GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Profiling Hackers

GIAC GSEC Gold Certification

Author: Larisa April Long, lapril@dc.rr.com
Advisor: Egan Hadsell

Accepted: January 26, 2012

Abstract:

White Hats. Black Hats. Hacktivists. Hackers run the gamut of human nature: good, bad, indifferent or scary. Hackers manipulate programs to push the limits of technology, and, whatever their purpose, they raise awareness to find and fix security flaws. While hackers have become the topic of conversation and news attention, the majority of people misunderstand them because a detailed hacker profile isn't offered.

© 2012 SANS Institute, Author retains full rights.

© 2012 The SANS Institute Author retains full rights.

1. What is a Hacker?

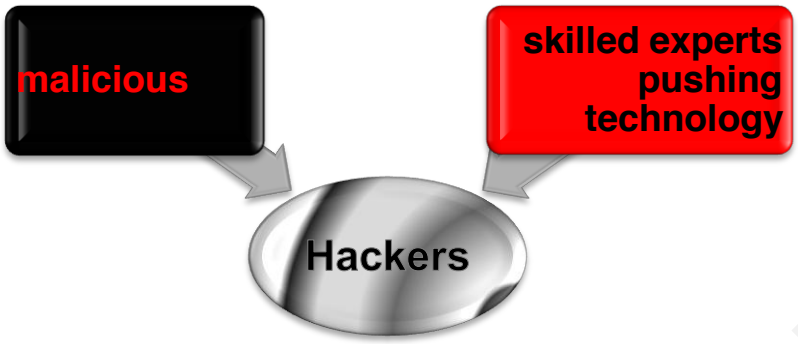
Hacking without permission and authorization is considered illegal. But let's face it, that's why the subject of hacking is so appealing. But for much of the population, hacking is an elusive subject. What is a hacker? Who hacks? How do they hack? Why do they hack? Can hackers force us into war? Can they bring down a government? Are they good or bad or a little of both?

Movies and TV are filled with examples of the uber hacker able to accomplish almost superhuman exploits while remaining covertly under the radar. Many hackers are considered chic geek because they can do what many cannot comprehend. The stereotypical hacker is considered either a basement dweller rarely ever seeing sunlight or someone against the grain who may look, act or talk differently than the norm. Entire books are written about hacking methods and methodology. There are as many different techniques as there are hackers, and each hacker has their own methods they prefer. Some use conventional tools while others merge different languages into a unique tool.

Before a hacker attempts access, information has to be gathered about what they are attempting to hack. That information is easily accessible via the Internet. If a hacker seeks to hack a company, vast amounts of information are available via the company's own website and blogs. Job listings will detail the types of computers, Operating Systems, and software that a company uses. Enumerating, or finding open ports, locating rogue wireless access points, fingerprinting an Operating System and scanning a network are accomplished with a variety of both active, also known as noisy, and passive, also known as quiet, tools. Firewalls can be bypassed, Intrusion Detection systems evaded and passwords cracked in order to gain access, escalate privileges, and exploit vulnerabilities. If the purpose is to be discrete, logs can be disabled and evidence eliminated.

Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.



In thinking about hackers, two divergent camps emerge: malicious or a skilled expert pushing technology. Some believe the term hacker is a derogatory one used only to describe malicious intent to steal credit card numbers or deface websites. Basically, hacker equals bad. The costs of hacker activity cannot be quantifiably measured in the losses to personal information, confidentiality, data, and increased security costs. In fact, monetary losses to cybercrime cannot even be agreed upon. They have either "doubled" from 2009 to 2010 (Homeland Security Newswire, 2010), "aren't reliable" (Zick, 2011), are up by "56%" (Biztech Africa, 2011), or are "erroneously overestimated" (CircleID, 2011).

Another problem is the hackers of yesterday had to rely on knowledge and skill to implement their attacks. "Twelve years ago, they actually were real hackers. You had to work and build your arsenal of tools" (Gross, 2011). Today, people with little to no experience can launch sophisticated attacks from websites with open source toolboxes. Script Kiddies fit into this category, and "is a derogatory term for black hat hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves" (Siciliano, 2011). This has greatly enhanced the negative image of hackers.

