DFLABS
CYBER INCIDENTS UNDER CONTROL

Threat Hunting Using Live Forensics

SANS Threat Hunting and IR Summit, 2018

Why Live Forensics?

- Need to acquire/preserve volatile artifacts
  - Running processes
  - Network connections
  - Open files
  - Hooks
- System cannot be shut down

Threat Hunting vs. IR

- IR starts with a pivot point
  - AV alert
  - Network connection
  - Data breach
  - Abnormal behavior
- Threat hunting seeks abnormal to pivot from

Signs of Evil

- Some things are bad no matter who you are
  - Misnamed processes
  - Running from abnormal directories
  - Connections to known-bad hosts
  - Abnormal process owners
- SANS Find Evil Poster: *https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf*

Signs of Evil

- Some things are more subtle
  - Unauthorized processes/services/tasks
  - Odd ports in use
  - Code injection/hooks
  - User actions
- Establish baselines – know what is normal!

Challenges for Live Forensics

- Live forensics tools must be run in a way that is…
  - ✓Documented
  - ✓Repeatable
  - ✓Secure
- Normally achieved via batch files on Windows hosts

So What’s Wrong with Batch Files?

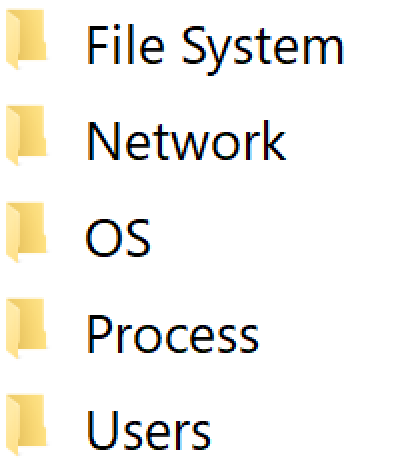
- No native logging or audit trail
- Some tools are OS or CPU architecture specific
- Batch files can be easily modified without warning
- Tools can be deleted or replaced

No-Script Automation Tool

- No scripting (obviously) required
- Easy to configure for different Windows versions and CPU architectures
- Detailed logging and hashing of all output
- Tools and commands can be verified before execution

Configuring NAT

Configuring NAT – Tools



File System

Network

OS

Process

Users

Tools Directory

File System
Network
OS
Process
Users

*.ini file

Configuring NAT – OS and CPU

- File System
  - 6-10.0
    - x64
    - x86
- Network
  - x86
  - x64
- OS

→ *Windows 7 x64*

- **File System**
  - **6-10.0**
    - **x64**
    - x86
- **Network**
  - x86
  - **x64**
- **OS**

Configuring NAT – Command Line Arguments

Network\ping.exe + Network\ping.exe.cmd

- *Only* command line args
  - Ex: -t -f 127.0.0.1, *not* ping.exe -t -f 127.0.0.1
- One execution per line
- End with blank line

Configuring NAT – Command Line Arguments

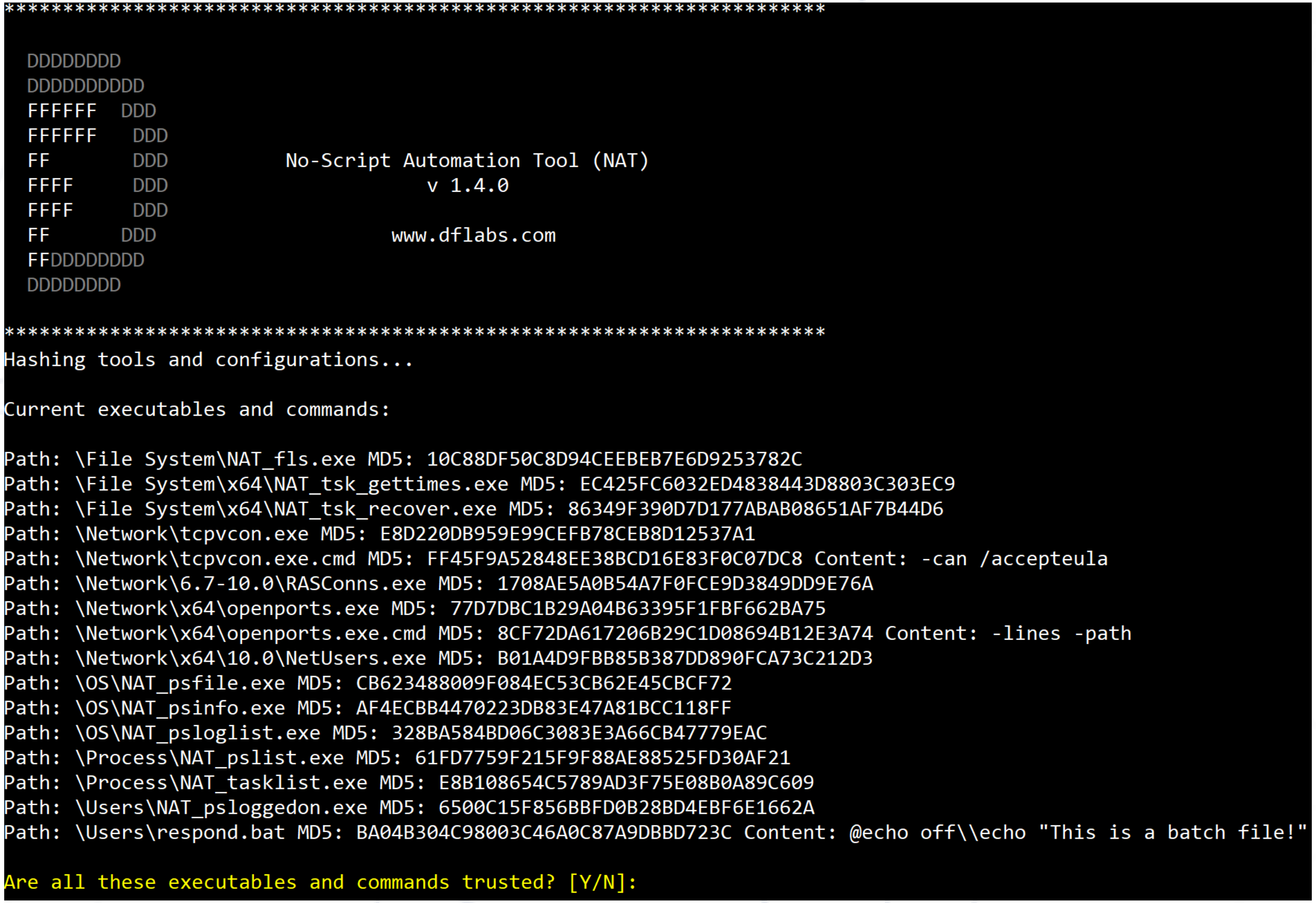
Variable	Use
%NOOUT%	By default, output from each tool will be written to a text file in the output directory specified at runtime. To prevent this for a specific tool, use the variable %NOOUT% as the sole argument in the .cmd file, or at the end of each line of command line arguments if other arguments are specified. This can be used when the output directory is specified as part of the command line arguments for the tool.
%OUTDIR%	To specify the output directory as part of the command line arguments, use the variable %OUTDIR% in place of the output directory. This variable will be dynamically replaced with the correct output directory each time the tool is executed. For example, "-o %OUTDIR%\output.txt" for mytool.exe will result in the command “mytool.exe -o <selected output directory>\output.txt being executed at runtime.
%SYSROOT%	To specify the Windows system root, which may vary between hosts, use the %SYSROOT% variable.

