Global Information Assurance Certification Paper

GSEC

GIAC Security Essentials

Practical Assignment Version 1.4b

Network Surveillance Analysis Plan and Task Checklist

Submitted by: Neo Mui Leng Cherriyln
Date: 17 August 2003

Table of Content

Network Surveillance Analysis Plan and Task Checklist

Abstract

Ownership of the network comes with the responsibility to maintain the well being of the networks and that traffic is at optimal. But more often than desired, the network will be abused by an intruder who has intention of accessing unauthorized resources, or just to cause congestion to the network traffic. Thus the network owner has additional responsibilities to identify and assess all potential threats, and taking the necessary precautions to monitor and prevent such intrusions.

To ensure a detailed and organized documentation is provided for the whole network surveillance process, this paper serves to provide a step-by-step process to achieve the objectives of the intended network surveillance task through complying with the basic Network Surveillance Analysis Plan and Task Checklist (NS-APTC).

After the network surveillance steps have been undertaken, analysis of the data would have to next. In order to confirm or dispel suspicions surrounding an alleged computer abuse, the analyst is required to have a certain amount of experience and domain knowledge to meticulously review all the information and evidence to form a critical opinion based strictly on evidence derived from the network surveillance process and the information provided by the network owner, with neither speculation nor personal bias involved.

As threats become more flexible and frequent, by relying solely on past events to identify and monitor attacks would only catch the amateurs who use the same tactics, thus the NS-APTC only serves as the baseline procedures for undertaking or performing network surveillance or simply, monitoring services. Interpreting the results of the network surveillance would more often than not requires specialized knowledge and an investigative mindset, leading us into the area of network forensic, which this paper does not attempt to cover.

1. Introduction

When an intruder, be it an insider or outsider, abuses the resources available through a computer network, the security of the network will be breached. Disgruntled employees may have taken aim to wreck havoc on the company network, or it could be competitors attempting to break into the network to steal proprietary information. The network owner has a responsibility to identify and assess the potential threats.[1]

1.1. Network Surveillance

Traditionally, surveillance is a critical and necessary step when investigating alleged crimes or abuses. The "suspect" is usually placed under surveillance, where he/ she will be constantly monitored. The purpose is to confirm suspicions, accumulate evidence, and identify any co-conspirators. The same goes for computer networks.

Network surveillance is a process concerned with the use of electronic means, passive or active, to obtain information about the nature, position, or movement over the network as a whole. It includes activities for coordination and assigning priorities to maintenance actions. The information necessary to support this process comes from alarms, measurements, and indicators of operational (including congestion) status.[2]

1.2. Network Surveillance Analysis Plan and Task Checklist

The scope of this paper is to create a basic Network Surveillance Analysis Plan and Task Checklist (NS-APTC) as the baseline procedures for undertaking or performing network surveillance or simply, monitoring services.

This paper serves to provide a step-by-step process to achieve the objectives of the intended network surveillance task, through complying with the following procedures recommended under the Network Surveillance Analysis Plan and Task Checklist (NS-APTC). This is to ensure a detailed and organized documentation is provided for the whole network surveillance process.

1.3. Check with Legal Counsel

Laws govern our world. Always check with your legal counsel before initiating any network surveillance task.[3] This is especially critical if the recourse actions involve legal proceedings, we do not want to jeopardize the whole case by infringing privacy laws in the process of performing network surveillance.

2. Overview of the Network Surveillance Analysis Plan and Task Checklist Process

Network surveillance is a critical step when investigating alleged computer crimes or abuses. The purpose of network monitoring is not intended to prevent attacks; but as a tool to accomplish a number of objectives:

- To confirm or dispel suspicions surrounding an alleged computer abuse.
- To gather evidence and information over the compromised network.
- To identify and verify the area of compromise.
- To determine the timeline of the activities leading to the alleged crime or abuse.
- To identify the parties involved in the area of compromise.

2.1. Deciding where and how to monitor

Now that we are clear on the objectives of performing network surveillance, so what are the next steps?

