

Using WinReporter[®] to perform security audits on Windows[™] networks

This document reviews how IS Decisions WinReporter[®] enables Windows[™] systems & networks administrators to conduct the following security tasks :

- ▶ *Vulnerability assessment*
- ▶ *Host based intrusion detection*
- ▶ *Forensic investigation*

WinReporter® rational: the “Swiss Army knife” approach

WinReporter® is the perfect tool to provide network administrators with an accurate picture of their infrastructure.

WinReporter® offers a set of 58 predefined reports that will help the network administrator in his audit and monitoring tasks: hardware upgrades, software updates and licensing, security checks, etc.

WinReporter® goes further and lets the network administrator drill down through all the information with specific queries. Even though WinReporter® is a general purpose administration tool, its powerful capabilities allow the network administrator to conduct security specific tasks.

In the remainder of this paper, we will narrow our focus on the security capabilities of WinReporter®.

Never underestimate internal threats

Experience has shown that about 80% of network attacks originate from insiders. This is the consequence of a neglected internal network security. Too often such security does not even exist. Missing patches, poor configurations and trust relationships are avenues for unskilled successful attacks. Corporate networks are often qualified as *“hard and crunchy outside, smooth and chewy inside”*...

A legitimate user within the company already has access to internal resources, does not have to defeat any firewall, or to cover its tracks.

Worst, should an external attacker gain an unnoticed access to the network, how could network administrators detect their subsequent actions?

To counter such internal threats, specific measures have to be implemented, and even though WinReporter®’s first mandate is not security auditing, WinReporter can dramatically improve the overall security of your infrastructure.

WinReporter® added value

Virtually all available information about the network is gathered by WinReporter®. This information ranges from hardware to software configuration. Additionally, WinReporter® can collect all event log information.

Event log management is the pillar of many security detective measures, and it is a good practice to audit all events logs. However, this is easier said than done.

Windows is good at collecting event logs, although when it comes to boil down tons of logs to timely get the right information, Windows falls short:

- ▶ The relevant information is scattered all over the network’s nodes.
- ▶ The provided information is far too insufficient.
- ▶ Should the node be compromised, the log information could be lost.
- ▶ Filtering and reporting capabilities are really poor.

WinReporter® fills the gap. It offers event log management in addition to its powerful configuration scanning capabilities. Once this information is pieced together, network administrators have a mighty mean to monitor every single event that might occur within the network.

WinReporter® as a security tool

What makes WinReporter® so powerful is its great flexibility: WinReporter's features allow network administrators to conduct the following security tasks:

- ▶ Vulnerability assessment
- ▶ Host based intrusion detection
- ▶ Forensic investigation

And to focus on what really matters: getting comprehensive and reliable information, and being able to discriminate what is really relevant.

To demonstrate such a statement, let's will examine each of these cases in turn.

Vulnerability assessment with WinReporter®

As a part of risk mitigation process, and in order to quantify the risk that his organization is running, a network administrator has to evaluate what are the infrastructure's vulnerabilities that an attacker could exploit.

Here is where things get complicated...

Based on the principal that an attacker will exploit the weakest link in the infrastructure's security chain, network administrators have to consider any flaw that could appear anywhere in hardware or software.

The genuine strength of WinReporter® is that it gathers and exploits all kind of information.

Wisely used, it will let the network administrator uncover a number of flaws. WinReporter® identifies security breaches and alerts network administrators to weaknesses before an attacker can find them.

This gives network administrators a unique opportunity to remove or mitigate these flaws before an attacker could exploit them.

WinReporter® provides in-depth information about security sensitive configurations such as:

- ▶ Missing updates: Service Packs and hotfixes installed.
How to proceed: Reporter > Reports > Windows > Versions & updates > Windows versions & updates
- ▶ Software that poses a threat: scanner, encryption tools, peer to peer files exchange software.
How to proceed: Reporter > Software > Software policy analysis
- ▶ Unusual user or group accounts
How to proceed: Reporter > Reports > Windows > Security > Users in groups
 Reporter > Reports > Windows > Security > Local accounts analysis
 Reporter > Reports > Windows > Security > Local administrator analysis
- ▶ Unauthorized device detection: rogue modem, NIC, wireless devices, floppy drives
How to proceed: Reporter > Reports > Hardware > Devices > Devices > network adapter | modem | floppy drive
- ▶ Unmanaged shared folders
How to proceed: Reporter > Reports > Windows > System > Shares analysis
 Reporter > Reports > Windows > System > Share permissions
- ▶ FAT partitions without access control means
How to proceed: Reporter > Reports > General > General Report > Disk Partitions
- ▶ Unusual or dangerous services
How to proceed: Reporter > Reports > Windows > System > Services analysis

WinReporter® is also a great mean to monitor other issues such as licensing or copyright control:

- ▶ Amount of instances of a given software
How to proceed: Reporter > Software > Install Analysis
- ▶ Peer to peer file exchange software that might waste network resources
How to proceed: Reporter > Software > Software policy analysis

This short list is far from being exhaustive. WinReporter® is designed with flexibility in mind, to better meet all organizations needs in terms of network monitoring.

