Task 1

You know that on a client there is a malware installed that sends back data to an URL starting with https://www.malware123.example.com. Sometimes some latters of the URL can be in uppercase. Write a YARA Rule to find this malware executable on the system.

Solution 1

```
rule Detect_Malware123_Communication {
    strings:
        $url = "https://www.malware123.example.com" nocase

    condition:
        $url
}
```

Task 2

Explain the diffrence between a TGT and a Service Ticket (from TGS) in Kerberos

Solution 2

TGT: Its primary purpose is to prove the user's identity to the Ticket Granting Service (TGS) without needing to repeatedly send the user's password.

Service Ticket: Service Tickets are issued based on a valid TGT. Service tickets allow the user to access specific services or resources on the network without requiring further authentication

Task 3

What are the advantages and disadvantages from the attackers view of a sliver ticket attack over a golden ticket attack

Solution 3

Advantages

- Only requires the hash of the target service account, not the krbtgt account hash.
- Less likely to be detected, because the KDC is not attacked

Disadvantage

- Only a specific service can be attacked
- The exact service must be known before the attack

Task 4

What is always the case for a vulnerability with an CVSS Score of 10?

Solution 4

No user interaction is required, the attack can be performed over the network.

Task 5

What problem is solved with implementing a unique-id in a web request, and where to implement it.

Solution 5

Without a unique-id it's hard to correlate logs from diffrent systems that one web request went through (eg. WAF, Loadbalancer, Webserver). It needs to be implemented in the first system of which you recieve logs that recieves the request .

Task 6

What does the acronym IOC stand for in cybersecurity, and what role does it play in incident response?

Solution 6

IOC stands for "Indicator of Compromise." It represents evidence of potential intrusion into a system, such as malicious file hashes, unusual IP addresses, or specific registry changes. These indicators are used in incident response to identify, analyze, and mitigate security breaches.

Task 7

Write a Sigma Rule to detect unauthorized use of PowerShell commands that bypass execution policy.

Solution 7

```
 title: Detect PowerShell Execution Policy Bypass
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    CommandLine|contains:
      - "powershell"
      - "-ExecutionPolicy Bypass"
  condition: selection
fields:
  - CommandLine
  - User
  - ParentImage
falsepositives:
  - Administrators using the command legitimately
level: high
```

Task 8

Explain the process of a Golden SAML attack and its implications.

Solution 8

Golden SAML Attack Process:

1. The attacker obtains the private key of the Identity Provider (IdP).
2. The attacker forges a SAML token with arbitrary claims (e.g., roles or groups).
3. The forged SAML token is used to access any service that trusts the IdP.

Implications:

- The attacker can impersonate any user, including administrators.
- It bypasses MFA and other security measures relying on the IdP.

Task 9

What is the primary benefit of using asymmetric encryption over symmetric encryption for email communication?

Solution 9

Asymmetric encryption enables secure communication without the need to exchange a secret key beforehand. The sender encrypts the email using the recipient’s public key, ensuring only the recipient can decrypt it with their private key. This reduces the risk of key compromise during transmission.

Task 10

Why is DNS over HTTPS (DoH) considered a double-edged sword in cybersecurity?

Solution 10

Advantages:

- Encrypts DNS traffic, preventing eavesdropping and man-in-the-middle attacks.
- Enhances privacy by hiding DNS queries from ISPs and other intermediaries.

Disadvantages:

- Makes DNS-based network monitoring tools ineffective, complicating threat detection.
- Can be exploited by malware to bypass traditional DNS filtering mechanisms.