Network surveillance can be achieved with a variety of methods. Comprehensive monitoring should be used on the subnet hosting the target computer. Usually a laptop configured with a sniffer that flags packet attributes as well as record content is most appropriate. Less comprehensive monitoring should be considered at the network boundaries, such as using logging features of routers to identify particular packet types as they enter or leave the client network.[3]

2.2. Deciding what to monitor

Performing comprehensive monitoring is always a more secure choice, however, sometimes resources constraints such as hard disk space and network bandwidth will limit the depth of the monitoring.

Therefore, to determine what to monitor, we should always look at the scope of compromise. In some cases, we can consider only logging all traffic to and from the compromised system. Of course we should also bear in mind to monitor all traffic originating at the compromised system as many attackers use backdoors that initiate outbound connections from the compromised system.

2.3. Common Scenario

A common scenario is that an unknown attacker has continually accessed an unbannered system and sabotaged critical working files within this compromised system. In a situation when the attacker is unknown, it could be an insider job or an attack from an external intruder. The following NS-APTC aims to guide the investigating analyst through a systematic checklist process to nail the attacker and gather evidence and information over the compromised network.

2.4. The 5 phases of the Network Surveillance Analysis Plan and Task Checklist (NS-APTC)

This NS-APTC will provide the 5 basic phases to render one to achieve the above objectives, through complying with the following procedures when performing all network monitoring tasks

a) Information gathering;

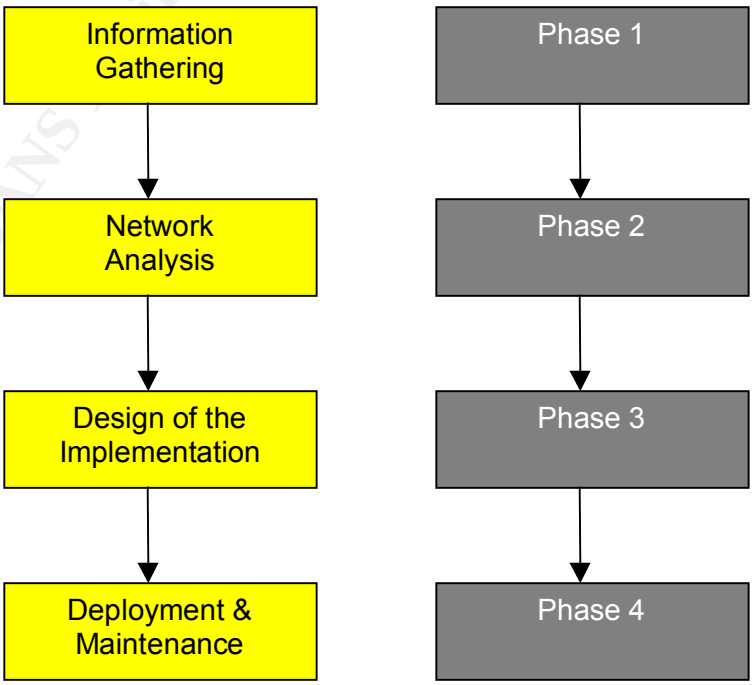
b) Analysis of target network;

c) Design of network monitoring implementation;

d) Deployment and maintenance process; and

e) Data analysis.

The 5 phases of the Network Surveillance Analysis Plan and Task Checklist (NS-APTC) can be visually described in the following figure:



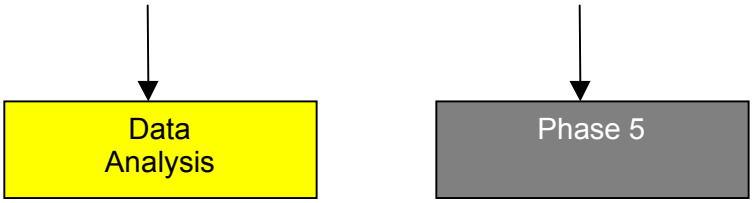


Fig. 1. Network Surveillance Analysis Plan & Task Checklist Phases

3. Information Gathering

Information gathering is the fundamental essence of the Network Surveillance Analysis Plan and Task Checklist (NS-APTC). It is during this initial channel of communication with the network owner that helps to optimize the performance of the process. Hence, it is essential to first understand the background and suspicions surrounding an alleged computer abuse achieve the following objectives:

- Determine the scope of compromise;
- Gather the essential technical information of the compromised network; and
- Affirm the objectives of performing the network monitoring service.

