Global Information Assurance Certification Paper

The Laocoon Option - Active Defense of Network Infrastructure

Table of Contents

Abstract/Summary

In the latter part of 2002, the City of Seattle made a long overdue hiring decision. One afternoon, I wandered into yet another of the less than thrilling, time-consuming meetings that are an IT manager's tedious lot in life, and met Mr. Kirk Bailey, our new Chief Information Security Officer.

I was relatively new to security as a career path, but I was enthusiastic about being more involved in the City's security decisions. The meeting at which I met Kirk was the Information Technology Security Board (ITSB). We had been meeting for many months, working on a nascent security policy and praying for the arrival of a CISO to guide us.

Be careful what you ask for.

Mr. Bailey is a rotund, jolly, boisterous, opinionated genius. He is a well known and some might say infamous personage in the information security world. I was a little overwhelmed with his passion for information security in that first meeting, but I have learned to respect and appreciate him.

The City now has an official information security policy and there are many more security irons in the fire on which I am proud to work with Kirk. One of the most compelling of those projects is the subject of this paper.

One day Kirk and I were discussing the many different ways the City should prepare itself against cyber attack. Kirk said, "Have you ever thought about actively defending ourselves?" I thought, "Here we go…," but I said, "No, I don't think so. What do you mean?"

He told me that he had been considering the implications of defending networks and infrastructure by actively attacking the attackers. The hacker wannabe in me immediately thought, "Cool!" But then, the more sensible and law-abiding side said, "But wouldn't that mean engaging in the same illegal activities that the attackers are using against us?"

With a sly grin Kirk answered, "Maybe…"

Thus was born one of the most challenging, enjoyable and thought provoking projects I have ever been involved in. We called it the Laocoon Option. It is named for the Trojan seer who warned the rulers of Troy not to bring the huge wooden horse, left as a gift by the Greeks, into the heart of their City. For his trouble the gods sent serpents to kill his sons and he was torn to pieces trying to defend them. His story represents the tragedy and suffering that can accompany the espousal of tough decisions in the face of bureaucratic blindness. We hope that by examining these options carefully and with forethought, we can avoid the pitfalls (and serpents) of having to make these tough decisions under the stress of an actual cyber-attack.

I will talk about the reasons we think this is a viable and important option. Then I'll discuss the legal considerations involved. I'll take a look at policy and protocols that we have outlined for our use in the City and discuss how we established them. Finally, I'll look at the strategies and toolsets that are necessary to pull this off and talk about how we plan to prepare for deployment.

The Why Questions

Why is this important? Why should you or your organization be thinking about this? Why would anyone in their right mind even consider sticking their head into this liability lion's mouth!? These are all good questions that have been debated extensively in many forums. I will attempt to answer them as the starting point for this discussion.

Why is this important?

As noted in the introduction, this project grew out of a discussion about the different ways to respond to attacks. Everyone in the information security field is well aware of the exponentially increasing hostile activity that our networks defend against everyday. The incidences of port scanning are steadily increasing. We receive new vulnerability updates from our software vendors sometimes on a daily basis. Spam, or un-solicited email, has grown to a point that it can legitimately be called a denial of service attack on the entire messaging infrastructure. The rule of "defense in depth" that all of us live and breathe, demands that we use every tool available to us in this constantly escalating war.

The problem is, we as the "white hat" community are in a losing proposition. We, by design and our very nature, work within the law and in cooperation with our industries and peers. The adversary is not tied down to those ethical, moral and legal restrictions. There are defensive strategies such as well configured IDS (Intrusion Detection Systems), current virus protection, good security policy and tested incident response practices. However, those are all too often found lacking in this technological battle.

So, we simply must consider every tool at our disposal. And if one of those tools requires us to break new ground and enter into the worlds of our attackers, then we'd better have thought about it ahead of time. We need to have established policy and protocols that have been vetted by our management and legal advisors, so that when we step into that minefield we do so with the best knowledge possible of the risks we take and where we need to place our feet.

I believe it is possible, and in fact imperative, to develop those protocols, enforce those policies, and exercise and refine those options to the extent that we can limit our liabilities while mitigating the risks involved. This is the essence of good

security practice: understanding and quantifying risk in order to proceed in the correct direction when faced with an incident.

Why should you or your organization be thinking about this?

I had one representative of a local government tell me that his organization preferred to not even consider these options so that if the situation ever arose, they could plead ignorance. If they had never developed the policies, protocols or tools to react, they would never have to make that tough decision! Pondering that later along with some of my legal advisors, I wondered if a policeman could escape liability for protecting the citizenship by refusing to learn how to use his or her gun? If they came upon a criminal who was about to shoot someone, they wouldn't have to think about pulling out their weapon to stop her because they had never taken the training! It seemed like a good analogy to me, and in fact my legal buddies thought I might have a point. The idea that you can escape liability by refusing to be prepared might not wash too well, especially if the public is harmed.

Therein lies the most compelling reason to be thinking about this. You need to seriously consider who will be harmed and to what extent, if your network is compromised. In the City of Seattle, we have a unique perspective in this regard. The City supports much of its own infrastructure including water, energy, waste, and of course public safety. The loss of control over our network could quite possibly affect the safety and well being of our citizens. There is a point at which we may well have to make a decision between stepping over the somewhat vague and ill-defined legal line in computer defense or seeing our citizens harmed.

Your situation may not be as drastic. That is why you should consider this question carefully. As you'll see in the protocols section, there are many levels of response that can be engaged in. The level to which you are willing to take any active defense measures must be weighed against the actual risk of harm and the risks you and your organization are willing to take to defend against that harm.

Why would anyone in their right mind even consider sticking their head into this liability lion's mouth!?

This last question is rhetorical and meant lightly to take us into the next chapter about legalities. As one person put it to me, "OK, I can see where this might actually make sense, but do you really want to be the person to deliver yourself or your company into court to argue the point?"

I think most of us would agree that is an uncomfortable question to think about. Some may be willing to put themselves in jeopardy but when it comes to exposing their employer to the possibility of court proceedings, they quail at the thought. And rightly so. Our ethics are all about protecting our employers from harm. It is a sticky wicket with no easy way through.

