

The Snapshot

When faced with an unknown potential computer security event it is important to gather as much information as possible to aid in determining whether the computer has actually been compromised.

Using the snapshot tool within Nigilant32 a first responder can gather information from multiple sources within the active system, including:

- System Information
- Processes
- User Accounts
- Network Connections
- Services and Drivers
- AT Scheduled Tasks

While there are already numerous tools available to capture this information, each tool works differently. Some tools provide command line output, others require specific commands to save the output. In addition, certain tools must be copied to the system prior to execution, potentially damaging the quality of the potential evidence.

It is for this reason that we developed Nigilant32.

Nigilant32 is an incident response tool designed to capture as much information as possible from a running system with the smallest potential impact. Nigilant32 has been developed with Windows 2000, XP, and 2003 in mind, and should work fine with computers running one of those operating systems.

Using Nigilant32 we can review and save a report of the running system that includes all the information highlighted above

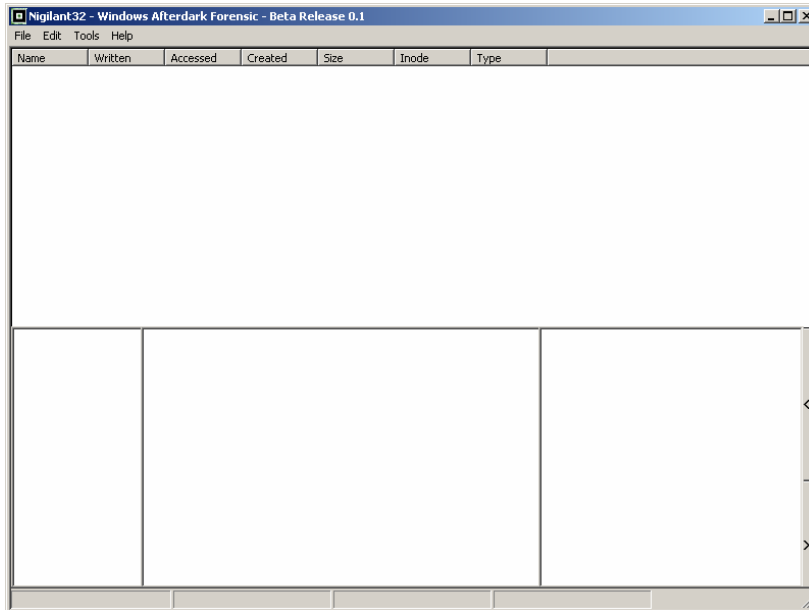
Let's look at an example.



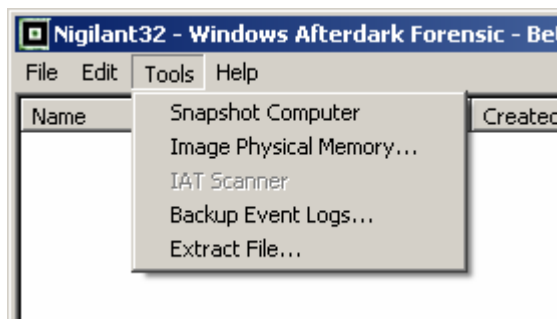
The Nigilant32 main console

This article is the first in a series of publications developed to assist the first responder in understanding the many uses of Nigilant32 <n-eye-jill-ant32> in an incident response capacity. In this article we cover the snapshot report.

Nigilant32 was developed by Agile Risk Management LLC, the most recent and update to date version can always be found at www.agilem.net.



In order to obtain a system snapshot, let's look at the Tools Menu.



The Tools menu will be adjusted over time as new tools and technologies are added.

The Snapshot Computer option will use both documented Win32 API commands, as well as undocumented system functions to obtain active system information.

Let's review the output of the Snapshot Computer command.

The report begins with a System Information Listing..

```

-----System Information Listing-----
OEM ID: 0
Number of processors: 1
Page size: 4096
Processor type: 586
Minimum application address: 10000
Maximum application address: 7ffefff
Active processor mask: 1

```

In this case we see that the active computer has one processor, a memory page size of 4096 bytes, minimum and maximum application memory addresses for application data, as well as active processor mask and type.

Following the system information we see the current logged-in username and machine name.

-----User/Machine Information Listing-----

User Name:Administrator
System Name:WIN2K-SP4

Next the report provides us a listing of the currently running processes. It would be naïve to assume that rootkit technology will be unable to hide processes from Nigilant32. The tools and techniques used by rootkits are changing rapidly and a universal and well regarded method has yet to be developed to ensure a proper recording of all processes. Nigilant32 will be modified to include new process detection mechanisms as they become available.

-----Process Listing-----

Priority Class Base:0
PID: 0
Thread Count: 1
Module ID: 0
Module Name:
Proces EXE File: [System Process]

Full Path:

Priority Class Base:8
PID: 8
Thread Count: 32
Module ID: 0
Module Name:
Proces EXE File: System

Full Path:

Priority Class Base:11
PID: 140
Thread Count: 6
Module ID: 0
Module Name: smss.exe
Proces EXE File: SMSS.EXE

Full Path: \SystemRoot\System32\smss.exe

...

At the end of the process listing we will see a listing of the total active memory on the system, both page file and physical memory.

