5;Ne=20;Ar=10;Xe=10;F=20;Kr=10;Rn=10}
Invoke-WebRequest -Uri http://127.0.0.1:1225/api/gas -Method POST -Body $postParams
```

vii. After many failed attempts to set laser, returned to zeek logs and noticed and ELFU folder hiding within the list of files

viii. Looked through the folder and saw two index.html files

ix. Opened the index.html files and found a database browser:

x. Tried and failed with the Source/Destination IP from Long Connections max/min duration thinking a long duration could mean lots of malicious connections are a short duration could also mean a malicious test connection

xi. Tried and failed with the Source/Destination IP from Beacons min score

xii. Tried the Beacons max score Source/Destination IP to successfully find the malware-infected system and reveal that the higher the Beacon score the more likely malicious activity is being executed.

Night 6 (“Challenge 6”)

- Splunk - What was the message for Kent that the adversary embedded in this attack?
  a. Log in to Splunk elf account and read chat clues to solve the 7 Training questions
     i. What is the short host name of Professor Banas' computer? Sweetums

1. Clicked on Search > Data Summary to see list of accounts

ii. What is the name of the sensitive file that was likely accessed and copied by the attacker? C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt
   1. Read clue about Santa and performed search: index=main santa
   2. Investigate first entry under results and see target file info under ParameterBinding(Format-List) field: value="C:\Users\cbanas\Documents\Naughty_and_Nice_2019_draft.txt

iii. What is the fully-qualified domain name(FQDN) of the command and control(C2) server? 144.202.46.214.vultr.com
   1. Read clue about Sysmon and do a Sysmon data search: index=main sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
   2. Investigate first entry under results and see the Example: badguy.baddies.com pattern under the <Data Name='DestinationHostname'> field

iv. What document is involved with launching the malicious PowerShell code? 19th Century Holiday Cheer Assignment.docm
   1. Perform the PowerShell logs data search: index=main sourcetype="WinEventLog:Microsoft-Windows-Powershell/Operational"
   2. Search oldest log by adding reverse to search: | reverse
   3. Apply a 10 second window by clicking on datetime of the first entry of results and clicking Apply on the +- 5 seconds default and re-perform original search with window applied and look through results Code 3, 4 events for two different process IDs
      a. Search first entry in results: Host ID c44dfd99-a4ba-452c-bf0d-07206a97112b and Runspace ID f01720e5-d340-460c-9184-31a3fc460a77
      b. Note DateTime on entry with message that PowerShell started: 5:18pm
   4. Next search Window Process execution events to find what launched the process: index=main sourcetype=WinEventLog EventCode=4688
      a. Click on block with timestamp 5:18pm to filter down to 7 related events
      b. Search entries for document name with Example: results.txt and find under Process Command Line field: C:\Windows\Temp\Temp1_Buttercups_HOL404_assignment (002).zip\19th Century Holiday Cheer Assignment.docm

v. How many unique email addresses were used to send Holiday Cheer essays to Professor Banas? 21
   a. Perform the stoQ search: index=main sourcetype=stoq | table _time results{}.workers.smtp.to results{}.workers.smtp.from results{}.workers.smtp.subject results{}.workers.smtp.body | sort - _time
   b. Count through the unique results in the results{}.workers.smtp.to field

vi. What was the password for the zip archive that contained the suspicious file? 123456789
   a. Search through the results{}.workers.smtp.body field of the previous results to see the zip file mention and the password in message

vii. What email address did the suspicious file come from? Bradly.Buttercups@elfu.org

a. Search results for the original email and reference the results{}.workers.smtp.from field for address

b. What was the message for Kent that the adversary embedded in this attack? <UNSOLVED>

i. Begin search for the hint 'results->payload_meta->extra_data->filename' field: index=main sourcetype=stoq | eval results = spath(_raw, "results{}") | mvexpand results | eval path=spath(results, "archivers.filedir.path"), filename=spath(results, "payload_meta.extra_data.filename"), fullpath=path."/".filename | search fullpath!="" | table filename,fullpath

ii. Find the entry for filename “19th Century Holiday Cheer Assignment.docm” and click on link to perform search: index=main sourcetype=stoq | eval results = spath(_raw, "results{}") | mvexpand results | eval path=spath(results, "archivers.filedir.path"), filename=spath(results, "payload_meta.extra_data.filename"), fullpath=path."/".filename | search fullpath!="" fullpath="/home/ubuntu/archive/c/6/e/1/7/c6e175f5b8048c771b3a3fac5f3295d2032524af/19th Century Holiday Cheer Assignment.docm"

iii. Search the results->archivers->filedir->path field and reference File Archive for first listed path, download file and use Gedit to read clue: “Cleaned for your safety. Happy Holidays!”

iv. Download and read second file for clue: “Cleaned for your safety. Happy Holidays! In the real world, This would have been a wonderful artifact for you to investigate, but it had malware in it of course so it's not posted here. Fear not! The core.xml file that was a component of this original macro-enabled Word doc is still in this File Archive thanks to stoQ. Find it and you will be a happy elf :-)”

v. Search for core.xml: index=main sourcetype=stoq | eval results = spath(_raw, "results{}") | mvexpand results | eval path=spath(results, "archivers.filedir.path"), filename=spath(results, "payload_meta.extra_data.filename"), fullpath=path."/".filename | search fullpath!="" "results{}.payload_meta.extra_data.filename"="core.xml"

vi. Search for core.xml: index=main sourcetype=stoq | eval results = spath(_raw, "results{}") | mvexpand results | eval path=spath(results, "archivers.filedir.path"), filename=spath(results, "payload_meta.extra_data.filename"), fullpath=path."/".filename | search fullpath!="" "results{}.payload_meta.extra_data.filename"="core.xml" and see same file dir paths as before - could not decipher message

Night 7 - 12+ (“Challenge 7 - 12”)

For the next several nights young cms19 traveled throughout the Pole in search of the passages to steam tunnels, master keys, sleighs bypasses, paper scraps, documents and weather data however she did not find the answers she sought. Alas, she was not discouraged and vowed to attempt the journey once more.