We've spent a great deal of time discussing this with some of the best legal minds in the country. They haven't given us all the answers yet, and they are fond of reminding us that they will be glad to supply us our "soap on a rope" and visit us now and then in our incarceration, but they have come up with some interesting theories that I will do my best to relate in lay-person terms below.

Legalities

There are several laws that may apply to you if you practice active defense measures. Besides the laws you might violate, there are some interesting theories as to which laws or theories of law might justify your actions. First I'll talk about the computer related laws that might create a liability and specifically how they would relate to the actions you might be taking. Then I'll look at the newest legal theories about how you might justify your actions and limit your liabilities.

Existing Law

First, there is the federal Computer Fraud and Abuse Act that every information security professional should be well aware of. Basically it forbids any unauthorized access to a protected system (for a definition of "protected system" see the section on policy that follows), or access above that for which you are authorized if that access causes $5000 or more in damage. It also forbids the trafficking in any information you might gain while accessing that computer such as passwords or other access information. And most important to you as a security professional, federal law enforcement (you know, those serious looking, polite folks with the wingtips?) might arrive at your door if you are in violation. They have the right to arrest you, take all computer equipment you have touched and give it back when they feel like it. This could be a small blot on your employment record if it happened at your place of employment.

It is also important to note that there may be civil liabilities as well, under this law. Thus, even though you might be under the damage levels of the law for a criminal case, you could still find yourself defending against a civil action.

Another federal law worth thinking about is the Wiretap Act. It forbids the interception, disclosure or use of any information transmitted electronically or through wire or even orally. It provides some nasty consequences if you are found guilty. There are some interesting exceptions however that we will talk about in the next section.

A similar federal statute is the Electronic Communications Privacy Act (aka ECPA). This prohibits unlawful access to electronic communications or disclosure of any information gained.

All of these laws could potentially come into play in the procedures you might consider for active defense. For instance, it is quite conceivable that a port scan

of an intruder could be construed as a violation of the Wiretap Act or ECPA. If any action you take could be interpreted as having caused damage, you might find yourself on the wrong side of the Computer Fraud and Abuse Act.

The discussion of damage brings us to a new federal act that has changed the legal landscape considerably. It has affected many of the rights of US citizens, but germane to our discussion it made some significant changes to the laws noted above. I'm referring to the Patriot Act.

The Patriot Act changed the definition of damages. As noted above it does not come into play until and unless the action causes $5000 or more in damages. However, it was not very clear what those damages could entail. One court in the case titled United States vs. Middleton, 231 F. 3d 1207, 1210-11 (9th Cir. 2000) created a definition that included the cost of responding to an incident, damage assessment, restoration of systems and data, and any lost revenue caused by the intrusion. The Patriot Act amended the Computer Fraud and Abuse Act to adopt that definition.

The Patriot Act also amended the damages section by making it allowable to aggregate the damages to different protected computers that occur over a one-year period. Both of these changes significantly lower the bar and make it that much more likely that you might be held liable for damages.

Significantly, they also raised the maximum penalty for first time offenders to 10 years for violation of the Computer Fraud and Abuse Act. Gives you pause, doesn't it?

In our state (as in most states) we also have other laws that apply to computer crime. Washington State has a Malicious Mischief statute that addresses the damage part of the equation. However, it sets significantly lower damage requirements. Damage of $1500 or more can be charged as a class B felony! Ouch! It also defines damage much more inclusively. It includes alteration, damage or erasing of information; the impairment or interruption of use of that information; or even diminution of value of any of the information. Washington State's Computer Trespass law doesn't require ANY damage to come into play. Simply having unauthorized access to a computer system or database that doesn't belong to you makes you liable to prosecution. This again lowers the bar even further on what might get you into deep doo doo (a technical legal term). Our state (and most others) also has similar statutes regarding privacy that parallel or enhance the penalties under the federal ECMA.

There are no doubt other laws that could be used to hurt you, but I'm sure you are already sufficiently worried. And you should be. In this regard you can't be too cautious and you can't be too paranoid. But there is some light coming down the tracks. With any luck it will be a kind and friendly guide out of the tunnel and not a train.

Legal Justifications

There are a lot of people talking about the ways that we might justify our actions in the legal arena. I will talk about a few of the more promising suggestions, but understand this is a wide-open and relatively new area of law. It is far from settled as to which, if any, of these arguments might stand the test of litigation.

The most frequently suggested legal justification for defending your networks is the law relating to self-defense. In all jurisdictions there are laws defining the limits and restrictions of self-defense. In Washington State the part of the criminal law that might be applied to active defense states that force may be used to defend yourself:

> (3) Whenever used by a party about to be injured, or by another lawfully aiding him or her, in preventing or attempting to prevent an offense against his or her person, or a malicious trespass, or other malicious interference with real or personal property lawfully in his or her possession, in case the force is not more than is necessary;
>
> (4) Whenever reasonably used by a person to detain someone who enters or remains unlawfully in a building or on real property lawfully in the possession of such person, so long as such detention is reasonable in duration and manner to investigate the reason for the detained person's presence on the premises, and so long as the premises in question did not reasonably appear to be intended to be open to members of the public.

(State of Washington RCW 9A.16.020 - Use of force -- When lawful)

This might seem to indicate that if you suspect you are about to be injured, or your property is about to be damaged, you could lawfully cause damage to the perpetrator of that harm. However as this law relates to using force against a person and not their property, it is anything but clear whether that will hold up in court to justify an active defense action.
For one thing these regulations are meant to provide a defense if you are charged criminally and might not apply in a civil suit. In fact there is some thought that because of the difficulty inherent in active defense you may well be at risk for civil liabilities. For instance, it is often very difficult to know who is the actual attacker. It is also difficult to be proportional in your response (using only the amount of force that is necessary and no more). Taking ill-considered or simply mistaken actions in either of these cases could cause harm that would expose you to civil liabilities.

Another more promising area of common law that might apply is nuisance law, which promises the citizenry the right to use and enjoy private property. Further it offers abatement rules if someone or something can be considered a public or private nuisance. A public nuisance is defined as one that interferes with a public right such as public health, safety, peace, comfort or convenience and that interference is continuing or could have a long-term effect on that public right. A private nuisance is one who commits “nontrespassory invasion” (I don’t know –

ask your lawyer!) of the enjoyment or use of private property caused by an intentional or even negligent action.