Given the number of high profile data theft, server compromises, and stolen passwords, it is easy to see how the public forms the negative opinion concerning malicious intent. There are many, though, who view hackers as highly skilled computer experts. They manipulate systems and expose vulnerabilities to point out the flaws before others can exploit them. Their actions inspire computer programmers to more securely code their software to protect against vulnerabilities. "A hacker is anybody looking to manipulate technology to do something other than its original purpose. That's not necessarily a bad thing" (Gross, 2011). The forerunners of

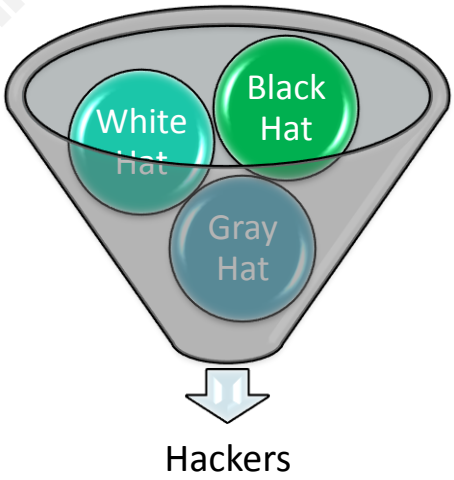
© 2012 The SANS Institute Author retains full rights.

Apple Computer and IBM, Steve Jobs and Bill Gates are considered hackers who manipulated technology to the point that their ideas and inventions became mainstream.

According to the hacking conference, DEF CON, they "hope, in a strange way, that by teaching people about hacking they will make the tech world safer. DEF CON is their playground of sorts. Many of the hacks aren't necessarily malicious. They are people toying around just to see what's possible. If they don't do it, then the really bad guys will, they say" (Sutter, 2011). Closing in on its twentieth year, DEFCON "has sprawled into a 15,000-person, four-day convention" (Sutter, 2011) for hackers to hone their skill and learn new techniques.

Many new hackers do not have to learn the skills necessary given the number of open source tools available, but serious hackers learn by doing. They learn computer languages, TCP/IP, Operating Systems, command line tools, firewalls, routers, social engineering, and basically investigate anything and everything computer related to figure out how it all works. And the only way to figure out how something works is to take it all apart. Universities teach hacking and incident handling skills, and countless books and videos exist. Hackers can make a legitimate living as security consultants, ethical hackers and pen testers.

1.1 How do you define a Hacker? Black, White or Gray?

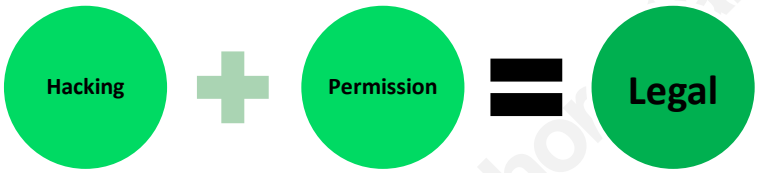


Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.

While the media likes to lump all hackers together, there are many different types. Some differentiate between the good, or White Hats, as computer security professionals who seek to protect computer systems by discovering the vulnerabilities before 'the bad guys,' or Black Hats.

The main difference between White Hats and Black Hats is permission. White Hats and Black Hats use the same skill set and techniques, but White Hats have permission to access the computer systems; Black Hats do not. As every computer course will describe, the main word in all definitions concerning hacking is 'authorization.' The law is clear and concise concerning authorization. If a hacker has authorization, they are within the law. No authorization is illegal and hints at malicious intent.



The Computer Fraud and Abuse Act (18 U.S.C. § 1030), defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" (FindLaw, 2011). The act defines illegal activities against protected computers by anyone who "intentionally accesses a computer without authorization or exceeds authorized access" (FindLaw, 2011) and defines protected computers as those used by the US federal government, by a financial institution, or for interstate or foreign commerce whether in the US or outside the US. "The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force" (Gorman & Barnes, 2011).

The strict legalities involved with hacking are the very reasons why professional pen testers and ethical hackers must be adamant in acquiring not only the requisite permissions but the necessary signatures from all parties involved before any action is taken. They must also outline the scope of the investigation, what methods they will be using, what they are allowed to do and, most importantly, understand what areas are considered 'off limits' to them from any

© 2012 The SANS Institute Author retains full rights.

company, group or individual who hires their services. Like doctors, most computer professionals are encouraged to 'do no harm.'

While the law is clear concerning hacking, the definition gets a bit fuzzy among the general population and even computer professionals. Added into this mix are the Gray Hats, or Ethical Hackers, who blur the line between White and Black. "The goal of ethical hackers is to help organizations take preemptive measures against malicious attacks by attacking systems themselves, all the while staying within legal limits. The philosophy stems from the proven practice of trying to catch a thief by thinking like a thief" (Graves, 2007).