To achieve the above, the investigating analyst should preferably hold a pre-investigation discussion session with the network owner and fully document all the relevant details pertaining to the alleged abuse in the Information Collection Checklist (refer to Appendix A). The "Information Collection Checklist" aims to serve as guidance in the pre-investigation discussion sessions. At the same time, it also serves as a tool to ensure that necessary information is obtained.

During the discussion sessions, the investigating analyst should try to understand the nature of the case and obtain necessary information from the network owner with regard to the scope of the compromise. The investigating analyst should also take this chance to briefly explain the process of the network surveillance to the network owner and affirm the requirements of the whole network surveillance task.

3.1. Necessary Technical Information

It is very important to obtain the necessary technical information from the network owner such as:

- The operating systems (OS) used in the compromised network;
- The network protocols used in the compromised network; and
- The LAN topologies of the compromised network.

Upon understanding the scope of the compromise, the next step is for the investigating analyst to gather information of the network design and physical layout of the target network, such as:

- A copy of the IP network diagrams;
- The list of assigned IP addresses and node numbers of each station using the target network;
- The number of network layers and domains of the target network;
- The list of domain names of the target network; and
- The site plan/ physical layout of the workstations.

3.2. Requirements from the network owner

The investigating analyst should also take this chance to request from the network owner a network account, an IP address and a node number for the network monitoring station.

All these are important inputs and steps we need to take before we embark onto the next stage to perform the network analysis.

4. Network Analysis

The analysis process entails a reorganization and classification of the information gathered in Phase 1. This second phase of NS-APTC requires the careful analysis and strategic planning of processing the information. Therefore, this is a very important process to enable the investigating analyst to provide the most appropriate design for the network monitoring implementation in the third phase.

4.1 Network Equipment

The investigating analyst is to list down all the network devices used in the target network in the Network Equipment Checklist (refer to Appendix B).

After which the investigating analyst is required to perform a search on the Internet to gather the full documentation or user manuals for each of the network

devices on the Network Equipment Checklist. All the detailed information found for each device should be correspondingly attached as part of the Appendix and it should also be indicated as the attached references in the Network Equipment Checklist (refer to Appendix B).

For the switches, which are used in the compromised network, the investigating analyst should indicate in the remark column in the Network Equipment Checklist (refer to Appendix B), whether the switches come with management software. There should also be indications in the remarks column of any important information pertaining to the respective network devices.

4.2. Classification of IP addresses

The purpose for reorganization and classification of the IP addresses is to facilitate the subsequent implementation process. At the same time, it would help to segment the scope of the target network, and thus help to identify and verify the area of compromise.

The investigating analyst is to create a Classification of IP addresses Checklist and classify all the assigned IP addresses primarily based on the respective corporate departments as the first criteria.

All the IP addresses within the same department would subsequently be organized in the ascending order of each workstation's node number.

Appendix C provides the generic template of the Classification of IP addresses Checklist.

4.3. Verification of Information

The investigating analyst is to make use of the Classification of IP addresses Checklist and the sitting plan/ physical layout diagram provided by the network owner to verify whether the assigned node number for each workstation tallies with the actual network connection point.

It is important for the investigating analyst to physically trace each workstation's network cable, and make sure it is plugged into the correct assigned node number tag pasted on the respective network points to ensure right documentation and analysis.

Therefore, it is essential to note down any wrong node number assignment on the Classification of IP addresses Checklist and the Verification Process Checklist (refer to Appendix D); and inform the network owner of such changes.
All other relevant issues are also to be noted in the Verification Process Checklist (refer to Appendix D) and verified with the network owner, before we move on to the Phase 3, for the design and network implementation stage.

