



Issue 13, January 30, 2009

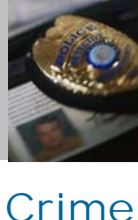
E-Telligence

2009 Calendar of Events

- Feb. 21, 2009
National Symposium on Technology Crime and Electronic Evidence
Toronto, ON, Canada
[Click here](#)
- Feb. 23-27, 2009
International Fraud Conference
Toronto, ON, Canada
[Click here](#)
- March 29-April 1, 2009
Cambridge University Internet Intelligence
Cambridge, UK
[Click here](#)
- April 13-16, 2009
Cyber Physical Systems Week
San Francisco, CA, USA
[Click here](#)
- April 20-24, 2009
18th Annual International World Wide Web Conference
Madrid, Spain
[Click here](#)
- April 27-29, 2009
Critical Infrastructure and Security Risk Vulnerability Workshop
Vancouver, BC, Canada
[Click here](#)
- May 12-14, 2009
APWG Spring Counter-eCrime Operations Summit
Barcelona, Spain
[Click here](#)
- June 18-19, 2009
Tri-Lateral Security Conference
Calgary, AB, Canada
[Click here](#)

HEADLINE NEWS — January 30, 2009

What's New on the Frontline!



More Help for Police in Battle Against Cyber Crime

Team Cymru has announced the availability of a new, no cost tool to assist worldwide law enforcement with cyber investigations. The Legal Investigation Hash Table (LIgHT) consists of a bundle of the entire set of malware hashes that can be queried individually via the company's existing command line tools.

Law enforcement officers can download and import these hash tables into their forensic software and identify all the known malware on a victim or suspect machine much faster than ever before. It's hoped that this tool will free up more time, allowing officers to concentrate on making their cases against the people that abuse internet users.

The malware database is available in the hashkeeper file format via Team Cymru's existing Battle portal for law enforcement. There is no cost for the use of this data. However, access is restricted to currently-serving law enforcement officers with credentials issued by their organizations.

Users should take careful note of the disclaimers on the site — in particular the fact that this data is intended for lead purposes only and may not be used as evidence in a way that may ever enter the public domain. Law enforcement officers can apply for an account at <http://www.team-cymru.org/BATTLE/> using the username: "battle" and the password: "p1nsm4p" without the quotes.

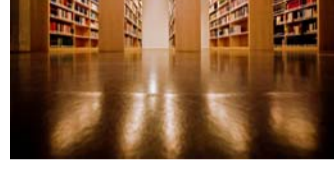
Team Cymru also expressed its appreciation to a number of police officers in Hong Kong and Australia who assisted with the project. More details, including instructions on how to load the hash files into Encase, can be found on the Battle site and in a separate email being sent to registered Battle users. As with the rest of the data that is made available to users of the Battle portal, malware hash data in this format is only for law enforcement use.

Law enforcement officers may not, under any circumstances, provide this data to anyone outside of their own law enforcement agency and, in doing so, could jeopardize the company's ability to continue to provide this service to law enforcement and may also result in individual Battle accounts being withdrawn.

For further information, contact investigations@cymru.com or use the chat function on the Battle portal, if you have access.

Welcome to E-Telligence

Twice a month, we'll be profiling guest writers, cyber crime news and important events to keep you informed.



Part 1: Using the Internet as an Investigative Research and Open Source Intelligence (OSINT) Tool

By David Toddington, Founder and President, Toddington International Inc

"The future masters of technology will have to be light-hearted and intelligent. The machine easily masters the grim and the dumb."

— Marshall McLuhan, 1969

In the late 1980s, before the development of the world wide web, futurist Alvin Toffler foresaw that in the coming millennium it would be information that would become "the commodity of greatest value."

It is now some twenty years later, the Internet is a part of our daily lives and Toffler was absolutely right. Without question, we now truly do live in an information based society.

It is currently estimated that the amount of data being globally generated is increasing at a rate of 66% per year. Information, as a commodity, is growing 10 times faster than any other commodity on the planet, natural or man-made and most of the data and information now being generated is to be found on the Internet.

Knowing how to effectively find data online and turn it into knowledge is now an essential skill-set. The role of the Internet is beginning to have a profound effect in just about every area of law enforcement, locally to internationally, tactically and strategically. Cost effective and able to provide decision makers with timely information, Internet-sourced intelligence has been proving itself highly effective in providing critical leads in ongoing investigations and intelligence gathering activities.