1.2 Hacker Definition: Authorization, Intention or Victim?

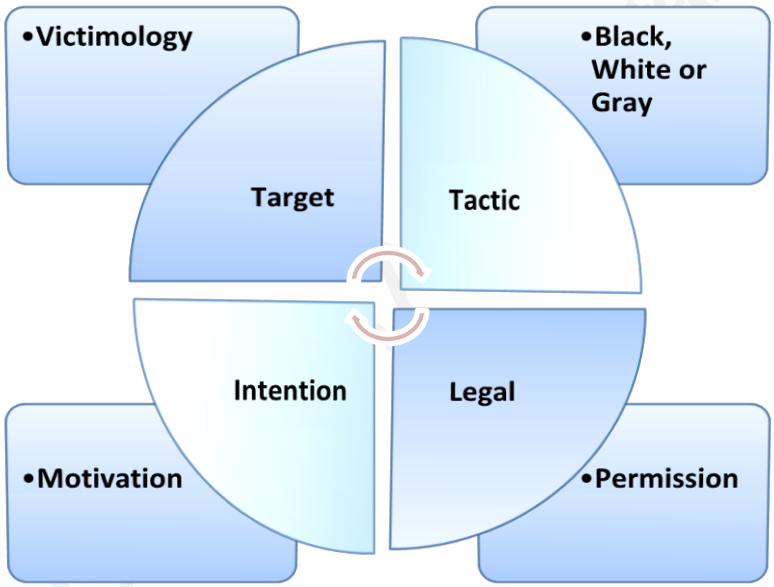
The three main areas included in a hacking definition is authorization, intention and victimology. Those who prefer the legal definition, are concerned with tactics alone. They are not conflicted in their hacking description: hacking without permission or authorization is wrong. But if this were the only way to define hackers, would all activities be considered equal? Would this place those who hack credit card accounts together with those fighting the Mexican drug cartel? On the other hand, without black and white rules, cyber space would be like the Wild West.

Those who prefer to understand the intention behind the hack might view hacking with malicious intent as wrong, Black Hat, and place those whose hacking activities do not hurt under the White or Gray Hat banner. The idea of intent is such a strong one that murder has many different degrees based solely on the intent of the perpetrator. If a prosecutor can prove someone intentionally sought to kill someone, the law states a charge of murder in the first degree can be sought. If however, intention is not known, cannot be proved or is not a mitigating factor, a lesser charge can be sought. Is the intention to exploit the vulnerability in order to publicize the risks so that it may be fixed? Or is the idea to profit from the vulnerability by informing other hackers, promoting illegal activities or securing bragging rights?

If the target defines hacking, then victimology comes into play. This is subjective because where is the line drawn? Is it illegal to hack a credit union but heroic to attack an online

© 2012 The SANS Institute Author retains full rights.

pedophile ring who engages in human trafficking? The definition of Hacktivists is subjective because they technically do not have access or permission but believe they are different due to their motivation. "Hactivism is the fusion of hacking and activism; politics and technology. More specifically, hacktivism is described as hacking for a political cause" (metac0m, 2003). Ideology is the reason they do what they do. Though Black Hats might commit their actions for profit, malicious reasons or recognition, Hacktivists believe their ideology, whether it is religious, political, revenge seeking, or to shed light on injustice, sets them apart and is the driving force for their actions.



To make things even more interesting, many within the hacking community have rejected the traditional white hat versus black hat and have retained custody of the black hat term further blurring the lines of what is good and bad. While the media tends to either hero worship or demonize, many find it safer to side with the legal definition, but difficult economic times erode legal definitions as many turn a blind eye towards hackers who attack those they believe to be corrupt.

© 2012 The SANS Institute Author retains full rights.

2. What is a Profile?

TV shows and movies showcase profiling and present it as if a crime can be planned, committed, profiled and solved within about an hour. Unlike fictionalized accounts, profiling is a delicate balance of criminology, psychology and forensics (Turvey, 2011) and requires an "exhaustive research effort" because "most crises have roots going deep into the past, much farther than we usually realize until after they erupt" (Grabo, 2004).

Profiling is understanding how and why someone does what they do. "The best predictor of future behavior is past behavior" (O'Donohue, 2011). A profile is a psychological tool that aids in the understanding of people's motivations and can be used in a variety of occupations. Criminal profiles have tracked serial killers by studying victimology, crime scenes and the methodology of the killer. Competitive intelligence profiles have been employed for businesses to keep apprised of the competition. "Competitive intelligence is a systematic program for gathering and analyzing information about your competitor's activities and general business trends to further your own company's goals" (Kahaner, 1996).

