Global Information Assurance Certification Paper

GSEC Practical assignment v. 1.4b
Option 2 – Case study in Information Security

"Unauthorized devices on ethernet networks"

Christian Chablais

Submitted 3/31/2003

Table of content

Summary

This paper has been prepared for the GSEC practical assignment v1.4b, option «Case study». It covers the following incident : a notebook had been connected without proper authorization on our network for a brief period of time. More generally, it addresses the issue of connecting unauthorized devices on internal private ethernet networks.

I first describe the situation on our network before the incident and what our vulnerabilities were. Then, after the incident has been discovered, I go though the steps that were followed to discover if the notebook had had any hostile activity while connected and if escalation was necessary.

As conclusion, I explain our counter-measures against this threat: a) Prevention, through the release and implementation of an Acceptable Use Policy (both in French and English), and b) Detection, through the installation of the free software «Arpwatch» and the regular consultation of Dhcp logs.

Introduction

The Internet world is running out of IP addresses. This is one of the reasons why we are moving from IP version 4 to IP version 6. This situation happened (a) because of the growing popularity of the Internet worldwide, and (b) because of the multiplicity of devices that can be plugged onto the Net : notebooks, mp3 players, games consoles, etc. Those devices could be characterized as “cool, nice, small and friendly”. They are easy to plug and so to gain instant access to any ethernet network, at least at level 2.

In November 2002, as I was ambling in the offices of my company, I saw one of those cool devices on the desktop of an employee. It was a nice, white and blue Macintosh notebook. The employee seemed to be playing some Tetris game with it. When I came back to my own desktop, I thought that although my colleague’s device had a fun look, it was a computer with full capabilities and, if it were compromised, it could launch any kind of

attack which could be devastating for the simple reason that it was at that moment directly connected on the GE internal network, therefore bypassing the filtering of the external firewall.

I worked out this concern before I could establish that this device had been effectively connected to our network for some time. I realized how vulnerable our company was to this threat. After I could satisfy myself that no such attacks had been launched, I began to look for counter measures.

Let's see first what the situation was before the incident happened.

Before the incident

THE COMPANY
GIAC Enterprise (GE) – a fictitious name - is a relatively small financial company with about 100 employees. GE has two offices, distant of about 500 km (300 miles), which act as disaster recovery site for each other. Its core business is to manage the financial assets of private clients : customers deposit their assets with GE and define the terms of a management agreement, which outlines the scope and style of management to be applied; it can be either conservative, dynamic or balanced. The assets then entrusted to GE's hands, it is their role to achieve the goal set with the clients, which is generally to increase the value of the assets over a mid-term horizon. As a financial company, security is a high concern for management, clients and auditors.

ETHERNET NETWORK AND IP ADDRESSING
Both sites are interconnected through a leased line and data are encrypted by a Cisco VPN. Both sites use a 10/100 mb ethernet network controlled by a Cisco catalyst switch. We use a class C IP addressing scheme (172.x.x.x format). Every host has a fixed IP address and we have a IP address database which centralize all them. It is the duty of the Sysadmin to update the database every time an address must be added, modified or removed.

DYNAMIC IP ADDRESSING
On each site there is a DHCP server : we use the NT4 server DHCP feature for this service. It is setup exclusively for the few traveling officers of the company. When they go from site A to site B or vice versa, they just plug their notebook in the LAN, get a valid IP address, and access the resources to which they have the proper authorization.

PHYSICAL PROTECTION OF SWITCHES
The Catalyst switches are located in the computer rooms, whose access is restricted. Only the IT staff can open the door with a code, and every access is logged. We have put a lot of restrictions to protect this point of the physical network, but on the other side, there is not much that can be done to prevent an employee to unplug the cable from his PC and insert it in the NIC of an unauthorized device. One day this had to happen…

POLICIES
We had two polices in place : one for the use of Internet and the other regarding the e-mails, because both management and the IT staff felt that these were the points where abuses might most probably happen within GE. Both are issue-specific policies. What was

missing was an “Acceptable Use” policy, which can be defined as a “Program Policy” with large coverage stating the overall security posture of the company. We acknowledged later how much this was important.

NETWORK INTRUSION DETECTION
A Snort box is screening traffic on each site’s gateway. Each alert is sent in MYSQL format to a central ACID console. Although it is not the panacea that resolves all IT security issues, it is a useful tool to determine if there is hostile activity on the internal network.

WEBSENSE
Every access to the Internet is filtered by a Websense host (ref. www.websense.com) . GE Internet Use policy states that the use of Webmail and Chat services is not authorized and that every access is logged and may be monitored. Logs are registered in a MS-SQL database, which revealed itself a useful resource to detect unauthorized activity.