Configuring NAT – Integrity File

NAT.exe -c

- Hash of tools/commands, contents of commands
- Password protected, AES-256
- Bypass with -x switch

Configuring NAT – Integrity File



```
**********************************************************************

  DDDDDDDD
  DDDDDDDDDD
  FFFFFF  DDD
  FFFFFF   DDD
  FF       DDD          No-Script Automation Tool (NAT)
  FFFF     DDD                      v 1.4.0
  FFFF     DDD
  FF      DDD                    www.dflabs.com
  FFDDDDDDDD
  DDDDDDDD

**********************************************************************
Hashing tools and configurations...

Current executables and commands:

Path: \File System\NAT_fls.exe MD5: 10C88DF50C8D94CEEBEB7E6D9253782C
Path: \File System\x64\NAT_tsk_gettimes.exe MD5: EC425FC6032ED4838443D8803C303EC9
Path: \File System\x64\NAT_tsk_recover.exe MD5: 86349F390D7D177ABAB08651AF7B44D6
Path: \Network\tcpvcon.exe MD5: E8D220DB959E99CEFB78CEB8D12537A1
Path: \Network\tcpvcon.exe.cmd MD5: FF45F9A52848EE38BCD16E83F0C07DC8 Content: -can /accepteula
Path: \Network\6.7-10.0\RASConns.exe MD5: 1708AE5A0B54A7F0FCE9D3849DD9E76A
Path: \Network\x64\openports.exe MD5: 77D7DBC1B29A04B63395F1FBF662BA75
Path: \Network\x64\openports.exe.cmd MD5: 8CF72DA617206B29C1D08694B12E3A74 Content: -lines -path
Path: \Network\x64\10.0\NetUsers.exe MD5: B01A4D9FBB85B387DD890FCA73C212D3
Path: \OS\NAT_psfile.exe MD5: CB623488009F084EC53CB62E45CBCF72
Path: \OS\NAT_psinfo.exe MD5: AF4ECBB4470223DB83E47A81BCC118FF
Path: \OS\NAT_psloglist.exe MD5: 328BA584BD06C3083E3A66CB47779EAC
Path: \Process\NAT_pslist.exe MD5: 61FD7759F215F9F88AE88525FD30AF21
Path: \Process\NAT_tasklist.exe MD5: E8B108654C5789AD3F75E08B0A89C609
Path: \Users\NAT_psloggedon.exe MD5: 6500C15F856BBFD0B28BD4EBF6E1662A
Path: \Users\respond.bat MD5: BA04B304C98003C46A0C87A9DBBD723C Content: @echo off\\echo "This is a batch file!"

Are all these executables and commands trusted? [Y/N]:
```

Running NAT

Running NAT – Options

Argument	Use
-h	Display help menu and exit
-x	Bypass integrity check
-c	Create integrity check file
-I <file>	Use the specified .ini file (default is default.ini)

Demo

DFLABS
CYBER INCIDENTS UNDER CONTROL

Final Notes

- Free – Use at your own risk!
- Download:

  www.dflabs.com/NAT

- Questions, comments, suggestions, memes, etc:

  john.moran@dflabs.com

Questions?

Thanks!

www.dflabs.com/NAT

John Moran
Senior Product Manager, DFLabs
john.moran@dflabs.com

DFLABS
CYBER INCIDENTS UNDER CONTROL