Political profiles have been helpful in studying the psychology of political leaders in order to create a better foreign policy and comprehending the leader's motives and methods. Interpreting what a country is likely to do is necessary whether the country is an ally or an enemy. The profiler must also understand historical precedent and current events. For criminal profilers, they must determine how the past might specifically relate to the case they are working on. Political profilers need knowledge of the history of the country they are specializing in, the psychology of the leader and culture, and the interaction between nations.

In all cases, profiling studies the motivation and methodology to determine if there is a pattern of behavior that might be deduced. For every action there is a reaction and vice versa. Nothing happens in a vacuum. Profiling hackers is similar to profiling other fields. Since technology changes on an almost minute to minute basis, computer professionals must constantly keep up with the latest attack techniques and signatures in order to prepare not only for threats planned and well publicized but also zero day threats. They also must acknowledge the history of hacking in general and famous hacks in particular.

© 2012 The SANS Institute Author retains full rights.

2.1. Profiling Limits: Judgement and Perception

There are limits to profiling. All profilers have to realize that judgment and perception are two areas that can limit intelligence analysis and profiling. Judgment is "what analysts use to fill gaps in their knowledge" (Heuer, 2010). This is similar to a mirror imaging which is "the natural tendency to assume that others think and perceive the world in the same way we do" (Heuer, 2010). If someone sees something happening and thinks, 'well, I wouldn't do that if I were them' they are practicing mirror imaging. This could be as mundane as being surprised that a friend orders sugar free lemonade at lunch to as serious as believing a bold attack is not taking place against an obvious honeypot because neither one is something you would do.

Perception is seeing "what we expect" to see rather than possibly what is there (Heuer, 1999). This happens all the time in glancing at a word and believing it to be the word that we expected to see rather than the actual word. A major problem with judgment is what Heuer describes as the 'availability rule.' "Two cues people use unconsciously in judging the probability of an event are the ease with which they can imagine relevant instances of the event and the number or frequency of such events that they can easily remember" (Heuer, 1999). Being able to remember past experiences of hacking and the ways that a particular company has been hacked is extremely important in providing better computer security, but it can be a hindrance if those are the only ways it is assumed a company can be hacked.

It is easy to fall into these fallacies because humans naturally try to connect the unknown with something known. Richards Heuer likens memory as a spider web of interconnected information with each new idea easily connected to the entire web. This is one of the major ways humans learn new ideas. It is interesting that one of the major techniques of learning new information is also a downfall to profiling because it might prevent profilers from keeping in mind that something is happening that they might not see just because it hadn't happened before.

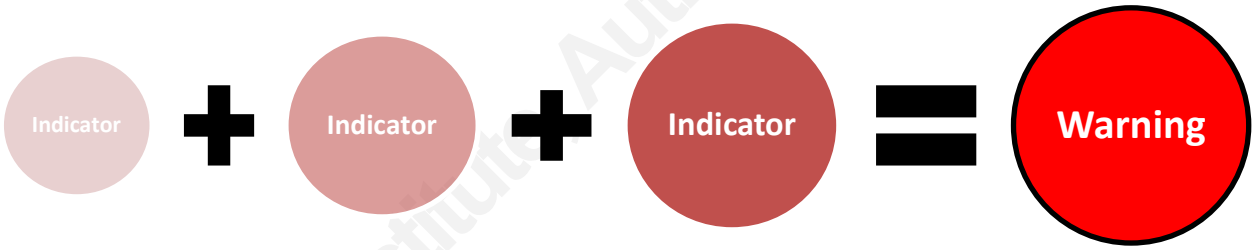
September 11, 2001 was such a shock because a terrorist attack of that magnitude had never been conducted before. Terrorism analysis indicated nonconventional methods would be employed especially after the biochemical Sarin gas attacks in the Tokyo subway system in 1995. Analysts believed terrorists would try to copy that attack and use more unconventional methods such as chemical, biological, nuclear or radiological attacks. Hijacking airlines and

© 2012 The SANS Institute Author retains full rights.

using the airline as a bomb was not considered something that terrorists would attempt given more dangerous and frightening methods of weaponizing chemicals, bacteria and viruses.

3. Indications and Warnings

Indications and Warnings, or I&W, is a traditional military analytic method to study similar past activity in order to see patterns that might predict future events. I&W can be used in conjunction with a profile when various scenarios are deemed plausible. It is intended to prevent surprise and allow for sufficient time to act. An indicator is a "theoretical step which the adversary should or may take in preparation for hostilities" (Grabo, 2004). It may not seem plausible given different circumstances, but there are tasks that must be accomplished in order to complete an event. If a nation is about to invade a neighboring nation, military action would indicate troops would be moved, logistics prepared, propaganda issued, and resources reallocated.