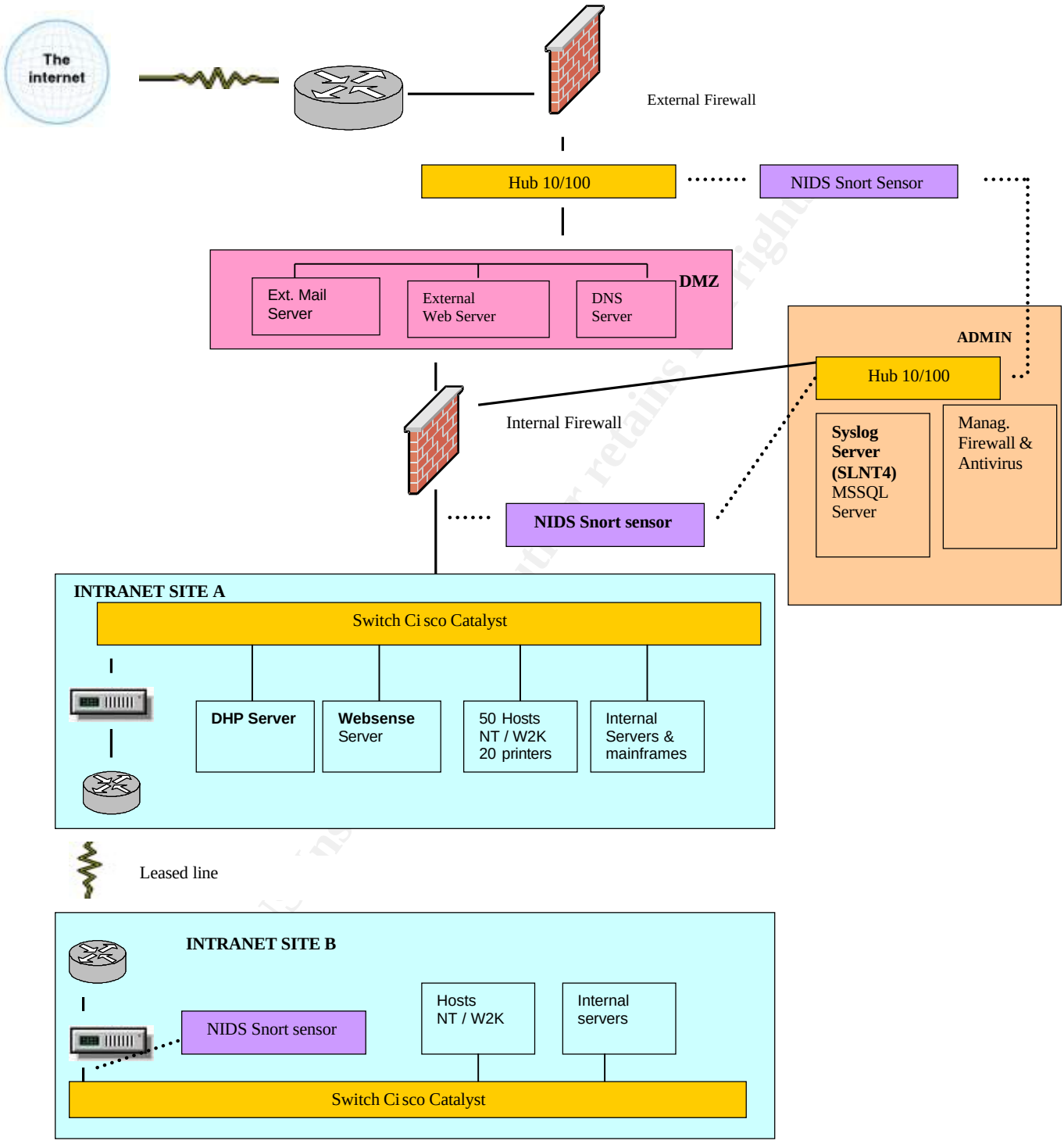
VIRUS
We have a Norton Antivirus Corporate Edition system, which distributes the new virus definitions to every host and, through its centralized console, allows us to monitor any virus alert. In addition to this control, e-mails are checked at the gateway with a different anti-virus software (F-Secure), and potentially dangerous attachments, like “.exe” or “.vbs”, files are blocked.

FIREWALL
There is an external IPTABLES firewall right after the provider’s router. At the next layer a Checkpoint firewall filters accesses, and operates a Network Address Translation.

CENTRALIZED LOG
To face the bulk of events generated from NT/W2K based servers, Unix servers and Cisco devices, we collect them in a centralized database. We have implemented it on a NT4 server using SL4NT (http://www.netal.com/sl4nt.htm), which emulates the Syslog daemon, and we have configured it to register all the messages in a MS-SQL server through the ODBC facilities. The logs are reviewed through a Web interface developed internally with Coldfusion. One feature is to view all logs generated by an IP address, and to sort them. This is a quick way to detect security alerts without having to connect to every single server separately. To log Windows-based servers events, we use Ntsyslog (http://sabernet.home.attbi.com/software/ntsyslog.html), a free software which forwards events to a Syslog server.

ON NEXT PAGE : NETWORK DIAGRAM OF GE

Network Diagram of GIAC Enterprise



RISK
Risk can be evaluated with the formula : "*Risk = Threat x Value x Vulnerability*".
The **threat** we had to face was the plugging of unauthorized devices directly on the internal network, and this is easy to do.
Our **vulnerabilities** at the time were :

- We had no Acceptable Use Policy which explicitly stated that devices could be networked only by the IT staff, and employees were not aware of the potential damages of this unforeseen action.
- We had DHCP servers, but we didn't monitor their activity.
- We had Snort sensors, but they were neither configured nor intended to detect unauthorized activity,

The dangers represented by an unknown ethernet device on the LAN were :

- A determined and skillful attacker might launch a network reconnaissance, then portmap discovered devices, exploit vulnerabilities it could find, sniff network to discover passwords, break into a vulnerable host and gain access to resources of GE. This process is described in the book "Hacking exposed" as "Privilege escalation".
- The intruder could simply launch a Denial of Service attack, or spread viruses, rendering important services of GE unavailable.
- If the attacker had no particular knowledge but his device were compromised, he could open a back door and give access to an external intruder into GE network.

All GE activity could be stopped for a long time or classified data could be disclosed : both represent a potentially high damage in **value** terms. Therefore, the risk of plugging unauthorized devices on the LAN is high.

It so happened that I could catch the unauthorized device - this is the good news. The bad news is that it could only be detected by pure luck : I was walking through the office and my attention was caught by this nice blue Mac notebook. What if I had not been in this office at this moment ? What if this violation had happened on the other site, 500 km away? I could see how vulnerable GE network was to this kind of attack, and had to improve its security. I had to learn from experience.