The abatement of these nuisances allows for trespass to chattels, meaning you can trespass onto someone else's chattel (property) in order to stop the nuisance. It still demands proportionality however, so as always you must know what you are doing and why and use only the force necessary to stop the nuisance and no more (*Christiansen, John R.)*

It has been well established that limited and unobtrusive port scans of computers outside your authority do not always violate the law. There is case law out there that was decided on the side of the defendant (Scott Moulton and Network Installation Computer Services, Inc. v. VC3 Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000)) which allowed that scanning of a network to test for vulnerabilities, under the facts of that case, did not violate the Computer Fraud and Abuse Act or the Wiretap Act.

There are also some precedents when speaking of protecting the public safety that are mentioned below in the policy discussion in the section titled Philosophy and Precedents. All of these are tentative and still remain to be tested. But you should be aware of them and be cognizant of how they affect the overall risk level of your actions. In other words, stay tuned, there's much more to come!

Policy and Protocol

When we started developing the procedures for active defense measures we had some long discussions on our team. We thought about what models would be appropriate to emulate. As a martial artist, I was inclined to consider the idea of training ourselves with the goal of avoiding harm to our attackers. One tenet of the martial arts is that you prepare to defend yourself but you strive to do everything in your power to avoid conflict, or to divert an attack without causing harm.

Some of our team members were members of the police department and they mentioned an internationally known law enforcement protocol called the continuum of force. This is analogous to the martial arts training I mentioned above. We were able to obtain a copy of the Seattle Police Department's Use of Force policy and I used that as a template to create the 'Use of Active Defense' policy that follows.

Philosophy and Precedents

The philosophy of the Use of Information Technology Active Defense Measures against intrusions or attacks upon critical information infrastructures is based upon precedents, which are common, internationally accepted, and codified within the fire and public safety protocols. The firefighter's or law enforcement

official's authority extends to property when they are controlling or suppressing a fire, or when protecting persons or property from existing or imminent danger.

This refers to a firefighter's authorization to enter private premises without notice where it is necessary for the purpose of controlling or suppressing a fire, or protecting persons or property from an existing or imminent danger (excerpted from the Quebec Fire Safety Act), the police use of force doctrine (Seattle Police Department Use of Force Policy), and other applicable laws.

Applying these protocols to active defense of information infrastructures would authorize the Information Technology Security Officers to:

A. Use the necessary means to intrude into a hostile computer or information system where there is serious threat to the protected systems and where said threat to the information infrastructure could potentially damage persons or property, for the purpose of removing or reducing the threat;
B. Prohibit access to and interrupt or divert traffic to the hostile computer (or a compromised interim device);
C. Authorize damaging of the hostile system to prevent the effects of the hostile intrusion;
D. Order any other measure necessary to secure the hostile computer and gain necessary forensic evidence; and
E. Accept or require, where the resources in house are insufficient, the assistance of any person or entity capable of providing assistance (i.e. Department of Defense, Department of Justice, law enforcement personnel)

This implied authority carries with it the responsibility of following strict protocols as to the determination of the identification and location of the actual intruder and their intent. It also requires follow-up documentation and review, the formats to be developed based on precedents from the fire and law enforcement protocols.

Policy

The City's use of active defense measures policy implements local, state and federal laws. The City asserts that to the extent that this policy may contain additional provisions not addressed in state law, such provisions are not intended, nor may they be construed or applied, to create a higher standard of care or a duty toward any person or to provide a basis for criminal or civil liability against the City, its officials or individual information technology security officers (hereafter referred to as "officers"). However, violation of such additional provisions may form the basis for disciplinary or other action. Personnel shall use only the minimal amount of active defense measures necessary to overcome a threat to the City's information technology infrastructure or illegal or uninvited access to that infrastructure.

I. Definitions

A. Active Defense Applications: the application tools used to defend information infrastructure from hostile systems.
B. Active Defense Measure: the action (compulsion or restraint) exerted upon a hostile computer or information system, which could include verbal or written warnings or use of application tools, to overcome a threat to the City's information technology infrastructure or illegal and uninvited access to that infrastructure.
C. Denial of Service Counter Attack: a general term for one type of active defense measure - the overwhelming of a hostile computer by the intentional inundation of data packets.
D. Functional Termination: the intentional application of active defense measures through the use of software applications or any other means reasonably likely to cause suppression of, or serious data loss to, the hostile computer.
E. Hostile Computer: any information technology hardware or system used to initiate an aggressive attack on the City's information technology infrastructure. Also, any such hardware that is used, whether with the owner's knowledge or not, to distribute an attack.
F. Information Technology Security Officers: any person or persons acting in an official capacity or with the authority of the City for the purposes of securing the City's information technology infrastructure.
G. Necessary: no reasonably effective alternative to the use of active defense measures appeared to exist and that the amount of active defense measures used was reasonable to effect the lawful purpose intended.
H. Protected System: any vital portion of the City's information technology infrastructure that is being safeguarded by information technology security officers.
I. Serious harm: any activity or attack that has the imminent potential to compromise public safety or to cause destruction of the City's critical information systems infrastructures (protected systems).

II. Levels of Response and Applications

In the event of an attack on the City's critical information systems infrastructure there are varying levels of response possible. There is no rigid hierarchy of specific sequences of the levels of response that require one level to be used before another. The level of response, and the types of applications used to respond, are dictated by the assessed risk and the severity of the attack. It is the responsibility of the officers who are monitoring the attack to make an informed decision as to the appropriate proportional response. The following are general categories of Active Defense Measure responses and applications forming a continuum from moderate responses to the most serious applications. *[Note: This section to be modified or expanded upon to reflect command and control procedures and use of tools.]*

A. Advertised presence of Intrusion Detection Service:

1. Warnings sent to intruder notifying them that their presence has been detected.
2. Repeated on decreasing intervals.

B. Warning messages:
   1. Cease and desist messages sent to intruders and their ISP (Internet Service Provider) via computer network messaging.
   2. Cease and desist messages sent via telephone to intruders and their ISP.

