Real-Time Cyber Threat Detection and Mitigation - Assignment

➢ Question 1

- What are the harmful payload/s?

  Payload:

  - POST/http/page588633/autodiscover/admin@localhost//powershell/autodiscover.json?x=a HTTP/1.1\r\n

- What are the CVE and CWE number/s of the web application threats?

  CVE Number:

  - CVE-2019-3702: A Remote Code Execution issue in the DNS Query Web UI in Lifesize Icon LS_RM3_3.7.0 (2421) allows remote authenticated attackers to execute arbitrary commands via a crafted DNS Query address field in a JSON API request.

  CWE Number:

  - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

- Write the snort rules for the harmful payload.

  Sonort Rules:

  - alert: generates alarm as specified and logs the packet.
    alert tcp 44.193.255. 188 any -> 192.168.2.31/24 any (content: “THREAT”; msg: “WARNING”;)
  - log: logs the packet directly
    log tcp 44.193.255.188 any -> 192.168.2.31/24 any (content: “THREAT”; msg: “WARNING”;)
  - drop: blocks and saves the packet.
    drop tcp 44.193.255.188 any -> 192.168.2.31/24 any (content: “THREAT”; msg: “WARNING”;)
  - reject: blocks the packet, logs it, and generates an error message according to the protocol.
    reject tcp 44.193.255.188 any -> 192.168.2.31/24 any (content: “THREAT”; msg: “WARNING”;)
  - sdrop: blocks the packet and does not save it.
    sdrop tcp 44.193.255.188 any -> 192.168.2.31/24 any (content: “THREAT”; msg: “WARNING”;)

- Write the sigma rule for the detection of these payloads.

    - Sigma Rule:

        » title: PowerShell ShellCode
        » description: Detects Base64 encoded Shellcode.
        » references:
            - https://twitter.com/cyb3rops/status/1063072865992523776
        » status: experimental
        » date: 2023/01/15
        » logsource:
        » product: windows
        » service: powershell
        » description: Script block logging must be enabled
        » detection:
        » selection:
        » EventID: 4104
        » condition: selection
        » level: critical
        » falsepositives:
            - Unknown
        » tags:
            - attack.execution

    - For Elastic Query;

        » winlog.event_id:"4104"

    - For QRadar;

        » SELECT UTF8(POST/http/page588633/autodiscover/admin@localhost//powershell/autodiscover.json?x=a HTTP/1.1\r\n) FROM events WHERE LOGSOURCETYPENAME(devicetype)='Microsoft Windows Security Event Log' AND "EventID"='4104'

➢ **Question 2**

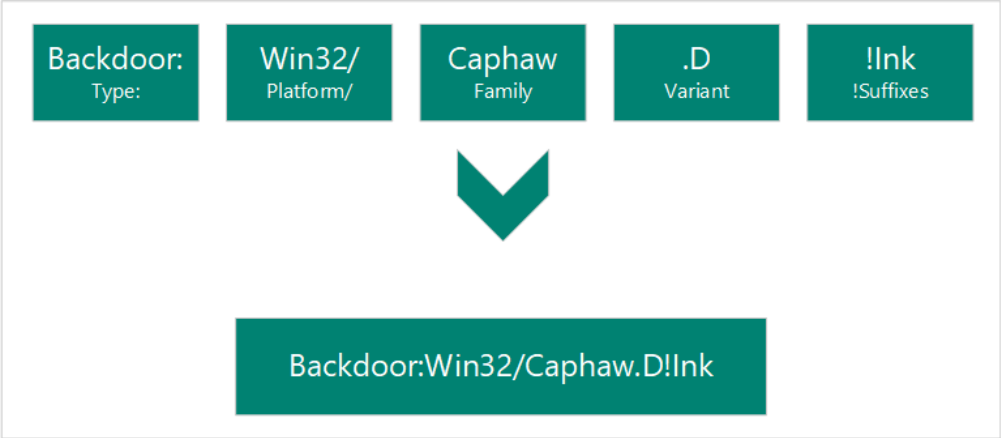
- What is the name of the malicious file/s downloaded by the accountant?

    - File Name: 217628___5020b7d2-306f-4d31-a65f-1c0dc2261c64.exe%3fprotocol=http

- What is the sha256 hash of the downloaded malicious file/s?

    - SHA 256: eb0a884d4eabc4f8811ecaa3e37acc8156c52b60a89537c5498df4c0e0c21f7

❖ **Note:** Malware names, according to Microsoft;



- What is the malware type of the malicious file/s?

    - Malware Type: Ransom

- What is the malware family of the malicious file/s?

    - Malware Family: Filecoder

- What are the used TTP/s according to the MITRE ATT&CK framework for malicious file/s?

    - Impact/ https://attack.mitre.org/tactics/TA0040/ - Data Encrypted for Impact/ https://attack.mitre.org/techniques/T1486/
    - Impact/ https://attack.mitre.org/tactics/TA0040/ - Inhibit System Recovery/ https://attack.mitre.org/techniques/T1490/
    - Defense Evasion/ https://attack.mitre.org/tactics/TA0005/ - Obfuscated Files or Information/ https://attack.mitre.org/techniques/T1027/
    - Command and Control/ https://attack.mitre.org/tactics/TA0011/ - Data Obfuscation/ https://attack.mitre.org/techniques/T1001/
    - Exfiltration/ https://attack.mitre.org/tactics/TA0010/ - Data Encrypted

    - Persistence/ https://attack.mitre.org/tactics/TA0003/ - Registry Run Keys / Startup Folder/ https://attack.mitre.org/techniques/T1547/001/

- What is the name of the malware/s, according to Microsoft?

    - Microsoft: Ransom:MSIL/Filecoder.ABL!MTB