During the incident

Back to the moment I saw the notebook. It took me 45 minutes before wondering "What if the Mac notebook had been wired to the network ? How could I know about it ?"

FIRST RESEARCH
The first think I did was to check the Snort ACID console : no abnormal activity had been detected. I was tempted to use NMAP to scan the network, compare the result to existing IP database and look for differences, but this could work only if the new device had been connected at the moment of the scan. Another resource I checked was the events generated by the NT Domain Controllers. Neither there could I find unauthorized accesses. I didn't stop there and kept on looking in logs until I found the evidence.

DHCP LOGS – UNKNOWN MAC ADDRESS
On NT servers, DHCP logs its activity in the directory "%SystemRoot%\System32\dhcp\", in files with the pattern "DhcpSrvLog.xxx", were "xxx" is an abbreviation for the day (Mon-Sun). There was the following entry :

```
Address :        172.X.X.162
Unique ID :           000393xxxxx
Client name :    [empty]
Client comment :      [empty]
Lease expires : 8.11.02 00:46
(note : I use "x" to sanitize information)
```

This was very unusual, because other regular entries had a valid Client name information. To figure out which device had got the IP address, I had to use the Unique Id info, which is the Mac address of the Nic. An up to date list is found at : http://standards.ieee.org/regauth/oui/oui.txt . Every Mac address is (or should) be unique, and as a convention the first 3 hexadecimal digits are reserved for the manufacturer. I found that 00-03-93 was attributed to Apple Computer Inc, Cupertino, US. Reverting to the employee, he admitted to me that he had plugged the notebook into our LAN.

MANAGEMENT DECISION

I took a breath and called the IT responsible person who was working in the other site. It was clear that the employee had done something unauthorized, and we were wondering why anybody would do something like that (we were somehow ingenuous at the time). But the question we had to answer at the moment was : had the device had any hostile activity while connected to the LAN ? Before taking a drastic decision, like forcing everybody to change one's password, we agreed to investigate the device itself.

Back to the employee, I asked him what he had done exactly and why. He said that he had just installed an ADSL connection at home and it didn't work as expected ; he just wanted to control that his notebook was configured properly. What he did was to unplug the cable of his workstation, insert it into his notebook's Nic, powered it on and browsed some Internet pages.

I had the confirmation he had accessed the Internet from the Websense Log database. There were two pages of this kind of activity :

```
www.gazetta.it 7.11.02 16:50 http 172.x.x.162 195130 Sports
```

There were some accesses to Apple.com too.

At this I moment went back to the GSEC course regarding Incident Handling. They teach us to take good and consecutive notes, which will be used for the follow up report. I began to write all the actions I took before, and kept on like that from this point on. Although it might look "exaggerated", I had to consider that a disciplinary sanction may have to be taken against the employee and I should have a consistent report for the management.

LOOKING FOR HOSTILE ACTIVITY

The main problem with this machine was that it was a Macintosh, and that I had no knowledge of its OS. How to figure out if any malware had been installed ? The employee assured me that the machine had been freshly re-installed the day before, and he showed me the original CDs. At this point a good option was to ask an external Mac expert consultant. Together with the IT responsible person we choose another road.

Before anything else, I updated the anti-virus signature file and scanned the network. No virus was found. I checked again the Events generated from the Syslog console, but no abnormal activity had been registered.

The rationale of the approach was : instead of checking the notebook from inside, I would consider it as a black box, isolate it in a network segment and analyze whatever would come out of it. For this operation I would rely on the firewall and some tools presented at the GIAC-Security Essential course : Snort and Tcpdump.

The notebook was connected to a Hub, together with a the Snort sensor and a Linux box running Tcpdump. The role of Snort was to identify and report any hostile activity, and Tcdpump would catch all traffic from and to the notebook ; it was started with "`tcpdump host 172.x.x.162 –w evidence.txt`", were the flag "-w" writes all the output to the file "evidence.txt " for later analysis. On the firewall I added a rule which would drop all traffic from and to 172.x.x.162 and log it. This would tell if the notebook tried to connect to the Internet, which is a typical behavior of a back door.

The notebook was switched on and let run for two minutes, and then was disconnected. During this period its activity was constantly monitored.

LOGS GENERATED
Snort didn't catch anything.

The firewall generated two entries :

```
172.x.x.162.49156 > 172.x.x.255.nbname (137) udp
172.x.x.162.49157 > 172.x.x.255.nbname (137) udp
```

Tcpdump was more prolific. Here is a summary of the events :

```
who has 172.x.x.162 tell 172.x.x.42
who has 172.x.x.162 tell 0.0.0.0
172.x.x.162 > 222.0.0.2 igmp
172.x.x.162 > 224.0.0.255
172.x.x.162.5333 > 222.0.0.251.5353 udp
172.x.x.162.49155 > 239.255.244.253 svrloc udp
172.x.x.162.49156 > 172.x.x.255.netbiosns broadcast
172.x.x.162.49157 > 172.x.x.255.netbios ns udp
172.x.x.162.49158 > ournameserver1.netbios-ns udp
```

The first events "who has" are related to Arpa traffic : the Nic announces itself on the LAN, which is a regular activity. I had some concerns with the traffic to hosts "222.0.0.2", "224.0.0.255", etc. In fact those are class D addresses (224-239 multicast) related to the Igmp protocol. I found a description of "IP Multicasting" at ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/ip multicast/index.htm . The logs of the firewall are related to broadcast traffic and seem legitimate.

I concluded from this little test that no evidence of hostile activity had been detected, and I could trust the employee when he said this was a fresh Mac installation from the original CDs. I would stress that this test does not replace a Forensic Analysis and does not pretend to, but, given the threat we had to face and my knowledge at the moment, it gave me an acceptable basis to take a decision and document it.