Internet-based Open Source Intelligence (OSINT) regularly provides early warning for disruptive events such as planned demonstrations and civil disobedience, background information to investigators with limited exposure to the subject matter and even cover in protecting sources and sensitive collection methods when disseminating analyzed data.

The key problem facing many investigators today is that they "don't know what they don't know" about searching the Internet. Recent statistics indicate that the average Internet user is highly inefficient and more likely to miss important information related to their query than not — most people use Google as their only search engine, enter only two keywords and go no further than the top ten results.

Online searching generally appears a very easy thing to do and herein lays its insidious nature; when the stakes are high and finding that one critical piece of data in the vast, quickly changing ocean of information that could change the course of an investigation, effective research skills are absolutely essential.

To use the unstructured approach and simple search techniques typical of so many Internet users, the most likely result will be missing data, wasted time and possible failure.

Effective online searching requires a good basic understanding of how the Internet is structured combined with the mechanics of different search engine technologies and the technical security and privacy issues that could see an investigator unwittingly compromise a sensitive investigation.

Effective online searching also requires critical thinking, tuned to the unique environments of many different online worlds, and the ability to effectively understand, analyze and disseminate the findings of an Internet based information-gathering project.

The World's Largest Repository of Information

"The value of a network grows as the square of the number of its users."

— Robert Metcalfe

Of critical importance to modern society, the Internet is a shared global resource of information, knowledge, and a means of collaboration among countless people and communities around the world.

While effectively impossible to quantify due to its decentralized structure, current estimates indicate that the "surface" world wide web (pages accessible through standard public search engines such as Google, Yahoo, Live, Ask) could contain as many as 20 trillion documents.

Combined with "deep" web sites (proprietary databases such as telephone directories, financial and personal information databases, etc.) and Web 2.0 sites (blogs, wiki and social networking sites to name a few examples), the estimated overall size of the web swells to potentially hundreds of trillions of documents with thousands of pieces of new information appearing every second.

Organizations that have implemented effective network security solutions may still have vulnerabilities, or holes, within their network. New vulnerabilities in networking devices, operating systems and applications, are regularly identified and reported in the media. Explicit details on how to exploit these vulnerabilities are rapidly available in numerous online locations, and are freely available to hackers and disgruntled employees alike.

A penetration test, sometimes referred to as "ethical hacking" is a controlled and managed model of an actual system intrusion by a trusted tester. It gives a realistic demonstration of an attempted break-in into your network, showing the real threats that you face from an outside intruder or an internal employee or business partner.

The Benefits of Penetration Testing

As a component of your organization's defence-in-depth security strategy, penetration testing provides several benefits:

- Identifies systems that are prone to attack or that may already have been compromised.
- Identifies gaps in the overall implementation of security, allowing organizations to rapidly implement the most cost-effective action plan to mediate risks.
- Helps managers to create and support business decisions, focusing their security budget or other resources on where they are needed most.
- Develops trust with strategic partners, suppliers, customers and others upon whom business depends.
- Fulfills requirements for regulatory compliance.
- Independent security audits are becoming a requirement for obtaining cyber-security insurance.

When to Conduct a Penetration Test

An organization should regularly schedule penetration tests of the network at least two times per year. These tests should be conducted by at least two different testers (internal and external third parties or multiple external third parties) to maximize the chance of identifying different vulnerabilities.

Penetration Testing Strategies

When considering the strategy to select when designing a penetration test, there are three parameters to consider — the attacker/defender knowledge profile, the attack route and the scope.

In a "white box test", the tester has complete knowledge of the internal network's architecture, operating systems and applications prior to testing. This strategy mimics the worst case scenario where the attacker has complete knowledge of the network.

A black box, or "blind" testing strategy, aims at simulating the actions of a real hacker. The tester has no prior knowledge of the target network. The tester might be given a website address or IP address and told to attempt to crack the website as if he were a hacker. The results of this testing methodology highlight identified vulnerabilities in a very compelling manner!

"Gray box tests," also known as "internal testing," is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an unauthorized visitor. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.

The Penetration Testing Process

Although the exact penetration testing methodologies will vary among testers, they generally follow the same series of phases:

- Discovery, in which information is gathered on the target organization through web sites and mail servers, public records and databases.
- Enumeration in which the penetration tester actively tries to obtain user names, network share information and application version information of running services.
- Vulnerability mapping in which the test team maps the profile of the environment to publicly know vulnerabilities.
- Exploitation, in which the test team will attempt to gain privileged access to a target system by exploiting the identified vulnerabilities.