5. Design of the Network Monitoring Implementation

The design of the network monitoring implementation is the most important phase in the NS-APTC. The investigating analyst has to first comprehend the scope of the compromise and from the analysis of the available information, produce a design that best achieve the objectives.

5.1. Network Monitoring tools

Investigations that require the capture of data as it travels over a computer network require the use of special software or hardware. Many of these solutions also include the ability to analyze the captured data.[4]

There is a wide range of network monitoring tools available in the market and it can be quite a headache in choosing the right one. The decision on using the right tool should be always be based primarily on the requirements and scope of the network surveillance task, which we have discussed earlier in Phase 1 and 2. However, this can still narrow down to quite a few selections. Thus, in this sense, the selection will then be based on the comfort of use of the investigating analyst.

One of the more popular and freely available packages is Ethereal, which runs on both UNIX and Windows systems. Using Ethereal on a computer connected to a network allows all traffic traveling over the network to be captured and analyzed either in real time or at a later date, allowing such activities as web surfing and network file accesses to be reconstructed.[4]

In addition, the link below provides a list of tools used for network (both LAN and WAN) monitoring and where to find out more about them:

http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

5.2. Shared Network

In a shared network infrastructure, every station's transmissions are visible to every other station within the same collision domain.

Thus, by attaching a network monitoring tool (at any point in a collision domain, one can acquire 100% of the transmitted packets from all the stations within that domain.

For a shared network with multiple domains, the network monitoring tool will be attached to the port on the primary hub if it is required to capture the network traffic of the whole environment.

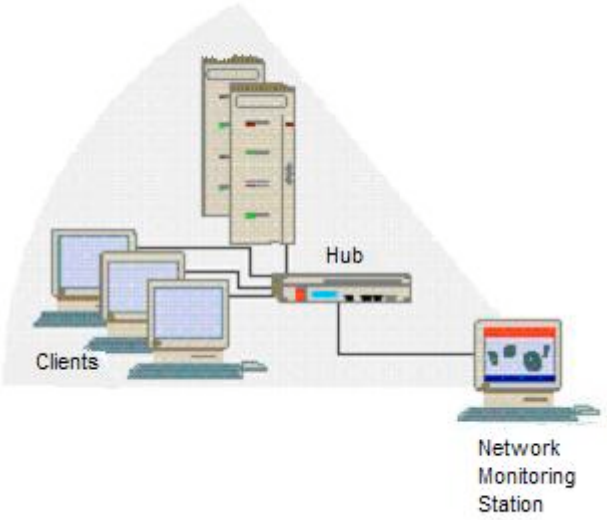


Fig. 2. A Shared-Media Network attached with network monitoring tool

5.3. Switched Network

A switched network does not forward all packets to all stations. Although broadcast and multicast packets continue to be forwarded out to all ports of a switch and, thus would reach all the stations in the broadcast domain. However, direct packets are forwarded in a more sophisticated manner. A "direct" packet contains a specific Ethernet address as the destination target address, meant for only one recipient. The switch evaluates the Ethernet destination address on all incoming data packets and would forward them only through the single port to which the intended target station is attached.

Therefore, while switched networks provide a more efficient use of the network media and infrastructure, it has also brought about some inherent limitations and restrictions to the network monitoring process.

5.3.1. Switches with Management Software

To enable effective network monitoring, the switch manufacturers have implemented a mechanism by which the switch administrator can select a port to be dedicated to the network monitoring process. This is done through the switch management software, where a command is issued that "mirrors" all traffic going in or out of a specific port that is connected to the target station, is copied and sent out to the special network monitoring port.

5.3.1.1. Configuration of the network monitoring port

The most common term used to refer to the special port configured for network monitoring is a "Mirror Port". However, various vendors may use different terminologies to refer to this special port, such as a "Span Port".

There are a variety of port mirroring options available from various vendors, thus it is very important to consult the switch documentation to understand the capabilities and configurations required to activate the port mirroring function.