Then everybody went back to business and it took us a few months before implementing counter measures which would reduce, to an acceptable level for GE, the risk of plugging unauthorized devices on the network.

After the incident

The countermeasures we took consisted in two points : (a) Prevent the plugging of unauthorized devices in the LAN, and (b) Detect it when it happens.

PREVENTION
We needed an Acceptable Use policy : policies are the foundation of the security processes in any enterprise. Given the fact that my technical background did not prepare me well for it, I found a valid formulation following the "GIAC Security Officer (GISO)" course. Then an "Acceptable Use Policy" was drafted, submitted to the management, approved by it, distributed and explained to the staff, and finally enforced.
The paragraph specific to the threat of plugging devices in the network reads :

4.5 Unacceptable use of systems :

- . . . Use of unauthorized devices without specific authorization : Users must not physically or electronically attach any additional device to GE systems or networks.

During awareness sessions, threats related to devices plugged in the network were explained to GE employees. The complete AU policy is enclosed as Annex and, as most GE employees speak French, and given the unfortunate fact that such documents are hard to find in Voltaire's tongue on the Internet, I have added the French version, also in the Annex. A last word about the AU policy : the scope of the policy includes external partners, contractors, etc., so that if they come with their own notebook, they must read and understand the AU policy before they can plug it in.

DETECTION
A) CATCHING NEW DEVICES ON THE LAN
The first choice was to use Snort to detect unauthorized Mac addresses on the LAN. I found a discussion about "snorting the Mac address" at Url : http://www.mcabee.org/lists/snort-users/Apr-02/msg00429.html. What I learned there is that "Snort was designed primarily to treat intrusion related to the Internet world ; switches pass Mac address of the packet coming through, but routers do not ; all packets coming out of a router will have the Mac address of the router interface. If you really want to track spoofing on your local network, Arpwatch is a far better tool."

So I started looking for **Arpwatch**. I found it is a Unix-based tool. Like Snort, it is an open source software, and I found a Rpm version on the Redhat site (www.redhat.com) , where it is described as "Network monitoring tool for tracking IP addresses on a network". The installation is straightforward, provided you already have the "libpcap" library running. Arpwatch starts listening on ethernet port and builds a database of pairs IP/Mac address. Every time a new pair is discovered or changed, Arpwatch updates its database, which is located in the file "/var/arpwatch/arp.dat" and generates a message.

I took advantage of our centralized log facility. As Arpwatch generates Syslog messages, the file `syslog.conf` was modified by adding the line "`daemon.* @loghost`", where `loghost` is our central Syslog server, as taught in the course "GiAC Security Essential, Unix day". A rule was added on SL4NT, where any message containing the substring "arpwatch" would generate an e-mail sent to the Sysadmin. I tested this by adding a new device with Dhcp configuration, and Arpwatch immediately detected it.

Arpwatch is simple, reliable and does an excellent job. It is the solution I was looking for to detect unauthorized devices on the LAN. It is now part of the duty of the Sysadmin to monitor it and to react to its alerts.

A Linux box had been added at both gateways together with the Snort box. The tradeoff is that it will not catch packets that do not pass there. Considering that all packets leaving the network must pass at the gateway, and all broadcast packets as well, it is an acceptable risk.

DETECTION
B) REGULAR LOG CONSULTATION
Logs are an invaluable source to detect intrusions attempts. I learned to read Dhcp logs and included in our regular duties. What's more, twice a year our database of IP addresses will be updated with the Mac addresses extracted from the file "`/var/arpwatch/arp.dat`", and differences will be checked.

RESIDUAL RISKS
At the moment, theses countermeasures represent an acceptable level of operation in regard with the threat of unknown devices on our LANs. Anyway, we would not be protected against a skilled and well informed attacker who could spoof both IP number and Mac address, or would launch an attack directly against an internal host in such a way that its packets would never pass through the gateways. These are residual risks, against GE would not be left without protection : Defense in Depth in applied on our resources and we could catch it by hardening the hosts and installing host-based intrusion systems like Black Ice, for example.

References

1) Websense : www.websense.com
2) Syslog Daemon for NT : http://www.netal.com/sl4nt.htm
3) "Hacking exposed", Scambray, McClure & Clure, Ed. Osborne/McGraw-Hill
4) Mac addresses : http://standards.ieee.org/regauth/oui/oui.txt
5) IP Multicasting: ftp://ftp.netlab.ohio-state.edu/pub/jain/courses/cis788-97/ip_multicast/index.htm
6) Rpm of Arpwatch can be found at www.redhat.com , source at http://www.securityfocus.com/tools/142

Annex 1: Acceptable use policy

1.0 Overview
Information technology ("IT"), the vast and ever growing area of computing and electronic data communications facilities and services, is used daily to create, access, examine, store and distribute material in multiple media and formats during the operations of the Giac Enterprises ("GE")
These systems are utilized for business purposes while serving the interests of GE, its clients and partners. Users of GE's IT resources have a responsibility not to abuse these resources.
This policy shall establish guidelines for the Acceptable Use of GE systems. It does not replace the existing general policies of GE, but shall serve to compliment them, within the spirit of the GE enterprise culture.

2.0 Purpose
The purpose of this policy is to **ensure an IT infrastructure that promotes the activities of Giac Enterprise**. It ensures that IT systems are used for their intended purpose and within the spirit of the GE enterprise culture. It promotes Confidentiality, Integrity, Availability and superior performance of systems.

3.0 Scope
This policy applies to employees, whether full time, part time or temporary employees, contractors, consultants, and other workers of GE, including all external companies. It shall also apply to all equipment that is owned or leased by GE, or connected to its network.

4.0 Policy
4.1 Appropriate use of the IT systems
- IT systems are to be used for their intended purpose within the scope of GE activity.
- Employees are responsible for exercising good judgement regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In absence of such policies, employees should consult their supervisor or manager.