The Risks Associated with Penetration Testing

Any penetration test is subject to the following limitations:

- A penetration test is a "point-in-time" snapshot; it can never be considered to be 100% comprehensive. If a new vulnerability is identified following completion of the test, then that vulnerability must be tested against the network.
- Sensitive security information may be disclosed, increasing the risk of the organization. For example, the testers will usually identify weak userID / password combinations, which could be used to compromise a network if accidentally released.

Controlling Risks — The Secrets of a Successful Penetration Test

Fully evaluate the individual tester(s). A penetration test is only as good as the individual doing the testing; therefore, when working with an external third party, ensure that you are comfortable with the individuals as much as with the third party vendor. Identify what security certifications the testers hold. Common security certifications include CCIE: Security, CEH, CISSP, CCSP, GIAC, OPSTA and Security+.

Conclusion

The proliferation of threats, from both the outside and the inside of the network, have ensured that penetration testing will be a required component of all network security programs. However, penetration testing on its own will not secure a network. Organizations have to ensure that the final step of "patching the holes" is completed, and that that mediation is fully documented.

Terry Cutler is a certified ethical hacker, master CNE, certified Linux professional and an internationally known author, trainer, speaker, and professional security consultant with Novell Canada. He is an expert in the fields of Novell technologies, penetration testing and Internet safety for children. He specializes in the anticipation, recognition and prevention of security breaches. He consults with several of the largest agencies in Canada on how to implement our products and reduce risk.

Terry is also a proud member of the High Technology Crime Investigation Association (HTCIA) To watch a free two hour presentation on ethical hacking, please visit his site at <http://www.terrycutler.com>

The enormity of the volume of information on the Internet and the lack of a definitive indexing system such as the Dewey decimal system used by libraries can create significant problems in using the web as an investigative research tool.

Becoming a good Internet researcher is not always quite as easy as it may initially appear; search engines can be awkward in that, while they may appear to be outwardly easy to use, finding specific pieces of information can be difficult and daunting due to the an engine's hidden, unique and significant limitations.

Dealing with the large amounts of data returned from a relatively simple query can be overwhelming and time consuming. The importance of information management skills and tools in even a moderately complex online investigation cannot be overstated.

Using Search Engines Effectively

Just as successful investigative work in the physical world requires specialized training and creative thinking, an online investigator must know *what* questions to ask, *where* to ask the questions and *how* to ask the question if they are consistently effective.

A search engine allows the matching of specific keywords to an online document through the use of automated software. Much like a book's index (as opposed to table of contents), which provides explicit pointers to specific keywords or phrases regardless of where they appear in that publication, search engines are full text indexes of web pages that locate keywords in matching documents regardless of where they are located on the web.

Search engines are very rarely used to their full potential by the average user. While there are many methods of maximizing the effectiveness of search tools, a simple technique to get the most out of just about any search engine is through the use of "enforced term operators".

One of the most popular enforced term operators is the use of quote marks when entering keywords into a search engine. Quote marks around keywords will force the search engine to produce results showing the keywords in the exact order that they were entered, a particularly useful technique when querying a subject's name.

A key problem with current search technology is that it is essentially "dumb"; while search engines can effectively match keywords they are not yet able to properly evaluate context and irrelevant sites will often be returned among any given search results.

Consider that variations in the spelling of a word may significantly affect search results: entering the American spelling of the phrase "organized crime", the Google search engine will produce more than 4.6 million hits.

Using the UK spelling "organised crime" Google produces more than 1.5 million results (a completely different page). Further illustrating this point, "marijuana" produces seven million results while "marijuana" produces more than 25 million very different results.

This lack of contextual understanding can create significant implications when searching for people's names (i.e. Rob, Robert, Bob, Bobby) online.

(Please see the next issue of E-Telligence for part 2 of this article.)

David Toddington will be teaching Internet Intelligence for ICC Commercial Services — a three-day course at Cambridge University on How to Use the Internet as an Effective Investigative Research Tool, March 29-April 01, 2009 (please see the link in this newsletter's calendar of events).

Toddington International Inc. provides a variety of specialized classroom and distance learning online investigative and research training programs to both the public and private sector and is a supplier to a number of police and government agencies in both the UK and Canada.

In partnership with the RCMP Pacific Region Training Centre, the Canadian Police College and the Ontario Police College, TII delivers a number of accredited, comprehensive 5-day classroom based training programs on using the Internet as an effective police research tool. In partnership with the OPC, TII offer an in-depth distance learning program. For more information and to sign up for the free bi-monthly Online Research Newsletter, visit www.toddington.com

Websites you should visit...