Several indicators could lead to a warning. A warning is "an intangible, an abstraction, a theory, a deduction, a perception, a belief. It is the product of reasoning or of logic, a hypothesis whose validity can be neither confirmed nor refuted until it is too late" (Grabo, 2004).

An indicator alone, however, is not a guarantee of conflict: context is important. If Canada begins to move their troops to the US border, this might be explained via military exercises that had been planned well in advance. If North Korea begins to move their troops towards the South Korea border, this will be more significant given the already tense historical precedence in conflict between the two. While any of the above indicators might not guarantee military action, the likelihood of military action increases with the number of indicators.

One indicator could be coincidence; two indicators raises a red flag and might suggest a warning of impending problems. Increased log activity might be an indicator, but that alone

© 2012 The SANS Institute Author retains full rights.

might not be enough to provide a warning. That, along with indicators of port scans and null sessions, would be enough to require a warning that an attack might be imminent or underway (The Sans Institute, 2011).

3.1 Know Your Enemy

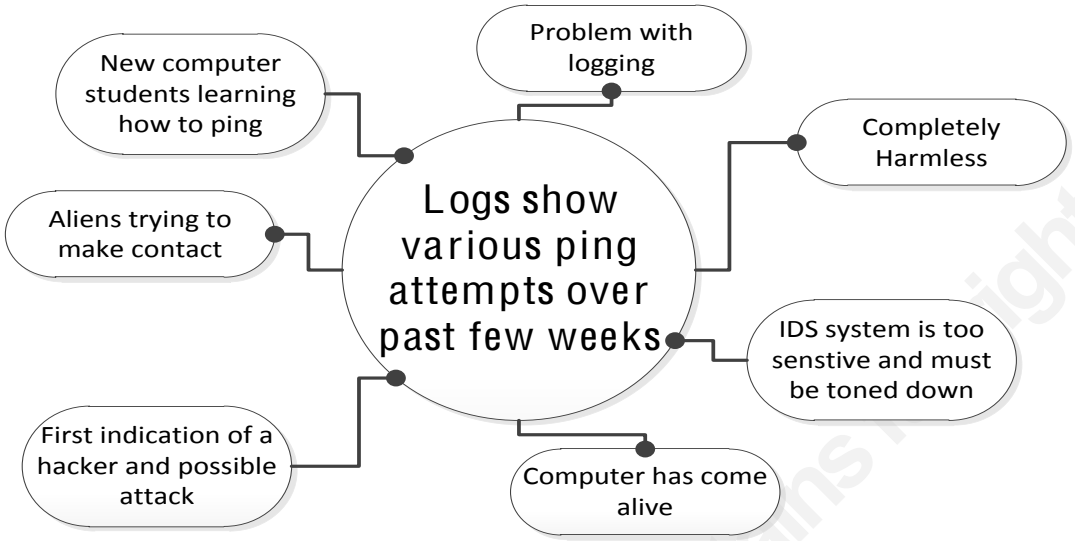
If an unknown group threatens to hack into the US infrastructure, the US would be wise to heed the warning, but it might not be given as much credence since little historical precedence exists from the unknown group. If, however, Chinese government hackers threaten to disrupt the US water supply, more people would take notice given the history and skill of the Chinese government hackers (Bliss, 2011).

If a company is worried about computer security (and whose isn't?) they could create an I&W checklist that might indicate the possibility of an impending attack or the need for heightened security. A very basic I&W might look like this:

Yes or No	Activity
Y or N	A well known hole is found in OS, firewall, or software that isn't patched right away
Y or N	Logs indicate higher than normal level of activity against gateway
Y or N	Port scans
Y or N	Null sessions
Y or N	Social engineering attempts to solicit passwords, email information
Y or N	Stolen laptops with sensitive information
Y or N	Attempted DDOS attack
Y or N	Website attacks: defacement, SQL injection, cross site scripting
Y or N	Virus protection finds suspicious files or software that might indicate backdoors
Y or N	Unsecure wireless access points
Y or N	Other similar companies have been hacked
Y or N	Many employees getting email scams generated from what looks like same person or group

It takes practice to profile, and there are many different books that help with intelligence analysis and profiling. A simple technique in profiling is brainstorming, mind mapping or creating scenarios in that every single idea no matter how preposterous is equal to all others. In these techniques, it is important not to edit initially. Pencil and paper, specialized software or Microsoft Word or Visio can be used.