5.3.1.2. Mirroring of multiple ports simultaneously

Some switches allow configuration of mirroring more than one port at a time through the switch management software.

It is also possible, with some vendors' equipment, to mirror all traffic within a VLAN simultaneously and have a copy of each packet transmitted in the VLAN sent to the mirror port.

Again, it is very important to consult the switch documentation to understand the capabilities and configurations required to perform mirroring of multiple ports simultaneously.

In the event of mirroring multiple ports simultaneously, note must be taken to consider the possibility that the aggregate of data packets from all the mirrored ports may exceed the bandwidth capacity of the mirror port, to which the exceeded data packets will be dropped.

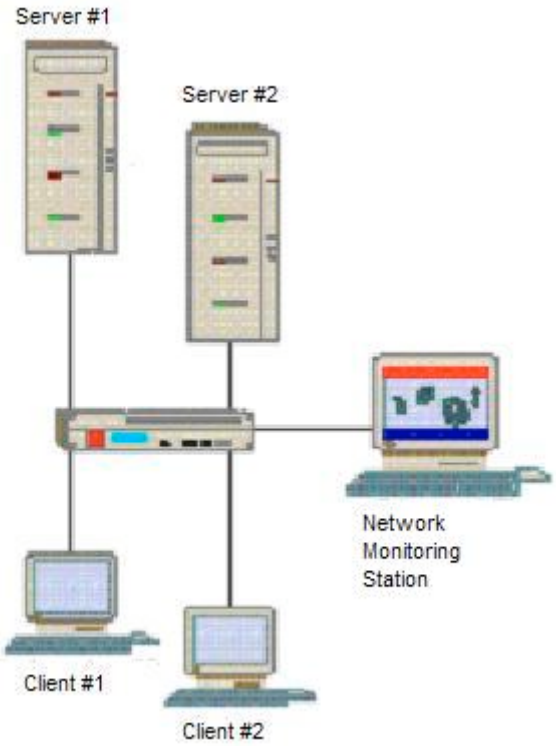


Fig. 3. A Managed Switched Network attached with network monitoring tool

5.3.2. Switches with Non-Management Software

Some switches do not have the switch management software installed in them. Hence, it is not possible to perform mirroring function on these non-managed devices. In such situation, the alternative is to insert a repeating hub between the switch and the client to be monitored and, attach the network monitoring tool to the hub.

Likewise, the hub should be inserted between the switch and the server, if it is intended to capture all the traffic to and from the server.

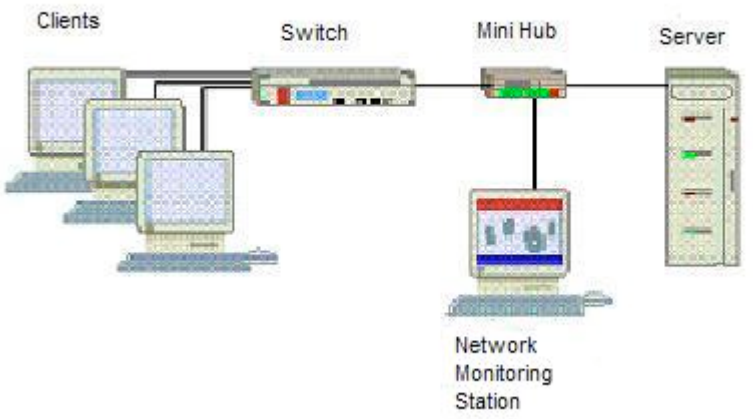


Fig. 4. A Non-Managed Switched Network attached with network monitoring tool

Having considered all options, it is better to implement the use of a monitoring hub for all switched network unless the situation does not permit so. This is to minimize the risk of causing configuration problems to the target network when deploying the mirroring method.

5.4. Design Checklist

Appendix E provides the generic form for the design of the network monitoring implementation checklist.

The investigating analyst is to provide a design diagram of the network monitoring implementation (refer to Appendix E) and indicates in the Design Checklist (refer to Appendix E) the physical location/s of the respective monitoring hub/s, as well as the physical location of the network monitoring station.

