smbtimeline

A journey from a 'should be 2 hours'-project to a little bit more work.
Who am I?

- Olaf Schwarz
- Austrian Energy CERT / CERT.at
  - https://github.com/AustrianEnergyCERT/ICS_IoT_Shodan_Dorks/
- Incident Handling, Forensics
- Member of BSidesVienna Crew
- Twitter: @b00010111
What you will not see today

- Game Changers
- One thing solving all your DFIR Challenges
What will be discussed today

- Admissions
  - I can not remember everything I once learned
  - I’m lazy
What will be discussed today

- Admissions
  - I can not remember everything I once learned
  - I’m lazy – efficient
What will be discussed today

- Admissions
  - I can not remember everything I once learned
  - I’m lazy – efficient
- Lowering the bar
But why SMB?

- Project to learn something
- Living of the land
  - Use tools & functionality native to system
  - Use tools & functionality already present on system
- Named pipes used in recent cases or by usual suspects
  - Turla/Snake
  - PsExec
- Remote Procedure Call & Distributed Computing Environment
Analysis Examples

- Wireshark – SMB V1-3 between two hosts
Wireshark – SMB V1-3 read + filename
Analysis Examples

- Wireshark – Flow-Graph
Analysis Examples

- TShark – SMB V1-3 Usernames
Analysis Examples

- TShark – Export of SMB filenames

```bash
$ tshark -n -r test.pcap -E separator="," -E quote=d -T fields -e smb.file -e smb2.filename | sort | uniq
```
○ Manually entering leads / findings into your timeline
Manually entering leads / findings into your timeline
Analysis Examples – next step

- Manually entering leads / findings into your timeline
  - No fun at all.
  - Inefficient
  - You should investigate and not ...
smbtimeline Features – overview

- CSV based timeline for SMB Version 1 traffic
- CSV based timeline for SMB Version 2 and 3 traffic
- Combined timeline in log2timeline CSV output format
- Strip out SMB traffic from larger pcap
- Generates a protocol
- Enrichments
Simple csv timeline

Fields:
- Packet & tcp stream id
- Packet date/time
- src & dst ip/port
- Parsed SMB command
- Account / Domain
- Filename & Path
- Service / Registry info
- info field
- ...

smbtimeline Features – csv timeline
smbtimeline Features – csv timeline

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> cd D:\smbtimeline\nPS D:\smbtimeline> C:\Users\olafs\AppData\Local\Programs\Python\Python37\python.exe .\smbtimeline.py -1 -f .\test.pcap

checking os
checking for tshark
running filter: smb_filter
parsing tshark output to timeline for smb_filter
smbtimeline Features – csv timeline

PS D:\smbtimeline> C:\Users\olafs\AppData\Local\Programs\Python\Python37\python.exe \smbtimeline.py -2 -f .\test.pcap

checking os
checking for tshark
running filter: smb2_filter
parsing tshark output to timeline for smb2_filter
smbtimeline Features – csv timeline

PS D:\smbtimeline> C:\Users\olaf\AppData\Local\Programs\Python\Python37\python.exe .\smbtimeline.py -2 -f \test.pcap
checking os
checking for tshark
running filter: smb2_filter
parsing tshark output to timeline for smb2_filter

PS D:\smbtimeline> C:\Users\olaf\AppData\Local\Programs\Python\Python37\python.exe .\smbtimeline.py -1 -2 -f \test.pcap
checking os
checking for tshark
running filter: smb2_filter
parsing tshark output to timeline for smb2_filter
running filter: smb_filter
parsing tshark output to timeline for smb_filter
smbtimeline Features – csv timeline

- Limitations:
  - It is an overview
  - Fully depending on the parsing of Wireshark / TShark
  - Wireshark / TShark csv output has limitations
  - Most of the defined SMB commands
Limitations:
- It is an overview
- Fully depending on the parsing of Wireshark / TShark
- Wireshark / TShark csv output has limitations
- Most of the defined SMB commands
- Not considered:
  - SMBv1: deprecated, obsolescent or obsolete commands
  - SMBv1: 'FLUSH', 'ECHO', 'FIND_CLOSE', 'NT_CANCEL', 'OPEN_PRINT_FILE', 'INVALID', 'NO_ANDX_COMMAND'
  - SMBv2: 'CANCEL', 'ECHO', 'CHANGE_NOTIFY', 'OPLOCK_BREAK'
smbtimeline Features – log2timeline

- log2timeline CSV output format
- Combined timeline for all SMB Versions
- Based on already enriched timeline
Limitations:
- MACB Strings vs. Network traffic
- Session establishment == -A-- ?
- Especially MACB Strings needs further validation and practice tests
smbtimeline Features – log2timeline

- **Format (some of the obvious once):**
  - Date
  - Time
  - Timezone
  - MACB – String
  - Source
  - Sourcetype
  - User
  - Host
smbtimeline Features – log2timeline