Host based intrusion detection with WinReporter®

In extended networks, information is scattered amongst all computers, and there is no convenient way to interpret this useful information. WinReporter® fills the gap left by Microsoft; it pushes further Windows auditing capabilities to emulate a host based intrusion detection system (HIDS).

A firewall is just the first line of defence of a network: a good start to ensure network security, but just the start, and by itself, insufficient.

Typically, best practices recommend using firewalls in conjunction with IDSs. IDSs come in two flavours, network based and host based. Both should be used since they address different threats. WinReporter® can perform the host based part of intrusion detection.

Thanks to WinReporter® versatility, network administrators can monitor all events occurring on network's computers. Since this is done using Windows auditing native capabilities, host monitoring does not hurt performance and remains cost-effective. WinReporter® capabilities provide an accurate picture of all occurred events.

Regular scans will reveal any sensitive information such as:

- ▶ User session information, logon/logoff activity
How to proceed: Reporter > Reports > Eventlog Report > Connections > Session history
- ▶ Process tracking
How to proceed: Reporter > Reports > Eventlog Report > Process Tracking
- ▶ Access control events
How to proceed: Reporter > Reports > Eventlog Report > File Access Report
- ▶ Computer reboot events
How to proceed: Reporter > Reports > Eventlog Report > Computers start & shutdown
- ▶ Close security events monitoring
How to proceed: Reporter > Reports > Eventlog Report > Generic Event Report

All attacks leave tracks, therefore suspicious behavior can be timely detected and necessary measures can be taken.

However, highly sensitive computers deserve real time monitoring. WinReporter® can detect changes once a scan is performed, not in real time.

To address this specific issue IS Decisions provides another tool called EvenTrigger® that monitors host events in real time and notifies network administrators right away.

Forensic investigation with WinReporter®

No network is 100% secure.

Information security is a trade-off between usability and protection; hence, sometimes the network is compromised. Even when things have gone wrong WinReporter® can help network administrators discover what happened.

Scanning the network and storing that information on a regular basis is mandatory to support accountability, legal investigations, and internal trends analysis.

This lets network administrators know in great details what a given user did in the past.

- ▶ Where and when did he log
How to proceed: Reporter > Reports > Event Reports > Connections > Sessions history
- ▶ What process did he run
How to proceed: Reporter > Reports > Event Reports > Process Tracking
- ▶ How and which file did he access
How to proceed: Reporter > Reports > Event Reports > File Access Report

This monitoring capability makes every user of the network accountable including the administrator group.

How to push your investigation further with WinReporter®

So far, we have covered how to use the readily available reports of WinReporter® in information security context. However, there is more you can do with WinReporter®, and savvy administrators can go further.

WinReporter® gives administrators full access to its internal database: thanks to this remarkable feature, administrators can fine-tune their queries and drill down on worthy information. This capability is all administrators need to spot missing critical information as well as more straightforward searches.

- ▶ For instance, an administrator might want to pinpoint who ran which binaries to start a given service on a specific workstation. This looks a bit cumbersome; however it could be an efficient way to discover who has planted back-door software on that workstation.
WinReporter® makes network administrators lives easier, just run:
Reporter > Tables > services and go for wanted service.
- ▶ A more every-day issue is copyright liability. In order to make sure that no mp3 file is stored somewhere in the network; all the network administrator has to do is run:
*Reporter > Tables > realfiles and search for *mp3 files.*
- ▶ WinReporter® can work hand in hand with dedicated security tools. The netcards table provides the network administrator with all authorized MAC addresses.
If a network sniffer detects a packet with a MAC different from a trusted MAC, the likelihood of an ongoing attack is high.

Conclusion

In today's networked business environment, it is essential to mitigate infrastructure vulnerabilities, and track security related activities in order to respond promptly to intrusion attempts, and hold everyone accountable.

Windows does not provide such capabilities, and to achieve such a mandate one needs to acquire a third party software specialized in that area.

A cost-effective solution is to make the best use of generic powerful tool such as WinReporter®.