It is also necessary to provide a brief description of the design for the network monitoring implementation. At the same time, the consideration factors that led to the final design must be indicated and explained in the Design Checklist.

One should always bear in mind that prior approval from the network owner is required before proceeding with the actual deployment.

6. Deployment and Maintenance

The deployment phase involves the physical implementation of the network monitoring design. The maintenance entails the collection of the data logs from the network monitoring station at regular intervals and, ensures the smooth and successful monitoring of the target network.

6.1. Physical Deployment of Network Monitoring Design

As most of the deployment processes are performed at external premises, the investigating analyst should request for a personnel preferably from the IT department to accompany them during the whole duration of the deployment process. This is to make sure that a witness is present to ensure the integrity of the process.

For a hub-based network, network monitoring is much simpler; and no addition of monitoring hub is required. The general deployment steps are to record the physical location of the network monitoring station and the node number it is connected to, change the IP address of the network monitoring station to the one provided by the network owner and reboot the network monitoring station. Next, attach a labeled hard disk to the network monitoring station and create a new log folder (of the current date, e.g.01082003) in the external hard disk.

Launch the network monitoring tool and customize the filters (refer to respective software user manual) that best cater to the objectives and requirements of the network surveillance task.

It is just as important to ensure the network monitoring tool is monitoring successfully by checking that the monitoring percentage bar is increasing and the logs are saved to the external hard disk when the buffer is full.

For a switched-based network, as mentioned above in 5.3.2, it is better to implement the use of a monitoring hub for all switched network unless the situation does not permit so. The general deployment steps are to record the physical location of the monitoring hub to be inserted between the primary switch and the server. Next, plug a straight cable to the uplink port of the monitoring hub and the other end of the straight cable should be plug into a port on the primary switch. Always label the node numbers on the ports of the switches, which the respective cables are to be plugged out to ensure systematic reference of any changes made. Connect the cables (of the monitored stations) onto the monitoring hub by stages. (e.g. 5 cables at each stage);

Similarly, record the physical location of the network monitoring station and the node number it is connected to, change the IP address of the network monitoring station to the one provided by the network owner and reboot the network monitoring station. Next, attach a labeled hard disk to the network monitoring station and create a new log folder (of the current date, e.g.01082003) in the external hard disk.

Launch the network monitoring tool and customize the filters (refer to respective software user manual) that best cater to the objectives and requirements of the network surveillance task.

Again, it is just as important to ensure the network monitoring tool is monitoring successfully by checking that the monitoring percentage bar is increasing and the logs are saved to the external hard disk when the buffer is full.

Appendix F provides the generic checklist for the deployment process, which serves as guidance during the physical implementation over at the (especially at external) premises.

6.2. Maintenance of the Network Surveillance Process

The frequency for the collection of data would be on the discretion of the investigating analyst who will consider the requirements of the network monitoring task.

7. Data Analysis

Data analysis is the most complex as well as the final phase of the NS-APTC. This critical phase will entail the integration of all the efforts and results of the earlier phases, to produce an answer to meet the objectives and requirements of the network surveillance task.

Data analysis would very much require the analyst to have a certain amount of experience and domain knowledge to meticulously review all the information and evidence and form a critical opinion to confirm or dispel suspicions surrounding an alleged computer abuse.

The investigating analyst must note that any opinion or conclusion drawn must be strictly based on the evidence derived from the network surveillance process and the information provided by the network owner. The opinion or conclusion must not be based on speculation of what could have happened.

It is also good to note that analysis work is variable; therefore this section merely aims to act as a guide to the analyst in his/her work. Appendix G provides the generic checklist for the data analysis process.

Before embarking on the review and analysis process, the investigating analyst should list the objectives of the review and analysis. Upon reviewing all the information and objectives, he/ she should list down the following:

- The target workstation/s;
- The target data to search for; and
- The time frame of the incident (alleged computer abuse).

Listing the objectives and identifying the above factors would help the analyst in narrowing down the scope of the compromise and hence aid him/her in optimizing the analysis process.