© 2012 The SANS Institute Author retains full rights.



The important thing is to think of all possible scenarios, and to even throw some out there no matter how preposterous in order to make sure 'no stone is left unturned.' Profiling and I&W seeks to prevent surprise. "If one accepts the premise of surprise, it will follow that what the adversary is preparing to do will not necessarily be that which is most obvious or seemingly plausible" (Grabo, 2004). By attempting to prepare for all contingencies and actions, it is easier to be better prepared and to make a detailed list of actions for each scenario.

4. Hacker I&W

Profiling a hacker or a hacker group is similar to profiling other groups. Dr. Sinai created 31 different indicators for forecasting terrorism (Sinai, 2002), and many can be manipulated to profile hackers. Much can be learned by examining the targets, leadership, history, motivation, strategy, tactics, triggers and hurdles. This will create an I&W list of potential future targets whether from a well known hacker group or a zero day threat. The blueprint for a hacker profile is fully adaptable for computer security professionals regardless of hacker intent.

4.1 Targets

In the Jack the Ripper killings in England in 1888, the police surgeon, Dr. George Phillips, "inferred a criminal's personality by examining the behavior of that particular criminal

© 2012 The SANS Institute Author retains full rights.

with his victim" (Turvey, 2011). This emphasis on the victim to understand the perpetrator can be used in hacking.

By examining and studying a target, more can be learned about the perpetrator. Ask why this person, government, or corporation. It is also just as important to ask why not someone else. If there are two governments, groups, companies or individuals with similar profiles, why is one targeted and not another? "We need to constantly be alert to what is not happening (but ought to be happening) as well as to what is" (Grabo, 2004).

Being able to understand the targets will go a long way in describing and understanding the methodology, motivations and tactics. Understanding the targets will help forecast future similar targets, what kind of security is needed and why the target is being singled out.

4.2 Leadership/Organization/History

The leadership and organization of any group is important. Is the hacker one individual, a group, or a government? If a group, how is the group organized? Is it a hierarchy with a traditional leader or an anarchy of loosely related individuals? If it is a government backed hacking attack, then they might be engaged in information warfare or cyber terrorism. Understanding their motives and their past attacks will help.

What is the history of the group? Trace the origins of the group to create a timeline of events. This is the part of the profile that is based not on supposition but on facts. When did the group begin? Do they have a website? How has their website changed to reflect their activities? Have their attacks increased in sophistication? This would indicate they are either acquiring knowledge with experience or gaining access to more sophisticated attackers.

Have their leaders been interviewed? What they say is important because "most propaganda is 'true'" (Grabo, 2004). Most leaders do exactly what they threaten to do, and, if they are not able to accomplish it, it isn't from lack of trying. If a group publicizes in advance an attack, and they are not able to carry it off does this mean they lacked the skill? The authorities stopped them? The victim's defenses were stronger?

© 2012 The SANS Institute Author retains full rights.

4.3 Motivations

What is their motivation or the "root cause for group's formation"? (Sinai, 2002). What do they claim to be the reason for their actions? Motivations can be derived from interviews, propaganda, any messages left as a result of the hacking, and the names they use both prior to, during and post hacking.

"When you come across intruders or malware make sure you understand the attacker's motivation. Without that, you're being prematurely reactive" (Grimes, 2011). In the end, it doesn't matter much if your server has been compromised or your passwords stolen, but the motivation of the attacker does matter. If the motivation is purely malicious, they might move on. If the motivation is more personal, other tactics should be used to stop them.

4.4 Methods

How do they go about doing what they do? This is the nuts and bolts of the hack. What tools do they use? What are their strategies and tactics? Do they plan well in advance giving plenty of time for research, reconnaissance and social engineering? Why this methodology? Is it their signature? Was this the only way to do the hack given the target? If not, why did they choose this way and not another?

Again, it is important to understand what damage was done and how much damage could have been done. Did the hacker do all the damage they could have or did they restrain their actions? This goes towards intentions versus capabilities: "A time-honored military precept…holds that intelligence should not estimate the intentions of the adversary, but only his capabilities" (Grabo, 2004).

Hackers have a multitude of techniques at their disposal. Just because they didn't use them doesn't mean they couldn't.

4.5 Accelerators & Triggers

An accelerator or trigger is something that happens prior to an attack. It could be a threat, an arrest, a law, a conviction, or a security vulnerability. There is something that happens that makes the time they choose the right time. Are there any accelerators or triggers prior to

© 2012 The SANS Institute Author retains full rights.

their actions? If so, were there similar events that did not lead to a hack? Can a pattern be derived? If similar things happened that did not produce a hack or even a threat of a hack… why?