C. Scans and probes of the intruding computer systems:
   1. Traceback probes; FTP (File Transfer Protocol) or HTTP (Hyper Text Transco Protocol) scans for possible access to offending computers.
   2. Other identification probes that do not cause damage to the offending computer but can be “felt”.

D. Non-terminal counter attacks:
   1. The use of defensive applications to block the attack.
   2. The use of firewall or other filters to close off all access from the attacking computer or information system.

E. Approaching terminal counter attacks:
   1. The use of more powerful defensive applications to actually suppress the attacking systems and put them out of operation.
   2. Denial of Service Counter Attack.

F. Functional Termination:
   1. The use of defensive applications to functionally terminate the attacking computer(s) or information systems.

III. Use of Active Defense Measures

A. Officers shall have used active defense measures whenever they:
   1. Use active defense measures against a hostile computer in the defense of a protected system from assault or the threat of assault, or
   2. Overcome a hostile computer’s aggression, or
   3. Use containment applications to place a hostile computer into isolation, or
   4. Use any application to suppress a hostile computer, or
   5. Use active defense applications against a hostile computer which causes damage, could reasonably be expected to cause damage, or results in a complaint of damage.

B. The use of active defense measures, other than functional termination, by an officer in the performance of official duties is justifiable when necessarily used:
   1. In defense of a protected system, or
   2. In the performance of a legal duty (e.g., protecting persons and property, providing for public safety, enforcing the law and otherwise performing the duties and obligations of an officer), or

3. To prevent an unprotected, unpatched computer or other information technology hardware system from being used as an instrument to commit an act dangerous to the protected system, or
4. In enforcing necessary restraint for the protection or restoration to health of the protected system, or
5. To effect the identification and prosecution of a person or persons responsible for initiating, programming and carrying out an aggressive attack on the protected systems by gathering forensic evidence regarding the identity, location and ownership of the systems initiating or being used in the attack.

C. Supervisory notification and reporting will be completed according to policy.

IV. Use of Active Defense Applications

A. An officer shall not use an active defense application for other than lawful purposes.
B. While engaged in the performance of their official duties, officers may use an active defense application against a hostile computer when the use is justifiable.
C. An officer will not be censured or disciplined by the City for a decision not to employ the use of an active defense application to suppress, deter or prevent the avoidance of detection of the hostile computer from forensic evidence gathering even though the use is justifiable.
D. Using an active defense application against an interim and possibly innocent computer system:
    1. An officer shall not use an active defense application against an interim computer system except when the use is justifiable, and
    2. That the necessary use of an active defense application to suppress, deter, or prevent the avoidance of detection of the hostile computer from forensic evidence gathering outweighs the impact to potentially innocent computer systems that may result from the officer using an active defense application.
E. Warnings, scans and probes do not constitute an active defense application.
F. Supervisory Notification Required
    1. Before an officer uses any active defense application, they will notify a supervisor.
    2. Whenever an active defense application is used or applied, a Use of Active Defense Measures reporting packet will be completed.

V. Use of Denial of Service Counter Attacks

Denial of service counter attacks are considered potentially terminal to the extent documented in current research. Therefore, the use of denial of service counter attacks shall be limited to those circumstances where the use of the active defense measure of functional termination is justifiable.

VI. Use of Functional Termination

A. In using functional termination to suppress or deter any hostile computer from the commission of any attack, an officer must have probable cause to believe that the hostile computer, if not stopped, poses a threat of serious harm to the protected system. Among the circumstances which may be considered by an officer as a "threat of serious harm" include, but are not limited to, the following:
   1. The hostile computer threatens the protected system with a known hostile scan or other signature preparations for an attack* in a manner that could reasonably be construed as an imminent threat of serious harm, or [*in progress: Appendix ??: Principals of Engagement Command and Control]
   2. There is probable cause to believe that the hostile computer has been used as an instrument to commit any attack involving the infliction or threatened infliction of serious harm, or
   3. To prevent avoidance of detection of the hostile computer from forensic evidence gathering.

B. The use of functional termination by an officer in the performance of official duties is justifiable when necessarily used:
   1. To suppress or deter a hostile computer which the officer reasonably believes is being used, or will be imminently used, as an instrument to commit a serious and aggressive attack on the protected system, or
   2. To lawfully suppress a denial of service attack if the hostile computer is armed with a known functional termination application, or
   3. To prevent the avoidance of detection by the hostile computer from forensic evidence gathering.

Reporting the Use of Active Defense Measures

Whenever an IT officer performing security enforcement related activity uses active defense measures as defined within this policy, they shall be required to complete notification and reports according to policy and this section. Use of warnings, scans and probes must be reported to a supervisor, but do not require the completion of a Use of Active Defense Measures packet.

[*Note: Development of appropriate forms and IT policy manuals will continue in conjunction with the Use of Active Defense Measures policy progress. Form numbers as listed below are for future reference only and used here as place holders.*]

Responsibilities

A. Officers

1. Complete a Use of Active Defense Measures Statement on a Department Statement (form [IT].6.3). Include the following information in the statement:
    a. Begin with the following preface: "This is a true and involuntary statement given by me in compliance with Section [IT].5 of the Seattle Information Technology Security Practices Manual."
    NOTE: No other language will be acceptable.
    b. Give a detailed description of the actions of the hostile computer warranting the use of active defense measures,
    c. A detailed description of the active defense measures used,
    d. A description of any apparent damage, any complaint of damage, or the absence of damage, to the hostile computer, and
    e. Document the in-person supervisory screening.
2. Complete a Technological Threat Report (form [IT].6.2) if the hostile computer combatively resists or is aggressive toward the protected system and the officer is reasonably certain the hostile computer is attempting to overpower, disable, or damage them.
3. Submit the Use of Active Defense Measures Statement, Incident Report, Technological Threat Report and any forensic evidence to a supervisor.
4. When active defense measures are used by an officer and a Use of Active Defense Measures Statement is required, an in-person screening of the incident by a supervisor must occur prior to the release of the technological containment of the hostile computer and must be documented in the Technological Incident Report (form [IT].6.1).