Having defined the scope of the compromise, the investigating analyst should next proceed to list down all the workstations that have communicated with the target machine during the incident time frame; and search for the target data in the packets log (refer to software user manual).

The investigating analyst should proceed to organize the evidence and attached them as reference. Finally, he/ she is to draft a Summary of Analysis after the analysis process (refer to Appendix G).

All opinions or conclusion drawn in the Summary of Analysis should be referenced to the evidence retrieved from the network surveillance process. Most importantly, the Summary of Analysis should address the requirements and objectives.

8. Conclusion

In recent years we have seen the exponential burst of business leveraging on IT, thus as the number of websites, emails and electronic files increases, and the ways to access them become more flexible, the threat to your information mounts. New attacks and covert methods for accessing corporate resources are occurring by the seconds. Hence, by relying solely on tracing of past events to identify and monitor attacks would only help to catch the amateurs who use the same tactics.

Therefore the Network Surveillance Analysis Plan and Task Checklist (NS-APTC) only serves as the baseline procedures for undertaking or performing network surveillance or simply, monitoring services. Interpreting the results of the network surveillance would more often than not requires specialized knowledge and an investigative mindset, which will lead us into the area of network forensic.

References

1. Joe Bardwell, "Network Security with EtherPeek NX", February 2003, URL:http://www.wildpackets.com/elements/whitepapers/NetworkSecurity.pdf

2. American National Standard for Telecommunications - Telecom Glossary 2000, URL: http://www.atis.org/tg2k/_network_surveillance.html

3. Kelvin Mandia and Chris Prosise, "Incident Response: Investigating Computer Crime", Osborne/McGraw-Hill, July 2001, ISBN: 0-07-213182-9

4. Rod Morries, "An Introduction to Computer Forensic Tools", 10 October 2002, URL: http://www.securityfocus.com/guest/16691

5. CERT® Coordination Center, "Monitor and inspect network activities for unexpected behavior", October 2000, URL: http://www.cert.org/security-improvement/practices/p094.html

6. Brian W Laing, "How do you implement IDS (network based) in a heavily switched environment?", URL: http://www.sans.org/resources/idfaq/switched.php

7. Joseph Bardwell, "Monitoring Your Ethernet Network", 2003, URL: http://www.wildpackets.com/elements/technical_briefs/TB003_MonitoringYourNetwork.pdf

8. WildPackets, "Applying EtherPeek to Switched and Gigabit Ethernet Network Management", March 2003, URL: http://www.wildpackets.com/elements/whitepapers/EP_in_Switched_Networks.pdf

9. Karen Kent Frederick, "Network Monitoring for Intrusion Detection", 28 August 2001, URL: http://www.securityfocus.com/infocus/1220

10. Kevin Timm, "Passive Network Traffic Analysis: Understanding a Network Through Passive Monitoring", 21 May 2003, URL: http://www.securityfocus.com/infocus/1696

11. Michael Nancarrow, "Protecting your Internal Systems from a Compromised Host", December 2001, URL: http://www.sans.org/rr/papers/9/707.pdf

12. Matt Bishop, "Computer Security", Addison Wesley, 2003, ISBN 0-201-44099-7

Appendix A–Information Collection Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

Background Information:

Nature of Case:	
Objective of Case:	
Monitoring Target:	
Operating Systems (OS) used:	
Network Protocols used:	
LAN Topologies:	

Contact Persons:

Case Management	**IT Department**
Name:	Name:
Title:	Title:
Tel:	Tel:
Email:	Email:

Has the owner been briefed on Network Surveillance Process?
YES ☐ **NO** ☐

Reason if No: _____

Has the owner been informed of purchase of additional hard disks for data storage?
YES ☐ **NO** ☐

Reason if No: _____

List of Information to Request from the Network Owner:

No	**Request Items**	**Date Requested**	**Date Obtained**	**Remarks / Reference To Attached Materials**
1	A copy of the IP network diagram			
2	The list of assigned IP addresses and node numbers of each station using the subject network			
3	The number of network layers and domains of the subject network			
4	The list of domain names of the subject network			
5	The site plan/ physical layout of the workstations			
6	A network account, an IP address and a node number for the network monitoring station			

_____ _____

Name/ Signature of Analyst Date / Time Completed

Appendix B – Network Equipment Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

List of Network Equipment:

No	Type of Network Equipment	Description	Attached Documents	Remarks
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Name/ Signature of Analyst

Date / Time Completed

Appendix C – Classification of IP Addresses Checklist

No	IP Address	Node No	Department	User
1	xxx.xxx.xxx.xxx	A1	Operations	GF Ho
2	xxx.xxx.xxx.xxx	A3	Operations	AB Tan
3	xxx.xxx.xxx.xxx	E20	Operations	TH Teo
4	xxx.xxx.xxx.xxx	A9	Finance	BB Wong
5	xxx.xxx.xxx.xxx	A10	Finance	HS Tan
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Appendix D – Verification Process Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

No	Issues to be Verified	Date of Request	Request Made To	Date of Issue Verified	Remarks
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Name/ Signature of Analyst

Date / Time Completed

Appendix E – Design Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

Design Diagram:

Name/ Signature of Analyst

Date / Time Completed

Physical Location of the Monitoring Hub/s: _____

Physical Location of the Network Monitoring Station: _____

Design Description: _____

Consideration Factors of Design: _____

Has the client been briefed on the Network Monitoring

YES ☐ **NO** ☐

Reason if No: _____

_____ _____

Name/ Signature of Analyst Date / Time Completed

Appendix F – Deployment Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

☐ **Deployment for Hub-Based Network:**

No	Procedures	Completed (Yes / No)	Comments
1	Install network monitoring tool on the network monitoring station		
2	Record the physical location of the network monitoring station and the node number it is connected to		
3	Change the IP address of the network monitoring station to the one provided by the client		
4	Reboot the network monitoring station		
5	Attach the external hard disk drive, containing a labeled hard disk, to the network monitoring station		
6	Create a new log folder (of the current date, e.g.01082003) in the external hard disk		
7	Launch the network monitoring tool and customize the filters (refer to software user manual)		
8	Ensure network monitoring tool is monitoring successfully		

☐ Deployment for Switched Network:

No	Procedures	Completed (Yes / No)	Comments
1	Record the physical location of the monitoring hub to be inserted between the primary switch and the server		
2	Plug a straight cable to the uplink port of the monitoring hub and the other end of the cable should be plug into a port on the primary switch		
3	Tag all the cables (to be uplink to monitoring hub) with their respective node number		

4	Label the node numbers on the ports of the switches which the respective cables are to be plugged out		
5	Uplink the cables onto the monitoring hub by stages. (5 cables at each stage)		
6	Install network monitoring tool on the network monitoring station		
7	Record the physical location of the network monitoring station and the node number it is connected to		
8	Change the IP address of the network monitoring station to the one provided by the client		
9	Reboot the network monitoring station		
10	Attach the external hard disk drive, containing a labeled hard disk, to the network monitoring station		
11	Create a new log folder (of the current date, e.g.01082003) in the external hard disk		
12	Launch the network monitoring tool and customize the filters (refer to software user manual)		
13	Ensure network monitoring tool is monitoring successfully		

Name/ Signature of Analyst

Date / Time Completed

Appendix G– Analysis Process Checklist

Case No:
Date:
Network Owner:
Investigating Analyst In-charge:

Addition information from Network Owner:

_____
_____
_____

Incident Analysis:

Objective of Network Monitoring task:	
Identify Target Workstation/s:	
Identify the Target Data Packets to Search for:	
Time Frame of Incident:	
Workstation/s that have Communicated with the Target Machine/s within the stipulated time frame:	

Comments after Reviewing Data Search:

_____
_____
_____
_____
_____
_____
_____
_____
_____

Summary of Analysis:

Name/ Signature of Analyst

Date / Time Completed

Last Updated: May 22nd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event