- **Format (less obvious once):**
  - **Type**
    - human readable SMB Command + Request | Response
  - **Short**
    - Type-Field + ip.src : srcport -> ip.dst : dstport
  - **Desc**
    - if present: search pattern, registry info, ...
  - **Extra**
    - Number of Packet/Frame, TCP Stream, Response_to, ...
smbtimeline Features – strip

- **Strip off non SMB traffic**
  - New temporarily pcap only containing SMB traffic
  - Only new file processed for timeline
  - Filter: (port 445 or portrange 137-139)
smbtimeline Features – protocol

- Protocol
  - smbtimeline version
  - Platform
    - TShark / Wireshark version used
    - TShark / Wireshark filter used
    - Limitations & explanations
  - csv timeline => log2timeline output mapping
  - No hash of the pcap file!
SMB 1 carries DCE/RPC in SMB Transport
SMB 2/3 carries DCE/RPC in SMB ioctl, read, write
“Sub-protocols” enrichment for
   SAMR, LSAD, SRVS, WKST, WINREG, SCMR, ATSVC
   Fills the ‘info’ field & adds information to ‘smb_action’ field
SMB 1 carries DCE/RPC in SMB Transport
SMB 2/3 carries DCE/RPC in SMB ioctl, read, write
“Sub-protocols” enrichment for
  SAMR, LSAD, SRVS, WKST, WINREG, SCMR, ATSVC
  Fills the ‘info’ field & adds information to ‘smb_action’ field
  'winreg.opnum == 15' vs. 'smb_action: smb_transaction BaseRegOpenKey'
  + 'info:opens specified key for access, returning handle'
smbtimeline Features – "Sub-protocols"

- **SAMR**
  - "Security Account Manager (SAM) Remote Protocol (Client-to-Server)"
  - Management functionality for account store or directory
    - samr.opnum == 12 -> SamrCreateUserInDomain
    - samr.opnum == 35 -> SamrDeleteUser
    - samr.opnum == 38 -> SamrChangePasswordUser
smbtimeline Features – "Sub-protocols"

- SRVS
  - "Server Service Remote Protocol"
  - Enable file & printer sharing, enable named pipes access
    - srvsvc.opnum == 14 -> NetrShareAdd
    - srvsvc.opnum == 28 -> NetrRemoteTOD
WINREG

- "Windows Remote Registry Protocol"
- Manage Windows registry remotely
  - winreg.opnum == 7 -> BaseRegDeleteKey
  - winreg.opnum == 15 -> BaseRegOpenKey
  - winreg.opnum == 2 -> OpenLocalMachine
SCMR
  "Service Control Manager Remote Protocol"
  Service configuration & control of service programs
    svcctl.opnum == 12 -> RCreateServiceW
    svcctl.opnum == 31 -> RStartServiceA
smbtimeline Features – "Sub-protocols"

- ATSvc
  - "Task Scheduler Service Remoting Protocol"
  - Get info, register and configure a task on remote machine
    - atsvc.opnum == 0 -> NetrJobAdd
smbtimeline Features – "Sub-protocols"

- LSAD
  - "Local Security Authority (Domain Policy) Remote Protocol"
  - Machine and domain security policies management
    - $\text{lsarpc.opnum} == 10 \rightarrow \text{LsarCreateAccount}$
    - $\text{lsarpc.opnum} == 19 \rightarrow \text{LsarAddPrivilegesToAccount}$
A few things I learned about SMB traffic & wireshark

- SMB commands not unique between smb 1 & smb 2/3
- Wireshark field names smb.XX smb2.XX
- Wireshark field names not always the same
  - smb.file vs. smb2.filename
  - smb.account vs. smb2.acct
  - winreg_OpenKey.keyname vs. winreg_CreateKey.name vs. winreg_LoadKey.keyname
- Packets can carry more than one SMB command
- Wireshark csv output vs. one packets 2 commands
Demo?
- [https://github.com/00010111/smbtimeline](https://github.com/00010111/smbtimeline)

---

**smbtimeline**

*An automated timeline for SMB Traffic*

smbtimeline is a tool to produce a timeline out of SMB traffic. Inspired by the manually work of putting together an investigative timeline from SMB traffic, its purpose is to provide a timeline from a given pcap file. Particularly as Incident Response is about to focus on the right amount of details at the right time, smbtimeline provides an overview about the SMB traffic and not showing every possible bit of information but still enriching packets with useful details. In order to archive this goal, smbtimeline arranges not only SMB commands, but also important commands taken from protocols which utilize SMB as transport medium, in an easy to handle .csv file.

**Supported RPC/DCE protocols transported by SMB**

SAMR, LSAD, SRVS, WKST, WINREG, SCM, ATSVC
License

- Free for use, redistribution and reuse
- No limitations
- Attribution would be nice if you reuse
License – why no limitations?

- Learning project
- Spare time project
- Contribution to the DFIR community
- I would not be where I'm today without free content of others
- If someone wants to steal the idea/code.. I will not be able to prevent it
Next to come

- Native plaso output?
- Output for other timeline tools?
- Refactoring: switch from csv output to json output?
Questions
Chuck Norris can delete the Recycle Bin ... permanently.