B. Supervisors

1. Review and approve all documentation submitted by the officer(s) prior to them going off-duty.
2. Gather any available forensic evidence of each hostile computer involved in a Use of Active Defense Measures reporting.
3. Gather the forensic evidence of each hostile computer only by voluntary, non-coercive means if at all possible.
4. Label the Use of Active Defense Measures forensics evidence with the Single Incident Number, hostile computer's identification, ownership and location, date and initials of the person who gathered the evidence.
5. Do not copy or retain any of the evidence. Place all evidence in the confidential Use of Active Defense Measures packet.
6. Document any apparent damage, complaint of damage, or absence of damage sustained by any protected system, however minor. Complete the Investigating Supervisor's Report of Information Infrastructure Damage (form [IT].6.4) if a protected system is damaged. (See Section [IT].5, III. - Use of Active Defense Measures.)
7. Complete the Use of Active Defense Measures Routing Transmittal Slip (form [IT].6.5) for every use of an active defense measures incident.
8. The "Supervisor's Summary of Incident" section of the form shall include the following:
    a. A brief description of the incident and active defense actions,
    b. A list of all known witnesses to the incident,
    c. A detailed description of all incident related damages sustained by the protected system or hostile computer,
    d. A detailed description of the use of active defense measures employed by the officer and any resistance by the hostile computer, and
    e. If gathering forensic evidence is not possible, a statement indicating that no forensic evidence was gathered and the reason why.
9. Prepare a Use of Active Defense Measures packet. Include the following:
    a. The original Use of Active Defense Measures Statement,
    b. The Use of Active Defense Measures Routing Transmittal slip,
    c. Forensic evidence, and
    d. Copies of all related reports.
10. Forward the completed packet through the involved officer's chain of command.
11. For those incidents where serious damage has occurred, or are of a sensitive nature, immediately forward a copy of the Use of Active Defense Measures Statement, together with copies of all related reports, to the CTO (Chief Technology Officer), using an Alert tag.

12. The Use of Active Defense Measures packet shall then be forwarded to the CISO (Chief Information Security Officer), and the Active Defense Oversight committee.
13. A copy of the Use of Active Defense Measures packet may be forwarded to the affected law enforcement jurisdictions by the CTO and the CISO.

C. Review of Incident

1. The CISO and Active Defense Oversight committee will review the incident.
2. They will create a report with their findings on the efficacy of the incident and their analysis of the justifications for the active defense measures that were employed.
3. The report will contain a section outlining ideas for better strategies, policy changes or training needs elicited from the review of the incident.

A copy of the final report may be forwarded to the affected law enforcement jurisdictions by the CTO and the CISO.

Referenced Forms

NOTE: The following forms are the primary forms we expect to use in reporting Active Defense Incidents. They were developed using Seattle Police incident reporting forms as examples. As noted above the development of all of the forms we referenced is work that will take place as we test our procedures.

We expect that as the reporting and review process is better refined, the need for different types of documentation will result in the creation of more applicable forms.

NOTE: The current United States Secret Service form SSF 4017 (Network Incident Report) may be a more applicable format than the police forms reviewed. The final form listed below is taken from that example.

City of Seattle Information Technology

ACTIVE DEFENSE INCIDENT REPORT

☐ INCIDENT
☐ INCIDENT AND SUPPRESSION
☐ SUPPRESION ONLY

INCIDENT NUMBER 03-

FORM # [IT].6.1

☐ DO NOT DISCLOSE
☐ NOT DISCUSSED
☐ DISCLOSE

THE PERSON MAKING THIS REPORT HEREBY DECLARES THE FACTS HEREIN ARE TRUE AND CORRECT, AND UNDERSTANDS THAT BY FILING A FALSE REPORT, THEY MAY BE SUBJECT TO CRIMINAL PROSECUTION. X

☐ HAZARD TO PROTECTED SYSTEM
☐ HOSTILE SCAN
☐ CRIMINAL ATTACK

INCIDENT CLASSIFICATION	TOOL USED	METHOD OF TOOL USE

LOCATION	FIRM NAME	CENSUS	BEAT

TYPE OF SYSTEM	PORT(S) OF ENTRY

DATE/TIME REPORTED	DAY OF WEEK	DATE(S) / TIME(S) OCCURRED	DAY(S) OF WEEK

☐ DATA STOLEN / RECOVERED (PROPERTY FORM [IT].6.6 MUST BE ATTACHED) ☐ NOTHING TAKEN ☐ UNKNOWN AT TIME OF REPORT ☐ VICTIM FOLLOW-UP LEFT

☐ EVIDENCE SUBMITTED ☐ IP ADDRESS SEARCH MADE ☐ IP ADDRESS FOUND ☐ FORENSICS ANALYSIS REQUESTED

DAMAGED - 1
HAS USABLE TESTIMONY - 2
DO NOT DISCLOSE - 3

CODE C (PERSON REPORTING) V (VICTIM SYSTEM) W (WITNESS)

PERSON/PROTECTED SYSTEM INVOLVED

CODE	NAME (LAST, FIRST, MIDDLE OR COMPUTER NAME)	SYSTEM TYPE	HOME PHONE	HOURS	1 ☐ 2 ☐ 3 ☐
ADDRESS (OR IP ADDRESS) ZIP CODE		OCCUPATION(OR USE)	WORK PHONE	HOURS	
CODE	NAME (LAST, FIRST, MIDDLE)	SYSTEM TYPE	HOME PHONE	HOURS	1 ☐ 2 ☐ 3 ☐
ADDRESS (OR IP ADDRESS) ZIP CODE		OCCUPATION(OR USE)	WORK PHONE	HOURS	