Is revenge a factor? Many state sponsored hacking events have come after another event such as an arrest, a threat of an arrest, a warning, or a crackdown by police. Some international hackers are classified as Cyber Terrorists who engage in what has been described as Cyber Warfare, information warfare or electronic warfare. Whether they are a group or a nation, their main targets are another nation's infrastructure, economy, or military. China, Russia, and Ukraine have been accused of actively pursuing this field. The FBI defines Cyber Terrorism as the "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents" (Search Security, 2001).

4.6 Hurdles

What were the hurdles that had to be overcome in order to perform the hack? What were the security measures prior to and during the hack from their target? Understanding the hurdles will help understand the sophistication and ability of the hackers. Is it a random attack by a hacking individual hoping to get lucky with a vulnerability? Or is it a sophisticated, coordinated attack by a group with the skills to do a lot of damage?

If they publically state their targets and do not get the result intended, were there hurdles from authorities or extra security measures? Or was the mere mention of an attack the actual attack? Sometimes terror comes not from lighting a fuse but by merely suggesting they know how.

4.7 Future

Given the knowledge of the attacker, will they continue to be a threat in the future? What security can be put into place that will help prevent the attack? Can a more sophisticated I&W be created with indicators that will better alert to a specific style of attack or attacks from this hacker that will help provide better warnings?

© 2012 The SANS Institute Author retains full rights.

5. A Hacker Profile Checklist:

Targets	who? when?	Individual	Company	Government	Group
		Why this target and not someone similar? Was the victim the only target? Who else was targeted?			
Hacker		Individual	Group	Government	
		Do they have a website? What is the history of the group? Can a timeline be created to chart progress of the group?			
Motivations		Why are they doing this? Is it malicious and financially motivated or for hacktivism?			
Methods		Do they have a signature? What tools, techniques did they use? Given their expertise, are there tools, techniques they could have used but didn't? Did they require an extensive amount of research and reconnaissance?			
Triggers		Was there anything that happened prior to their past attacks? Arrests? Legislation? Threats?			
Hurdles		What security did they have to bypass to attack? Were they able to bypass firewalls, IDS, routers, complex passwords? Was the attack successful?			
Future		With knowledge of both target and hacker, will this hacker continue in the future?			

Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.

A sample hacker profile:

Targets	who? when?	Individual	Company Amazon.com Dec 9, 2010	Government	Group
	Why this target and not someone similar? Targeted Was the victim the only target? No Who else was targeted? Paypal, Mastercard, Visa, everyDNS, PostFinance				
Hacker		Individual	Group Anonymous	Government	
	Do they have a website? Yes What is the history of the group? Loose confederation of hacktivists Can a timeline be created to chart progress of the group? Yes				
Motivations	Why are they doing this? Revenge Is it malicious and financially motivated or for hacktivism?				
Methods	Do they have a signature? Warned before attack What tools, techniques did they use? DDOS Given their expertise, are there tools, techniques they could have used but didn't? Yes Did they require an extensive amount of research and reconnaissance? It was strictly a DDOS attack without the need for more complicated hacking techniques				
Triggers	Was there anything that happened prior to their past attacks? Arrests? Legislation? Threats? Amazon removed Wikileaks from their servers				
Hurdles	What security did they have to bypass to attack? It was strictly a DDOS attack without the need for more complicated hacking techniques Were they able to bypass firewalls, IDS, routers, complex passwords? No Was the attack successful? No				
Future	With knowledge of both target and hacker, will this hacker continue in the				

Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.

	future? Yes What can be done to counteract this attack in the future? Stronger servers, powerful firewalls, strong filtering rules, closing open ports, patching systems, etc

6. Conclusion

There is no way to guarantee what the future holds, but computer security professionals need all the tools at their disposal. Like doctors and lawyers, computer professionals face a daily battle of understanding the latest technology, threats and countermeasures. It is a never ending battle from well publicized threats to zero day attacks.

Like the majority of professions, there are good and bad hackers and ones who damage the reputation of the profession. Profiling and I&W can be part of a defense in depth to protect vulnerabilities. Building a hacker profile is similar to other profiles. It is important to study previous hacks, both successful and not, to understand the steps necessary. For a hack to be accomplished, the hacker makes a plan, exploits a vulnerability, launches malware, bypasses a firewall, steals a password, maps a network, maintains access, escalates privilege or pursues a DDOS attack. In other words, they have to find a way in. These necessary steps could be broken down into indicators.