Fourth Annual Tri-Lateral Security Conference in Calgary
<http://www.trilateralcalgary.ca>

CISCO 2008 Annual Security Report
www.cisco.com/go/securityreport

No Advertising, No Bias, No Hidden Agenda (Advice Site)
<http://www.which.co.uk/advice/shop-safely-online/index.jsp>

If you need to print...



The E-Telligence newsletter is a green document and is not designed to be printed.

If you wish to print an article, just copy and paste the information into a Word document and print in the normal manner. The environment thanks you!

Capitalizing on the Benefits of a Penetration Test

Did you know that the most serious financial losses occur through virus attacks (more than \$42.7 billion), unauthorized access (more than \$31.2 billion), and theft of proprietary information (more than \$30.9 billion).

Organizations that have implemented effective network security solutions may still have vulnerabilities, or holes, within their network. New vulnerabilities in networking devices, operating systems and applications, are regularly identified and reported in the media. Explicit details on how to exploit these vulnerabilities are rapidly available in numerous online locations, and are freely available to hackers and disgruntled employees alike.

A penetration test, sometimes referred to as "ethical hacking" is a controlled and managed model of an actual system intrusion by a trusted tester. It gives a realistic demonstration of an attempted break-in into your network, showing the real threats that you face from an outside intruder or an internal employee or business partner.

The Benefits of Penetration Testing

As a component of your organization's defence-in-depth security strategy, penetration testing provides several benefits:

- Identifies systems that are prone to attack or that may already have been compromised.
- Identifies gaps in the overall implementation of security, allowing organizations to rapidly implement the most cost-effective action plan to mediate risks.
- Helps managers to create and support business decisions, focusing their security budget or other resources on where they are needed most.
- Develops trust with strategic partners, suppliers, customers and others upon whom business depends.
- Fulfills requirements for regulatory compliance.
- Independent security audits are becoming a requirement for obtaining cyber-security insurance.

When to Conduct a Penetration Test

An organization should regularly schedule penetration tests of the network at least two times per year. These tests should be conducted by at least two different testers (internal and external third parties or multiple external third parties) to maximize the chance of identifying different vulnerabilities.

Penetration Testing Strategies

When considering the strategy to select when designing a penetration test, there are three parameters to consider — the attacker/defender knowledge profile, the attack route and the scope.

In a "white box test", the tester has complete knowledge of the internal network's architecture, operating systems and applications prior to testing. This strategy mimics the worst case scenario where the attacker has complete knowledge of the network.

A black box, or "blind" testing strategy, aims at simulating the actions of a real hacker. The tester has no prior knowledge of the target network. The tester might be given a website address or IP address and told to attempt to crack the website as if he were a hacker. The results of this testing methodology highlight identified vulnerabilities in a very compelling manner!

"Gray box tests," also known as "internal testing," is performed from within the organization's technology environment. This test mimics an attack on the internal network by a disgruntled employee or an unauthorized visitor. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an authorized user could do to penetrate specific information resources within the organization's network.

The Penetration Testing Process

Although the exact penetration testing methodologies will vary among testers, they generally follow the same series of phases:

- Discovery, in which information is gathered on the target organization through web sites and mail servers, public records and databases.
- Enumeration in which the penetration tester actively tries to obtain user names, network share information and application version information of running services.
- Vulnerability mapping in which the test team maps the profile of the environment to publicly know vulnerabilities.
- Exploitation, in which the test team will attempt to gain privileged access to a target system by exploiting the identified vulnerabilities.

The Risks Associated with Penetration Testing

Any penetration test is subject to the following limitations:

- A penetration test is a "point-in-time" snapshot; it can never be considered to be 100% comprehensive. If a new vulnerability is identified following completion of the test, then that vulnerability must be tested against the network.
- Sensitive security information may be disclosed, increasing the risk of the organization. For example, the testers will usually identify weak userID / password combinations, which could be used to compromise a network if accidentally released.

Controlling Risks — The Secrets of a Successful Penetration Test

Fully evaluate the individual tester(s). A penetration test is only as good as the individual doing the testing; therefore, when working with an external third party, ensure that you are comfortable with the individuals as much as with the third party vendor. Identify what security certifications the testers hold. Common security certifications include CCIE: Security, CEH, CISSP, CCSP, GIAC, OPSTA and Security+.