Suspect #1

COMPUTER NAME	SYSTEM TYPE	O.S.	VERSION	SUB VERSION	MAKE	MODEL	CPU

IP ADDRESS	DOMAIN	LOCATION	WORK HOURS	USE	OWNER

IP ADDRESS, DNS NAME, DOMAIN,	DOMAIN OWNER

BA/CIT. NO.	CHARGE DETAILS (INCLUDE ORDINANCE OR R.C.W. NUMBER AND CHARGE NARRATIVES)	☐ BOOKED ☐ CITED ☐ Y S C ☐ K C J

1. ADDITIONAL PERSONS OR COMPUTERS - CODE, NAME, TYPE, USE, DATES., IP ADDRESS, DAMAGE, REPAIR, DOMAIN ADDRESS & OWNER, HOURS, AND IF DISCLOSURE OF NAME IS PERMITTED.
2. ADDITIONAL SUSPECTS - DETAIL INFORMATION IN SAME ORDER AS SUSPECT BLOCK.
3. VICTIM'S DAMAGE - DETAILS AND WHEN ANALYSIS OCCURRED.
4. PROPERTY DAMAGED - DESCRIBE AND INDICATE AMOUNT OF LOSS.
5. PHYSICAL\ELECTRONIC EVIDENCE - DETAIL WHAT AND WHERE FOUND, BY WHOM, AND DISPOSITION.
6. TOOLS OR COMPUTER USED BY SUSPECT AND DISPOSITION.
7. LIST STATEMENTS TAKEN AND DISPOSITION.
8. RECONSTRUCT INCIDENT AND DESCRIBE INVESTIGATION.
10. OUTLINE TESTIMONY OF PERSONS MARKED "HAS USABLE TESTIMONY" ON FRONT.

ITEM #

I HEREBY CERTIFY (DECLARE) UNDER PENALTY OF PERJURY UNDER THE LAWS OF THE STATE OF WASHINGTON THAT THIS REPORT IS TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF ()

PRIMARY OFFICER'S SIGNATURE | SERIAL # | UNIT # | DATE SIGNED | PLACE SIGNED: SEATTLE, WA

PRIMARY OFFICER'S PRINTED NAME	SECONDARY OFFICER	SERIAL UNIT	APPROVING OFFICER SERIAL

Incident Number 03-

Form [IT].6.1 Rev. 2/03

City of Seattle
Information
Technology

ACTIVE DEFENSE STATEMENT

UNIT NUMBER	INCIDENT NUMBER
0	03-

FORM # [IT].6.3

DATE	TIME	PLACE	PROTECTED SYSTEM

STATEMENT OF: ☐ SECURITY OFFICER ☐ WITNESS ☐ VICTIM SYSTEM ADMIN ☐ OTHER

NAME (LAST, FIRST, MIDDLE AND/OR COMPUTER NAME)	SYSTEM TYPE	DOB OR DATE IN SERVICE	DATE/TIME OF EVENT

X _____ **WITNESS** _____ **WITNESS** _____

STATEMENT TAKEN BY

City of Seattle
Information
Technology

ACTIVE DEFENSE INCIDENT REPORT

UNIT NUMBER	INCIDENT NUMBER
0	03-
	FORM # [IT].6.3

Subject:
☐ Site under attack ☐ Active Response ☐ Investigation in progress ☐ Closed

What action do you require:
☐ Immediate response from CISO
☐ Review of active response by Security Risk Committee
☐ Follow-up forensics on captured data
☐ None at this time
☐ Other (please give details):

Site Involved (name and location):

Point of Contact for Incident:
Name/Title:
Organization:
Email: 7 x 24 contact information

Alternate Point of Contact for Incident:
Name/Title:
Organization:
Email: 7 x 24 contact information

Type of Incident:
☐ Malicious code: virus, Trojan horse, worm
☐ Probes/Scans (non-malicious data gathering – recurring, massive, unusual
☐ Attack (successful/unsuccessful intrusions including scanning with attack packets
☐ Denial of service event
☐ High embarrassment factor

Type of Response:
☐ Cease and desist messages (sent directly to source of attack via phone or data connection)
☐ Scans and probes of intruding systems (traceback, ftp or HTTP scans, other identification or forensics probes)
☐ Non terminal counter attack (blocking applications or filters)
☐ Near terminal counter attack (powerful suppression application or denial of service

☐ Functional termination of intruding systems
Date and Time of incident (specify time zone):
Summary of Incident:
Type of service, information or project compromised or threatened (be specific): ☐ Sensitive unclassified such as privacy, proprietary, or source selection ☐ Critical infrastructure command and control ☐ Other
Damage Done: Number of local systems affected: Estimated number of remote or attacking systems affected: Nature of local loss or damage: Nature of remote or attacking loss or damage: System downtime: Cost of incident: ☐ Unknown ☐ None ☐ <$10K ☐ $10K - $50K ☐ >$50K
Other entities contacted (list name and contact information): Department IT Support Staff: Department Management: Chief Technology Officer: Chief Information Security Officer: Law Enforcement: Other:

Tools and Deployment

The next step in the process of preparation for active defense was to develop a toolset. There are a wealth of free resources on the Internet and with the current budgets that was the price level we were looking for.

We spent some months developing a list of tools and organizing that list into the different types and uses of those tools. A group of computer science students from one of the local universities helped us by putting together the following document. I have copied (with their permission) the first part of their extensive survey of tools because I think it is a perfect example of the type of toolset you should consider putting together for active defense.

Survey of Potential Tools under Linux/BSD

Primary Author: Mike Clement
Secondary Authors: Brandon Uttech
Nathan Harkenrider

Version 1.0 – September 9, 2003

License and Contact Information

Contact Information:

Author	Email	Home Phone
Mike Clement	clemenm@seattleu.edu	(206) 568-3956
Brandon Uttech	uttechb@seattleu.edu	(206) 447-8216
Nathan Harkenrider	harkenn@seattleu.edu	(206) 447-8216

Overview

This document is intended to give the reader an overview of potential Active Defense tools listed within. It documents the platforms, features, potential uses, and possible extensions of each tool. The reviewer's comments and recommendations on each tool are also included. It does NOT attempt to be an exhaustive search of all potential tools, nor is it a detailed study of the functionality and usefulness of any specific tool.

All testing was done under FreeBSD 4.8-RELEASE, a Unix-variant Open-Source Operating System. Tools were selected from the FreeBSD ports collection, browsable at:
http://www.freebsd.org/ports/
We attempted to select only Open-Source, free-of-cost tools for this survey. These tools were developed either by a single author or a group of developers; however, we only list one primary author, or a single group, per tool. Tests of tools were run against Windows 2000 Professional, Windows 2000 Server, FreeBSD, OpenBSD, and Debian Linux systems among others.