-----Memory Usage-----

Memory Load: 28
Total Physical: 267894784
Available Physical: 191037440

Total Page File:	648314880
Available Page File:	578154496
Total Virtual:	2147352576
Available Virtual:	2121568256

Next the report will contain the current Operating System and Platform, in this instance we have Windows 2000 Professional.

-----OS Information-----

Operating System: Windows 2000
Operating System: Professional

Nigilant32 also provides a listing of the Network devices on the system, as well as their current address, gateway, and netmask.

-----Network Devices-----

Network Adapter Name: AMD PCNET Family Ethernet Adapter
IP Address: 172.16.10.12
Network Mask: 255.255.255.0
Gateway Address: 172.16.10.1
Gateway Network Mask: 0.0.0.0
Physical Address: 000c29540e88

Following the network device listing we are provided a listing of the current user local user accounts on the system. Often a compromise will result in the creation of new user accounts, such as "test" or "backup". An attacker may use these accounts to access the system in a more conventional manner.

-----Local System User Accounts-----

Name: Administrator
Comment: Built-in account for administering the computer/domain
Full Name:
RID: 500

Name: Guest
Comment: Built-in account for guest access to the computer/domain
Full Name:
RID: 501

Next Nigilant32 presents a listing of the ports and processes open on the system. It provides us with the Process Name, Protocol, IP, and in some cases, Handle Number. The Handle number is assigned by the operating system and is used to keep track of network ports and processes. We can use the information provided to locate open ports and processes that were unauthorized or are not part of our standard configuration.

-----Current Network Ports and Processes-----

Handle Number: 112
Local IP: 172.16.10.12:139
Protocol:[TCP]
Process:System

The way in which network processes and ports information is displayed will vary by operating system.

Handle Number: 116
Local IP: 172.16.10.12:139
Protocol:[TCP]
Process:System

Handle Number: 124
Local IP: 172.16.10.12:139
Protocol:[TCP]
Process:System

Handle Number: 128
Local IP: 172.16.10.12:139
Protocol:[TCP]
Process:System

Handle Number: 132
Local IP: 172.16.10.12:137
Protocol:[UDP]
Process:System

Handle Number: 136
Local IP: 172.16.10.12:138
Protocol:[UDP]
Process:System

Handle Number: 164
Local IP: 0.0.0.0:445
Protocol:[TCP]
Process:System

Handle Number: 172
Local IP: 0.0.0.0:445
Protocol:[UDP]
Process:System

One of the final items provided is an enumeration of the services found on the system. This list includes both traditional software services such as “WinLogon” and “Internet Information Services” as well as drivers such as “Microsoft ACPI Driver” and “Abiodsk”. Often a compromised system will contain unauthorized services, some of these can be used to provide the attacker with additional access.

-----Services Enumeration-----

Service Display Name: Abiodsk
Service Name: Abiodsk
Binary Path:
Process Id: 0
Service Start Type:Service Disabled

Service Display Name: abp480n5
Service Name: abp480n5
Binary Path:
Process Id: 0
Service Start Type:Service Disabled

Service Display Name: Microsoft ACPI Driver
Service Name: ACPI
Binary Path:\SystemRoot\System32\DRIVERS\ACPI.sys

Service enumeration includes both traditional services and drivers.

Process Id: 0
Service Start Type:Driver On-Boot Start

Service Display Name: ACPIEC
Service Name: ACPIEC
Binary Path:
Process Id: 0
Service Start Type:Service Disabled

Service Display Name: adpu160m
Service Name: adpu160m
Binary Path:
Process Id: 0
Service Start Type:Service Disabled

Lastly, Nigilant32 enumerates an “AT” scheduled tasks. These are scheduled tasks assigned using the AT command line tool. Often attackers use AT to schedule listening processes or outbound shell forwarding using Netcat (“nc.exe”).

-----AT Scheduled Tasks Enumeration-----

No AT Scheduled Tasks Found.

This provides a summary of the information available in a Nigilant32 Snapshot report. As we detailed earlier, this information can be used as part of an incident response project, however with the rapid advance of rootkit and subversion technologies, the data provided in this report should be reviewed carefully and corroborated with other information sources wherever possible.

Matthew Shannon has over seven years of professional experience in private industry, including KPMG LLP, ExxonMobil, and United Technologies. Mr. Shannon has successfully led multiple information security assessment engagements, including successful penetration of multi-million dollar financial institutions, both international and domestic. In addition, Mr. Shannon has been the lead investigator on numerous computer forensics engagements, including intellectual property theft and employment law. Mr. Shannon is also a well received speaker and author. He has instructed the United States Secret Service on specific digital forensics techniques and was a well received speaker at the DEFCON 11 annual Information Security conference in Las Vegas Nevada. Additionally, Mr. Shannon has been published in the International Journal of Digital Evidence for his work on incorporating statistical inference into digital forensics investigations as well as multiple bar journal articles and online digital forensics publications.

Mr. Shannon graduated cum laude from The University of Florida in Decision and Information Sciences (BSBA) in 1999. He is a member in good standing of ISSA, in addition, Matthew holds numerous professional information technology certifications, and is the developer of Nigilant32, Agile Risk Management LLC's Incident Response Tool.

Matthew M. Shannon CIFI,
CISSP
Principal
Agile Risk Management LLC
mshannon@agilerm.net