4.2 Proper authorization
- Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

4.3 Privacy
- Because of the need to protect GE systems, management cannot guarantee the confidentiality of information stored on any network device belonging or linked to GE.
- Due to security reasons and network maintenance, authorized staff of GE may monitor equipment, systems and network traffic at any moment. Conditions applicable for such monitoring to occur include: :
    - When necessary to identify or diagnose systems or security problems and vulnerabilities,
    - To ensure systems integrity,
    - When required by law,
    - When there are reasonable grounds to believe that a violation of law or a significant breach of GE policy may have taken place,
    - When inspection or monitoring may produce evidence of misconduct,
    - When such access is required to ensure essential operative functions of GE,
    - During mandatory audits.
- In general all access to systems are registered without the user's consent. The review of data without the users' consent may occur only with the immediate supervisor's consent, or during mandatory routine audits.
- Specific aspects of email and Internet usage is a subject to to be discussed in later sections

4.4 Data property
- Data created on company systems remain the property of GE.

4.5 Unacceptable use
The following activities are strictly prohibited :

- Use that impedes, interferes with, impairs, or otherwise harms the activities of others : for example bomb mailing, spamming or hoaxes,
- Harassing or threatening use.
- Use which **damages the integrity of IT systems** such as:
    - Attempts to defeat system security include but are not limited to: :
        - Password cracking,
        - Ports scanning,
        - Network mapping or monitoring,
        - Denial of Service attack,
        - Systems vulnerabilities testing,
        - *NB : those operations are reserved to authorized infosec staf*
    - Trying to guess passwords or trying to access resources without proper authorization,
    - Hiding identity or stealing identities,
    - Knowingly distributing viruses, copying hostile or malicious software on networks or systems,
    - Modifying or canceling data in order to harm or for personal profit,
    - Use of unauthorized devices without specific authorization : Users must not physically or electronically attach any additional device to GE systems or networks.
    - Installing software : all software must be installed by system administrators,
- Use of GE systems to attempt intrusions into external systems or to damage them.
- Installation of "pirated" or other software that are not appropriately licensed for use by GE.
- Any use in violation with contracts,
- Any use in violation with the law,
- Any use in violation of external network policies
- Making fraudulent offers of products or services originating from any GE account.

4.6 Personal account responsibility

Users are presumed to be responsible for any activity carried out under their IT Systems and accounts. Users are responsible for the following:

- To choose, protect and change their password in accordance with the Password policy.
- To avoid, whenever possible, using group accounts ; they will prefer personal account.
- To secured PC and laptops with a password protected screen saver which will lock the system after 10 minutes maximum. Sessions must not be open to anyone when leaving the work station for any extended period of time Windows stations can be locked using the "ctrl alt del" .

4.7 Locking and protecting workstations

- All hosts connected to the GE Internet/Intranet/Extranet, whether owned by the employee or GE, shall be continually executing approved virus-scanning software with a current virus database.
- On every host – except notebooks – floppy and CD drives will be locked. Files registered on CDs, floppies or any electronic device will be copied only by a System administrator, who will ensure that there are no viruses nor malicious programs.
- Software can be installed or removed only by System Administrators.
- Information stored on portable computers and Personal Assistants is especially vulnerable, special care needs to exercised. Protect notebooks and Personal Assistants (PDA's)' in accordance with Infosec recommendations.
- No modem can be installed on fixed workstations. Exceptions must be approved by the Infosec who will publish a related procedure.

4.8 Encryption of data

Users are encouraged to encrypt files, documents and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. However, users must decrypt information when necessary upon official and motivated request.

4.9 Use of Internet

Internet is available to all employees and co-workers within the scope of GE activity.
Every user must exercise sound judgement regarding the reasonableness of Internet usage . He(she) will refer first to his(her) supervisor to know what the guidelines are (ref. 4.1 Appropriate use of IT systems).
Notwithstanding the following guidelines apply to everyone :

- **Access restrictions :**
    - access to chat services and instant messaging is prohibited.

- Access to webmail services (ex: hotmail, yahoo mail, etc) is prohibited. Electronic communications must take place through the GE electronic messaging system.
- Access to chat and webmail services should be blocked automatically. However Internet sites that provide such services can be created at any moment and at any point in time and may pass through the filter of GE. In these circumstances access is not blocked automatically, these restrictions apply in all cases and users are not authorized to access these services.

- **Other unacceptable uses :**
  - Publish or send confidential or sensitive data on the Internet without managements prior written authorization.
  - Use of services that are not necessary to GE operations that would fill all or most of the connection band capacity. For example listening to a radio with non financial content or downloading webcam images, (if they fill the connection capacitiy).
  - Monitoring : every access to any site on the Internet is registered and can be reviewed. This log will be used in particular to verity if users try to circumvent restrictions described e above.
  - Download of programs, for example, programs can be installed only by System administrators, ("4.7 Locking and protection of workstations").They are not allowed to download and install software from the Internet.
  - Sites with hostile content damages the integrity of IT systems is not allowed ("4.5 Unacceptable use") , nobody must access a site with a similar content. This applies particularly to sites of a "hacking" category.

4.10 Emails

The GE electronic messaging system allows to communicate through the Internet during GE operations.

- Reading or using private or non GE email systems is not authorized on the GE network. Electronic communications can take place only through the GE electronic messaging system.
- Users must use extreme caution when opening email attachments, especially when received from unknown senders. Before activating macros in documents (Word, Excel, etc), contact the System administrator who will control them ; in case of doubt, do not activate them. Avoid to click on icons related to programs (extensions "exe", "vbs", "bat", etc.)
- Log : all messages To and From Internet are registered.
- Controls. When controlling emails on a "regular" and "routine" basis, authorized personal will view the sender and recipient addresses, as well as the date and time of the message. The complete content of the message shall be reviewed only in the case of a breach of policy or law , or if a breach of policy of law is suspected. The decision to read the full content of a message must be made with the accord of the supervisor, or, in the case of a security alert, with the consent of the Infosec manager or company management.