Notes on the Tools table:
Tool Severity refers to the level of harm or visibility each tool can inflict on remote hosts. The levels range from not creating any network traffic (such as sniffers) to disrupting existing connections or bogging down the network (connection killers, packet flooders), to actually maiming or crashing remote hosts. An "X" means it is fairly certain that the tool in question can create that level of an attack. A "?" means the tool might be able to perform at that level, either through clever usage or extension of the program, or in the case of Intrusion tools, it may be useful in preparing for a remote host intrusion.
"Wireless" tool packages are specifically designed for 802.11b or WLan networks.
"Our Pick" indicates that we thought the tool was particularly interesting or useful.
The size listed for each tool is the package size for the tool itself; this generally includes any plugins or add-ons installed with the package, but does not account for any underlying dependencies (e.g. XWindows, PERL, libpcap, etc).

During this survey, other surveys of security tools were found. Following is a list of websites where further tool listings can be found:

http://www.isecom.org/projects/operationaltools.htm
http://www.nmap.org/tools.html
http://luge.cc.emory.edu/psl.html
http://www.antihackertoolkit.com/tools.html

					Tool Severity						Platforms							
Name		Version		Size (kB)	Passive	Probe	Disrupt	Intrude	Destroy		Lnx/BSD	Win32	OS X	Other		Has GUI	Wireless	Our Pick
angst		0.4b		30	X	X					X							
arirang		1.6,1		317		X		?			X			X				
authforce		0.9.6		30				X			X							
boclient		1.21		31				X			X							
bsd-airtools		0.2		165	X			X			X						X	X
ctrace		0.8		20	X	X					X							
despoof		0.9		24	X	X					X							
dlint		1.4.0		34	X	X					X							
domtools		1.5.0		254	X	X					X			X				
dsniff		2.3		328		X	X	X			X	X	X	X				X
echoping		5.0.1		30		X	?				X							
ethereal		0.9.10		11,300	X						X					X		X
ettercap		0.6.7		962	X	X	X				X	X	X					X
firewalk		1.0		29		X					X							
flood		0.20030108		139			X				X							
fragrouter		1.6		32		?		?			X							X
hackbot		2.20		84		X		X			X			X				
hammerhead		2.1.3		2,313			X				X			X				
hping		2.0.0r2_2,1		81		X	?				X			X				
john		1.6.32		896				X			X	X						
jwhois		3.2.1		144	X						X							
l0phtcrack		1.5		267				X			X							
LaBrea		2.3		52	X						X	X	X					X
lcrzoex		4.17.0		1,697		X	X	?			X	X						X
lft		2.0		65		X					X	X	X	X				
mdcrack		1.2		173				X			X							
nat		2.0		218		X		?			X	X						X
nbtscan		1.0.2		26		X		?			X	X						
nemesis		1.32		151		X					X	X	X	X				X
nessus		1.2.7		~7,000	?	X	?	?	?		X	X						X
netsed		0.01_1		19		X	?	?			X							
nmap		3.00		~1,000		X					X	X	X	X		X		X
p0f		1.8.2_1		59	X						X	X		X				
queso		980922		31		X					X			X				
rain		1.2.9.b1		55		X	X				X							X
scanssh		1.60b_1		25		X					X							
sendip		2.3		298		X					X							
siege		2.56		74			X				X							
siphon		0.666beta		12	X						X		X					
slurpie		2.0b		20				X			X							
sniff		1.0		34	X						X							X
ssldump		0.9b3		65	X	?					X			X				
tcpshow		1.74		29	X						X							
thcrut		0.1		166		X		?			X			X			X	
whisker		1.4_1		143		X					X							
xprobe		0.0.1p1		23	X						X							
zombiezapper		1.2		33			X				X							

Deployment Plans

The final step is the actual deployment of the toolset and active defense options. The first part of that process is the merging of the policy and procedures with the toolset. Then you need to begin testing and training of information security "officers" (as defined in the policy document) in the use of the tools. Finally, you need to take the information from the test exercises and refine your policies and develop a concise "order of battle." I'll take a brief look at each of these steps.

Merging Policy and Toolsets

In the interest of time I won't show you here the entire documentation that we have developed to merge our tools with the policy. Instead I will just give you a couple of quick examples. You will want to develop your own toolsets and plug them in as appropriate to your needs.

For the scanning of an attacking computer there are several possible tools listed. Depending on the type of information you want to gather and the location of the attacking computer system you might use Ethereal, a packet capture utility that takes information from TCPDump and makes it easier to use. You might also want to use a whois program such as JwhoIs to do a trace back on the IP address of the attacker.

If you wanted to do more intensive probes, you might use Hping, a tool that will do trace routes, pings, OS fingerprinting, and more. It also allows you to spoof addresses and could be used to flood the attacking computer system.

As you can see, there are multitudes of tools out there that can be used. One possibility that we have been considering is combining tools into sets that are automated at some level. This would give us a way to respond more quickly to an attack and possibly make program level adjustments up the continuum of response. This is a big part of the process that you should consider carefully and test frequently.

Testing, Exercises and Refining

We are setting up a lab with DSL lines to the outside (of course completely segregated from any City networks). We will have laptops with the toolsets and possibly some routers, switches, etc. to emulate a small network. We'll set up both hardware and software firewalls and configure them as both host and network IDS (Intrusion Detection Systems) for the sake of collecting good logs. The configuration of those firewall/IDS systems will need to be open enough to allow us to test and log information but also protect us from real attacks. Most likely the configuration will be dynamic, changing depending on the procedures or exercises we are conducting. We have contacted a couple of other groups who have war wagons or incident response labs set up and running. They have agreed to play with us as we start exercising our scenarios.

The first thing we intend to do is to verify our connections with each other with some simple pinging and identification tools. We'll see if we can find each other and then move up from there to running some scans to see what kind of information we can gather. We'll use those tests not only to learn how well our tools work, but also to gather signatures of the effects of the tools. We'll be checking our IDS logs to use that information to document the signatures so we can recognize and respond to them effectively. By comparing notes with the other players we can learn how quickly and effectively our tools work. We can also better decide which tools are stealth tools or how an attacker might respond to the effects of tools that actually impact their systems.