The indicator list can be analyzed to determine if a warning is necessary. "Warning is a skill unto itself, requiring an understanding of the attitudes and disciplines of potential adversaries as well as their capabilities, their history, their culture and their biases" (Grabo, 2004).

"Hacking can be in the positive fashion. There is a white-hat side to hacking and I think we're going to need to breed a lot of white-hat hackers right now to fight the black-hat hackers. Right now, they're winning the war" (Gross, 2011).

© 2012 The SANS Institute Author retains full rights.

7. References

Biztech Africa. (2011, August 2). *Cybercrime Losses Up By 56%.* Retrieved January 3, 2012, from Biztech Africa: http://biztechafrica.com/article/cybercrime-losses-56/977/

Bliss, T. C. (2011, October 27). *Chinese Military Suspected in Hacker Attacks on U.S. Satellites.* Retrieved from Bloomberg Businessweek: http://www.businessweek.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html

CircleID. (2011, July 27). *Cybercrime Losses Overestimated, Say Researchers.* Retrieved January 3, 2012, from CircleID: http://www.circleid.com/posts/cybercrime_losses_overestimated_say_researchers/

FindLaw. (2011). *18 U.S.C. § 1030 : US Code - Section 1030: Fraud and related activity in connection with computers.* Retrieved December 8, 2011, from FindLaw: http://codes.lp.findlaw.com/uscode/18/I/47/1030

Gorman, S., & Barnes, J. (2011, May 31). *Cyber Combat: Act of War.* Retrieved December 13, 2011, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html

Grabo, C. (2004). *Anticipating Surprise: Analysis for Strategic Warning.* Lantham: University Press of America.

Graves, K. (2007). *CEH: Official Certified Ethical Hacker Review Guide.* Indianapolis: Wiley Publishing.

Grimes, R. (2011, February 8). *Your Guide to the Seven Types of Malicious Hackers.* Retrieved December 8, 2011, from InfoWorld: http://www.infoworld.com/d/security-central/your-guide-the-seven-types-malicious-hackers-636?page=0,0

Gross, D. (2011, August 15). *"Mafiaboy' breaks silence, paints 'portrait of a hacker'.* Retrieved from CNN.com: http://www.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html?iref=obnetwork

Heuer, R. (1999). *Psychology of Intelligence Analysis.* CIA Center for the Study of Intelligence.

Heuer, R. (2010). *Structured Analytical Techniques for Intelligence Analysis.* Washington DC: CQ Press College.

Homeland Security Newswire. (2010, March 16). *U.S. Cybercrime Losses Double.* Retrieved January 3, 2012, from homeland security newswire: http://www.homelandsecuritynewswire.com/us-cybercrime-losses-double

Kahaner, L. (1996). *Competitive Intelligence.* New York: Touchstone.

Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.

metac0m. (2003, December). *What is Hacktivism? 2.0.* Retrieved December 8, 2011, from The Hactivist: http://www.thehacktivist.com/whatishacktivism.pdf

O'Donohue, W. (2011). *Difficult Personalities.* Lucky Bat Books.

Search Security. (2001, September). *CyberTerrorism.* Retrieved December 8, 2011 , from Search Security: http://searchsecurity.techtarget.com/definition/cyberterrorism

Siciliano, R. (2011, March 25). *Seven Types of Hacker Motivations.* Retrieved December 8, 2011, from infosec Island: https://www.infosecisland.com/blogview/12659-Seven-Types-of-Hacker-Motivations.html

Sinai, D. J. (2002). Forecasting Terrorism. *IS 348: Forecasting Terrorism* . Virginia, USA: American Military University.

Sutter, J. (2011, August 6). *DEF CON: The event that scares hackers.* Retrieved from CNN.com: http://www.cnn.com/2011/TECH/web/08/05/def.con.hackers/index.html?iref=allsearch&hpt=te_r7

The Sans Institute. (2011). Defense In-Depth. In *Security 401 SANS Security Essentials* (pp. 203-204). The Sans Institute.

Turvey, B. (2011). *Criminal Profiling: An Introduction to Behavorial Evidence Analysis.* Oxford: Elsevier Ltd.

Zick, C. (2011, October 16). *Microsoft Report Challenges Convention Wisdom on Cybercrime Losses.* Retrieved January 3, 2012, from Security, Privacy and the Law: http://www.securityprivacyandthelaw.com/2011/10/articles/cybersecurity-cybercrime/microsoft-report-challenges-conventional-wisdom-on-cybercrime-losses/

Larisa April Long, lapril@dc.rr.com

© 2012 The SANS Institute Author retains full rights.