5.0 Controls and enforcement

The Infosec department will control regularly the IT systems to ensure that this policy is applied, particularly reviewing logs generated by the accesses and uses of systems.
Infosec will clearly indicate if exceptions are admitted and document them, indicating the motivation, the systems and the users in question.
In general, any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Responsibilities

- **Any user of GE resources** , as defined in the "Scope section", is responsible for applying these guidelines when using GE IT systems.
- The **Security officer** is responsible for reviewing this policy once a year. He/she will organize technical and information training sessions at the minimum of once a year.
- Each **department manager** shall be responsible for distributing and confirming that the policy is read and understood by each employee. The department manager will also ensure that all new hires will be provided a copy of the policy as part of their orientation. Whenever necessary he(she) will provide guidelines concerning personal use of Internet/Intranet/Extranet systems (cf. "appropriate use of IT systems") .
- **Infosec** shall be responsible for auditing IT resources to ensure compliance with this policy on a random selected basis.
- **System administrators** shall configure the systems and provide adequate support in the implementation of this policy.

- **Internal auditor** shall be responsible for the periodic review of IT resources to ensure compliance with this policy and reporting to authorities.

7.0 Definitions

- **Intranet** : the internal network of GE
- **Extranet** : the network of partners and suppliers who have a closer relationship with GE and having a partial access to our network.
- **Infosec** : department of GE who has the responsibility of IT systems security. Details about those individuals in the Infosec department can be located in the "Manuel de la politique de sécurité".

8.0 Related documents

Exceptions :

- Use of personal mail accounts (POP)
- List of modems connected directly to the workstations

Procedures

- Use of modems with "pcanywhere" on the workstations
- Recommendation for the protection of laptops and Pdas

9.0 Cancellations

10. Revisions history

- Effective date :
- Next revision :

Annex 2: Utilisation acceptable des systèmes (Directive)

1.0 Aperçu
Les Technologies de l'Information (" IT ") représentent l'ensemble des techniques, des systèmes et des services utilisés pour le calcul et la communication des données électroniques. Elles sont utilisées chaque jour pour créer, accéder, examiner, enregistrer et distribuer des données dans le cadre de l'activité du Giac Entreprises (" GE ").
Les systèmes IT doivent être utilisés dans un but professionnel et pour servir les intérêts du Groupe, des clients et des partenaires de GE. Dans ce cadre, les utilisateurs ont la responsabilité de ne pas abuser des ressources qui leur sont mises à disposition.
Cette directive établit les lignes à suivre pour une utilisation acceptable des systèmes de GE. Elle n'a pas pour but de remplacer les directives plus générales du groupe GE, comme le règlement interne par exemple, mais de les compléter dans le cas spécifique de l'utilisation des systèmes, en gardant à l'esprit de la culture d'entreprise de GE.

2.0 Objectif
L'objectif de cette directive est de **définir l'utilisation acceptable des systèmes IT afin qu'ils puissent promouvoir les activités du Groupe Giac Entreprises** . La directive s'assure que les systèmes sont utilisés dans le but pour lequel ils sont mis à disposition et dans l'esprit de la culture d'entreprise de GE. Elle veut promouvoir la Confidentialité, l'Intégrité, la Disponiblité et les Performances maximales des systèmes.

3.0 Personnes et systèmes concernés
Cette directive concerne tous les employés fixes ou temporaires, cadres, consultants, ou toute autre personne travaillant pour le Groupe Giac Entreprises, sociétés externes y compris. Elle s'applique également à tout le matériel possédé ou loué par GE, ou connecté sur son réseau.

4.0 Directive

4.1 Utilisation appropriée des systèmes
- Les systèmes IT doivent être **utilisés dans le but pour lequel où ils sont mis à disposition** , dans le cadre de l'activité de GE.
- Chaque utilisateur doit exercer son propre jugement pour déterminer quelle la **part d'utilisation personnelle raisonnable des systèmes** . Il se référera d'abord au responsable de son département qui doit créer une ligne de conduite concernant l'utilisation personnelle des systèmes Internet/Intranet/Extranet. En l'absence de telles directives chaque employé devra consulter son supérieur ou sa direction.

4.2 Accès autorisés
- Les utilisateurs ne peuvent accéder qu'aux éléments des systèmes IT pour lesquels ils ont reçu une autorisation appropriée.

4.3 Protection de la sphère privée (privacy)
- En raison des besoins de protection des systèmes de GE, la Direction ne peut pas garantir la confidentialité des informations enregistrées sur les systèmes appartenant ou reliés au réseau de GE.
- Pour des raisons de sécurité et de maintenance du réseau, le personnel autorisé de GE peut monitorer les équipements, les systèmes et le trafic réseau à n'importe quel moment. Les conditions dans lesquelles un tel contrôle peut avoir lieu sont :
    - lorsqu'il est nécessaire d'identifier ou de diagnostiquer des problèmes *ou des vulnérabilités* sur des systèmes et sur le réseau.
    - lorsqu'il s'agit de préserver l'Intégrité des systèmes
    - lorsque cela est requis par la loi
    - lorsqu'il y a une bonne raison de croire qu'il y a violation d'une directive ou de la loi
    - lorsque l'inspection ou le monitorage peut déterminer s'il y a eu un écart de conduite
    - lorsqu'un tel accès est requis pour assurer les fonctions opératives essentielles de GE
    - lors des audits obligatoires
- Ainsi, de manière générale, tous les accès aux systèmes seront enregistrés sans autorisation préalable des utilisateurs. La consultation de ces données sans le consentement de l'utilisateur aura lieu seulement avec l'approbation du responsable de département, ou dans le cadre de contrôles de routine obligatoires.