We will take all the information gleaned from these first tests and use them to refine our protocols and attack plans. Once we have things as clearly defined as possible, we're ready for the real fun!

At that point we will be asking an outside group to create a "capture the flag" exercise similar to those held at DefCon. With that in place we will exercise our plans together with one or two other labs. Again, once we have completed those exercises we will exchange information with each other and use the information to refine our plans and protocols.

As with any security policy and procedure, it is important to keep exercising and refining based both on new knowledge and changing technology. We will do so and I recommend that you plan on doing so as well.

Conclusion

If you or your organizations are connected to the Internet, you will be attacked. It might be as simple and benign as scanning, or it could be anything up to and including the complete destruction of your systems. If you are in charge of protecting those systems it is important to consider what you have to protect, how important each piece is to your organization, and how far you are willing and able to go to protect it.

That is just basic information security practice but it leads inevitably to the position of this paper. To protect your assets you must have all the tools in place and have practiced using them. I believe that active defense is a valid and important part of that toolset. I advocate the continued examination of these options as well as the exchange of our experiences throughout the information security industry. I am currently looking into starting a forum specifically on this subject and I hope that anyone who has made it to the end of this tome will contact me so we can all keep this conversation going.

References

Singh, Simon. The Code Book. New York: Anchor Books, 1999.

Sharp, Walter Gary. CyberSpace and the Use of Force. Falls Church: Aegis Research Corporation, 1999.

"18 U.S.C. 2511 Interception and Disclosure of Wire, Oral, or Electonic Communications Prohibited." 24 APR 2000. Department of Justice. 04 Jan 2004. <http://www.cybercrime.gov/usc2511.htm>.

Preston, Ethan and Lofton, John. "Computer Security Publications: Information Economics, Shifting Liability and the First Amendment." 2002. MC&L. 05 Jan 2004. <http://www.mcandl.com/computer-security.html>.

"Electronic Communications Privacy Act." 2003. America Online Legal Department. 05 Jan 2004. <http://legal.web.aol.com/resources/legislation/ecpa.html>.

Preston, Ethan. "Finding Fences in Cyberspace: Privacy and Open Access on the Internet." 2000. University of Florida Levin College of Law. 09 Jan 2004. <http://grove.ufl.edu/~techlaw/vol6/Preston.html>.

Jennings, Andrew. "Law Statutes Relating to Self Defense in Washington." 2002. Andy\'s Tae Kwon Do. 09 Jan 2004. <http://jenningscc.com/TaeKwonDo/Laws%20-%20WA.htm>.

Lemos, Robert. "Is vigilante hacking legal?." 27 Feb 2003. ZD Net – CNET News.com. 09 Jan 2004. <http://zdnet.com.com/2100-1105-990469.html>.

Moulton, Scott. "Nmap Hackers: RE: nmap illegal to use?." Online posting. 11 Jun 2001. Nmap Hackers. 11 Jan 2004.http://seclists.org/lists/nmap-hackers/2001/Apr-Jun/0011.html>.

Fyodor. "Nmap Hackers: Re: nmap illegal to use?." Online posting. 10 Jun 2001. Nmap Hackers. 11 Jan 2004. <http://seclists.org/lists/nmap-hackers/2001/Apr-Jun/0008.html>.

Bhatt, Abhinav. "Port Scanning and its Legal Implications." 2004. Asian School of Cyberlaw. 11 Jan 2004. <http://www.asianlaws.org/cyberlaw/library/cc/ptscanning.htm>.

Samson, Martin. "Scott Moulton and Network Installation Computer Services, Inc. v. VC3." 2004. Phillips Nizer LLP. 11 Jan 2004. <http://www.phillipsnizer.com/library/cases/lib_case37.cfm>.

Poulsen, Kevin. "Port scans legal, judge says." Security Focus News 18 Dec 2000. 11 Jan 2004 http://www.securityfocus.com/news/126

Lee, Chris. "Argentina backs hacking as 'legal'." vnunet news 16 Apr 2002. 12 Jan 2004 http://www.vnunet.com/News/1130937

"WACIRC Law Enforcement Guidelines for Reporting and Responding to Computer Crimes." Washington State Department of Informaton Services. 12 Jan 2004. <http://www.dis.wa.gov/portfolio/PDFs/WACIRCGuidelines.pdf>.

"The Computer Fraud and Abuse Act (as amended 1994 and 1996)." 09 Jan 2004. <http://www.panix.com/~eck/computer-fraud-act.html>.

Christiansen, John R.. "Actively Defending Against Security Breaches: Is it Legal to "Hack Back?" Is it Ethical? Is it Smart?." CyberCrime III, King County Bar Association. Woman\'s University Club, Seattle, WA. 21 Nov 2003.

"Secret Service Form 4017: Cyber Threat/Network Incident Report ." United States Secret Service. 09 Jan 2004. <http://www.usss.treas.gov/net_intrusion_forms.shtml>.

Mitchell, Steven D., and Elizabeth A. Banker. "Private Intrusion Response." Harvard Journal of Law & Technology Summer 1998: 700 - 732.

"Toward Deterrence in the Cyber Dimension." Report to the President's Commission on Critical Infrastructure Protection 1997.

Jayawal, Vikas, William Yurcik, and David Doss. "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism." Proceedings of the IEEE International Symposium on Technology and Society (ISTAS) June 2002: .

Kerr, Oren. "Cybercrime\'s scope: Interpreting 'access' and 'authorization' in computer misuse statutes." New York University Law Review November 2003: .

Dittrich, Dave. "A Framework for Active Defense." Agora. City of Seattle's Dome Room, Seattle. 12 Sep 2003.

Dittrich, Dave and Christiansen, John R.. "Panel: "Active Defense"." SecureWorld Expo. , Bellevue, WA. 25 Sep 2003.

Clement, Mike, Brandon Uttech, and Nathan Harkenrider. "Survey of Potential Tools under Linux/BSD." Sept 2003: .

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 New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event