Conclusion

The proliferation of threats, from both the outside and the inside of the network, have ensured that penetration testing will be a required component of all network security programs. However, penetration testing on its own will not secure a network. Organizations have to ensure that the final step of "patching the holes" is completed, and that that mediation is fully documented.

Terry Cutler is a certified ethical hacker, master CNE, certified Linux professional and an internationally known author, trainer, speaker, and professional security consultant with Novell Canada. He is an expert in the fields of Novell technologies, penetration testing and Internet safety for children. He specializes in the anticipation, recognition and prevention of security breaches. He consults with several of the largest agencies in Canada on how to implement our products and reduce risk.

Terry is also a proud member of the High Technology Crime Investigation Association (HTCIA) To watch a free two hour presentation on ethical hacking, please visit his site at <http://www.terrycutler.com>

You'll be Interested in This

Mac Malware Will Become Endemic Amongst High-Risk Groups
ZDNet (01/26/09) ; O'Donnell, Adam

The appearance of two trojan outbreaks on Mac machines in mid-January has IT security experts wondering if a "Mac malware epidemic" is imminent, writes engineer Adam O'Donnell. Even if attackers have not succeeded in bringing down Mac's notoriously impenetrable platform, experts believe that Mac malware is now proliferating file-sharing applications. Fortunately, the average user is probably not exposed to the risks, as the recently-exposed trojans are not circulating outside of the high-risk population, according to O'Donnell.

Anyone with a computer infected by the new batch of Mac malware will stay infected regardless of human interaction due to the absence of any tools for the identification and extraction of malware. The real question security experts are asking is if the compromising of Macs is a lucrative enough endeavor for malware authors to continue to exploit the platform. If not, the scare will be forgotten in time; otherwise, Mac users are advised to update and download new patches for their Time Machine software.

[\(go to web site\)](#)

Obama Unveils Cybersecurity Agenda
NextGov.com (01/23/09) ; Nagesh, Gautham

President Barack Obama has laid out a number of goals for improving the security of the nation's information networks. For instance, he has promised to declare the nation's IT infrastructure a strategic asset. In addition, the president has said he would appoint a national cyber advisor who would be responsible for developing a national cyber policy and for coordinating the efforts of federal agencies to improve cybersecurity.

President Obama has also pledged to prevent trade secrets from being stolen online from U.S. businesses by working with the private sector to develop new security technologies that would protect this information.

Finally, the Obama administration has said it would work to develop the next generation of secure computers, software, and networking for national security applications and other vital parts of the nation's cyber-infrastructure.

[\(go to web site\)](#)

Cyber Tips: Choosing an ISP



How do you choose an ISP?

There are thousands of ISPs and it's often difficult to decide which one best suits your needs. Some factors to consider include:

- Security:** Do you feel that the ISP is concerned about security? Does it use encryption and SSL for more information) to protect any information you submit (e.g., user name, password)?
- Privacy:** Are you comfortable with who has access to your information and how it is being handled and used?
- Services:** Does your ISP offer the services you want? Do they meet your requirements? Is there adequate support for the services?
- Cost:** Are the ISP's costs affordable? Are they reasonable for the number of services you receive, as well as the level of those services? Are you sacrificing quality and security to get the lowest price?
- Reliability:** Are the services your ISP provides reliable, or are they frequently unavailable due to maintenance, security problems, a high volume of users, or other reasons? If the ISP knows that services will be unavailable for a particular reason, does it adequately communicate that information?
- User Support:** Are there published methods for contacting customer support? Do you receive prompt and friendly service? Do their hours of availability accommodate your needs? Do the consultants have the appropriate level of knowledge?
- Speed:** How fast is your ISP's connection? Is it sufficient for accessing your email or navigating the internet?
- Recommendations:** Have you heard or seen positive reviews about the ISP? Were they from trusted sources? Does the ISP serve your geographic area? If you've uncovered negative points, are they factors you are concerned about?

For more information, please visit <http://www.us-cert.gov/cas/tips/ST04-024.html>

The Global Centre for Securing Cyberspace provides a collaborative environment that will directly impact present and future criminality on the Internet. It's a cooperative centre concept dedicated to preventing, reducing and eliminating the criminal advantage of cyberspace. Bookmark www.gcsc.org for our website.

Please email us if you have questions, special events, story ideas or experiences you would like to share. We hope you've enjoyed reading this webletter and we look forward to bringing you E-Telligence again soon.

If you wish to unsubscribe, please contact: kathy.macdonald@gcsc.ca