- Certains aspects spécifiques du contrôle de la poste électronique et de l'utilisation d'Internet font l'objet d'un chapitre séparé plus loin dans cette directive.

4.4 Propriété des données

- Toutes les données créées sur les systèmes du groupe restent la propriété de GE.

4.5 Utilisation inacceptable des systèmes

Les actions et comportements ci-après ne sont pas autorisés :

- Toute utilisation qui interfère avec les activités des autres ou provoque un dommage : par exemple les messages envoyés en masse (" bomb mail "), les messages non sollicités (" spam ") ou les virus de type canulars (" hoaxes ")
- Toute utilisation qui a pour but de menacer ou de harasser autrui
- Toute utilisation qui **menace l'Intégrité des systèmes** , soit :
    - Les **tentatives de déjouer la sécurité IT** . Les moyens peuvent , sans s'y limiter, être les suivants :
        - programmes qui devinent les mots de passe (" password cracking ")
        - balayage des ports (" ports scanning ")
        - toute forme de monitorage ou de reconnaissance du réseau
        - attaque de type Déni de Service
        - les tests de vulnérabilités des systèmes (" vulnerability assessment ").
        - **NB : Ces opérations sont réservées au personnel autorisé de l'Infosec.**
    - Essayer de deviner les mots de passe ou toute tentative d'accéder aux ressources pour lesquelles on ne dispose pas d'autorisation
    - Cacher son identité, se faire passer pour un autre utilisateur.
    - Distribuer des virus lorsqu'on le fait en toute connaissance de cause, ou en installant ou copiant des programmes hostiles ou malicieux sur les serveurs ou le réseau
    - Modifier ou effacer des données dans le but de nuire ou pour son profit personnel
    - L'installation et l'utilisation d'appareils non autorisés sans accord spécifique des administrateurs de système.
    - L'installation de logiciels sur les systèmes sans passer par les administrateurs de systèmes.
- Toute utilisation des systèmes de GE pour tenter de s'introduire ou endommager des systèmes externes
- L'installation de logiciels piratés , de copies non autorisées ou pour lesquelles on ne dispose pas de licence.
- Toute utilisation en violation avec les contrats
- Toute utilisation en violation avec la loi
- Toute utilisation en violation avec les directives des réseaux externes
- Faire des offres frauduleuses de produits ou de services à partir d'un compte chez GE.

4.6 Responsabilité personnelle

Chacun est présumé responsable des activités qui sont menées sur son système et avec ses comptes. Dans ce cadre les utilisateurs devront :

- choisir, protéger et changer leurs mots de passe comme indiqué dans la directive " Mots de passe ".
- éviter, dès que cela sera possible, d'utiliser des comptes de groupe pour leur préférer des comptes avec une identification personnelle.
- sécuriser les PCs et laptops avec un écran de veille protégé par mot de passe qui bloquera le système après 10 minutes au maximum. Les sessions ne doivent pas être accessibles à tous lorsqu'on quitte son bureau ; il faut alors bloquer sa station avec la séquence de touche " ctrl alt del ".

4.7 Blocage et protection des postes de travail

- Tous les postes de travail qui sont connectés au réseau de GE, qu'il soient propriété de GE ou pas, doivent à tout moment exécuter un programme anti-virus approuvé par l'Infosec avec un base de données de virus ajournée.
- Sur tous les postes de travail - à l'exception des notebooks – les accès aux lecteurs disquettes et cd-rom seront bloqués. Les fichiers contenus sur les CDs, disquettes ou toute forme de stockage de masse électronique, seront copiés par un administrateur de système qui vérifiera qu'il n'y ait ni virus ni programme hostile.
- Les programmes sur les postes de travail et le serveurs ne peuvent être installés, modifiés ou effacés que par les administrateurs système.

- Parce que les informations stockées sur les ordinateurs portables et les assistants personnels sont particulièrement vulnérables, une attention particulière doit être portée à leur protection. L'infosec publie les recommandations " portables " et " assistants personnels " à cet effet.
- Aucun modem ne peut être installé sur les postes de travail fixes. Les exceptions, si elles devaient être nécessaires pour la maintenance de logiciels, devront être approuvées par l'Infosec qui publiera une procédure adéquate.

4.8 Cryptage

- Les utilisateurs sont encouragés à crypter les fichiers et les documents pour les protéger lorsqu'ils sont enregistrés sur disque ou envoyés sur les réseaux. Les utilisateurs doivent cependant être prêts à décrypter les informations lorsque cela est nécessaire sur demande officielle et motivée.

4.9 Utilisation d'Internet

Internet est mis à disposition des collaborateurs dans le cadre des opérations de GE. Chaque utilisateur doit exercer son propre jugement pour déterminer sa part d'utilisation personnelle raisonnable d'Internet, et se référera d'abord à son responsable de département pour connaître la ligne de conduite à suivre (réf. 4.1 " Utilisation appropriée des systèmes "). Cependant les aspects suivants s'appliquent à tout le monde :

