Threat Hunting with Wireshark

# Situation

Your organization recently suffered a data breach from an attacker inside the network. We don’t know how they got in, but they obtained an IP address in the local subnet and have compromised at least one workstation and possibly a server. We need to know:

1. What workstation the attacker compromised
2. The attack vector used and any associated users or credentials.
3. What was taken (if anything)
4. Is the attacker still on the network or have they left a backdoor?
5. Do we expect another attack?
6. How can we prevent this **internal** attack from happening again?

# Information

**Attacker –** 10.10.0.7

**Victim –** 10.10.0.4

## Helpful Hints

The attack took place quickly, and we know that there is little extra traffic. It seemed like the attacker knew what to look for and acted quickly.

The system attacked was in dev, and had encryption turned off for most services, meaning we are likely able to read traffic in the clear.

The new developer has not had a chance to harden the dev system and has been out on vacation for a few days.

The plan for the service is to deploy an IIS front-end that serves as a web-based file-share

# Resources

* What is SMB? What IT Decision Makers Need To Know | Visuality Systems - <https://visualitynq.com/resources/articles/what-is-smb-what-it-decision-makers-need-to-know/>
* Microsoft SMB Protocol Authentication - Win32 apps | Microsoft Learn - <https://learn.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-authentication>
* SMB - <https://wiki.wireshark.org/SMB>
* SMB2 - <https://wiki.wireshark.org/SMB2>

# Sections

## Part 1 – Observations

### Questions

#### 1.1 | What is the victim’s hostname?

#### 1.2 | What type of host is the other endpoint on the local 10.10.0.0/24 subnet?

#### 1.3 | Are there any objects you can export right away?

#### 1.4 | What is the most likely attack vector?

#### 1.5 | What is the *Wireshark* filter for NT Status: STATUS\_SUCCESS in both SMB and SMB2

#### 1.6 | What is the *Wireshark* filter to detect *Write* activity on the SMB2 protocol?

### Notes

## Part 2 – Scanning and Enumeration

### Questions

#### 2.1 | What indicators exist that this **pcap** starts with a “*nmap”* scan?

**Bonus**: When did the **protocol-specific scan** start and what protocol was queried?

**Bonus**: Would you consider this a **"targeted" scan?** Why or Why Not?

#### 2.2 | What is an indicator that the username that started a **negotiation request** in **Packet 127** is successful?

#### 2.3 | What **username is used to enumerate** the shares on the target?

#### **2.4 | What shares exist** on the target, and **which were access granted** to?

#### 2.5 | Can the **client write shares** to the server?

#### 2.6 | What common type of plant name is used to indicate a client (attempted) to connect to a share in the *Wireshark* “info” column?

**Bonus:** Provide **any or all** the following:

1. The “OpCode” for the answer in **SMB2**.
2. Display-filter expression to list only packets containing the answer in **SMB2**.

### Notes

## Part 3 – Compromising the Victim

#### 3.1 | How many packets take place between the “Time” 315.861028 and 317? (Round to the nearest hundred)

#### 3.2 | What is/are the **most common type of SMB command(s)** in this short period*? (Hint: smb.cmd, smb.cmd == […something])*

#### 3.3 | **What type of attack** does this look like?

#### 3.4 | **What "Session Setup Response" packet and “stream” number** are part of the successful login attempt and what is the username?

#### 3.5 | **Why can’t we see a password**, even though the session setup is unencrypted?

### Notes

## Part 4 – Data Exfiltration

#### 4.1 | What is the name of the “Tree” the attacker connected to (including the IP and formatting) to perform their objectives?

**Bonus:** What is the command the attacker could have used with ***smbclient*** to connect to the attacker assuming the same IP as is in the pcap?

#### 4.2 | What is the significance of the “KeepAlive” requests and responses between the attacker and victim?

#### 4.3 | What is the **name of the file** the attacker reads?

**Bonus:** What does it tell the attacker they can expect to find on the share?

**Bonus:** Can you find and decode the encoded “Data” that represents the text document?

#### 4.4 | What is the **name and the type of file** exfiltrated from the victim?

**Bonus:** What SMB command was used on the client side to get the file onto their system?

#### 4.5 | What are the **“OpCodes” for the following SMB2 commands** and use one in an example display-filter

1. *Find* –
2. *Create* –
3. *GetInfo* –
4. *Read* –
5. *Close* –
6. Filter Example –

### Notes

## Part 5 – Second Foothold

#### 5.1 | What is the **name of the webshell** uploaded by the attacker?

#### 5.2 | What is the **common command name (e.g., read, create), packet number, and opcode Hex number** for the command used to place the file on the system?

1. *Common Name* –
2. *Packet Number* –
3. *OpCode (in hex)* –
4. **Bonus:** What was the **SMB command** used to “place” the file on the system?

When the attacker next connects, what port and service are they connecting to, and over what Layer 7 **protocol**?

#### 5.3 | WHEN THE ATTACKER NEXT CONNECTS, **WHAT PORT AND SERVICE ARE THEY CONNECTING TO**, AND OVER WHAT LAYER 7 protocol?

#### 5.4 | What is the **name of the user** the attacker is running commands as in the webshell?

#### 5.5 | What are **the three “enabled” privileges** available to the attacker?

**Bonus:** What is one or more publically available exploit associated with ***SeImpersonatePrivilege***?

### Notes

# Student Summary

To record the engagement in your own words, practice writing a summary, and work through the “key findings” of the engagement, please answer the questions below. Most can also be supplemented with what potential remediations exist.

#### What overall security flaws allowed the attacker to enumerate the shares on the victim?

#### What specific vulnerability allowed the attacker to gain read/write access to the share?

#### Why could we read the exfiltrated data in plain text? What major security flaw does this implicate is present on the system?

#### How did the attacker move to a different service on the system?

#### What would the inevitable consequences of the attacker exploiting the privilege found in question 6.5? What is this type of attack called?