- **Restrictions d'accès**:
  - les accès aux **discussions en ligne** (" chat ") et autres services de **messagerie instantanée** (IRC, " Instant messaging ", …) ne sont pas autorisés.
  - Les accès aux services de messagerie par interface Web (" **Webmail** ", par exemple " hotmail ", " bluemail ", " yahoo mail ", etc.) ne sont pas autorisés non plus. Les communications électroniques ne peuvent se faire que par l'intermédiaire du système de poste du Groupe.
  - Les accès aux services de discussion et de messagerie Web seront en principe bloqués automatiquement. Cependant il est dans la nature d'Internet que des sites ou des services qui entrent dans cette catégorie peuvent être créés à tout moment et échapper momentanément au filtre du groupe GE. Dans ce cas, même si l'accès n'est pas bloqué automatiquement, cette restriction s'applique et l'utilisateur n'est pas autorisé à y accéder.
- **Autres utilisations inacceptables** :
  - Publier ou envoyer des informations sensibles sur Internet sans l'accord de la Direction.
  - Utiliser des services qui ne seraient pas nécessaires aux opérations de GE et occuperaient une grande partie ou toute la capacité de la connexion à Internet. Un bon exemple est écouter un service radio non professionnel ou consulter des images Webcam qui occuperaient une large bande passante.
- **Monitorage** : chaque accès au site est enregistré et peut être consulté .Ce log des accès sera utilisé en particulier pour vérifier si des utilisateurs essaient de contourner les restrictions décrites ci-dessus.
- **Téléchargement** de programmes : de la même manière que les programmes ne peuvent être installés que par les administrateurs systèmes (" 4.7 blocage et protection des postes de travail "), il n'est pas permis de télécharger et d'installer des programmes depuis internet.
- **Sites à contenu hostile** : de la même manière que tout utilisation qui menace l'Intégrité des systèmes n'est pas autorisée (voir " 4.5 utilisation acceptable "), on ne doit pas accéder sciemment à un site qui offre un contenu similaire. Cela vaut en particulier aux sites de la catégorie " hacker " ou similaire.

4.10 Courrier électronique

Un service de messagerie interne relié à Internet est mis à disposition des collaborateurs dans le cadre des opérations de GE. Dans ce cadre :

- la consultation et l'utilisation du courrier électronique privé ou appartenant à une société en dehors du groupe n'est pas autorisé sur le réseau de GE. Les communications électroniques ne peuvent se faire que par l'intermédiaire du système de messagerie du Groupe.
- les utilisateurs doivent être extrêmement prudents lorsqu'ils ouvrent des pièces jointes, spécialement si elles sont envoyées par des expéditeurs inconnus. Avant d'activer des macros dans des documents (Word, Excel), il faut contacter l'administrateur système qui procédera à un contrôle ; en cas de doute, ne pas l'activer. Evitez de cliquer sur les icônes qui représentent des programmes pour les exécuter (extensions " exe ", " vbs ", " bat ", " msi " etc.).
- **Enregistrement** : tous les messages De et Vers Internet sont enregistrés.
- **Contrôle** : dans le cadre de contrôles ponctuels et réguliers des emails, les personnes autorisées pourront visualiser les adresses de l'expéditeur et du destinataire ainsi que la date et l'heure du

message. Le contenu complet des messages sera consulté seulement dans les cas de violat ions des règlement internes ou de la loi, ou lorsqu'on soupçonne une telle violation. La décision de lire le contenu complet des messages doit être prise avec l'accord du responsable , ou dans le cas d'une alerte concernant la sécurité, par un responsable de l'Infosec ou un membre de la direction.

5.0 Contrôles et Sanctions

Le département Infosec procédera à des contrôles réguliers des systèmes IT pour s'assurer que la directive d'utilisation est appliquée, en particulier en consultant les traces électroniques générées lors des accès et l'utilisation des systèmes.

Il devra clairement indiquer si des exceptions sont admises et dans ce cas en documenter le motif, les systèmes et les utilisateurs concernés.

De manière générale, tout employé qui viole cette dir ective pourra être sujet à des sanctions disciplinaires, qui peuvent aller jusqu'au licenciement.

6.0 Responsabilités

- Tous **les utilisateurs des ressources de GE** , tels qu'ils ont été définis dans la sectio n " Personnes et systèmes concernées ", ont la resp onsabilité de suivre les consignes de cette directive dans l'utilisation quotidienne des systèmes.
- **L'Officier de Sécurité** a la responsabilité de réviser cette directive une fois par année. Il (elle) organisera des séances d'information au moins une fois p ar année, ainsi que la formation nécessaire pour tous les utilisateurs.
- Chaque **responsable de département** a la responsabilité de distribuer cette directive et de confirmer qu'elle a été lue et comprise par chaque collaborateur. Il s'assurera que tous les nouveaux employés en reçoivent une copie. Il devra, s'il le juge nécessaire, définir la ligne de conduite à suivre dans son département concernant l'utilisation personnelle des systèmes Internet / Intranet / Extranet, en accord avec la Direction Générale (utilisation appropriée des systèmes).
- Le département **Infosec** a la responsabilité de contrôler les ressources IT à intervalle irrégulier pour s'assurer que la directive est suivie.
- Les **administrateurs** doivent configurer les **systèmes** et apporter leur support technique pour que la directive puisse être effectivement implémentée.
- Le **réviseur interne** a la responsabilité de contrôler les systèmes pour s'assurer qu'ils sont en règle avec cette directive, et de le reporter aux autorités.
-

7.0 Définitions

Intranet : le réseau interne du groupe GE.

Extranet : les réseaux des partenaires ou fournisseurs avec lesquels le groupe GE entretient des relations privilégiées et qui ont un accès partiel à notre réseau.

Infosec : Département du groupe qui s'occupe de la séc urité des systèmes IT. La composition de l'infosec est détaillée dans la manuel de politique de sécurité.

8.0 Documents liés la directive

Exceptions :

- Utilisation de comptes de postes personnels (pop)
- Modems connectés directement sur les postes de trav ail

Procédures

- Utilisation des Modems avec Pcanywhere sur un poste de travail
- Recommandations pour la protection des laptops et des assistants personnels

9.0 Annulations

10.0 Historique des révisions

- Entrée en vigueur :
- Prochaine révision :

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS