SHIELD Security Research Center

Hisys Journal

VOL.15

HITACHI
Inspire the Next

Hitachi Systems, Ltd.

Hisys Journal VOL.15

TABLE OF CONTENTS

About this Publication

– This publication is a publicly available product on the Hitachi Systems Security Research Center website, SSRC (Shield Security Research Center). The website also hosts back-issues (note – in Japanese), SSRC research results among other documents.
SSRC: http://www.shield.ne.jp/ssrc

Terms of Use

– This publication is produced by Hitachi Systems for informational purposes. Hitachi Systems cannot guarantee against mistakes or mistakes. Further, Hitachi Systems cannot take any responsibility for the manner in which information in this publication is used. The information in this publication was taken at a specific point in time. Thus, there may be cases where this information becomes outdated.

Jim O'Gorman a.k.a. Elwood & Marty Aharoni a.k.a. muts Interview

-Hacker Extraordiannares!
-Authors of Kali Linux
-Behind the scenes of development

When you view a demonstration at any security conference presentation, you will likely see a picture of the Kali Linux dragon on the desktop of the presenter's PC. Kali Linux has earned support from many hackers for it's distribution which specializes in penetration testing. We spoke with the developer, Mati Aharoni and his affiliate in offensive security, Jim O'Gorman on Kali Linux and Training Courses.

– Interviewer: Risa Kasahara
– Photos and Layout: Ken-ichi Saito

Offensive Security Training Valued Throughout The Industry

Risa Kasahara (afterwards, R): Hello, thank you very much for taking time for this interview as you are very busy with Blackhat Training Briefings. Today I would like to ask you about your perspectives on Offensive Security and Kali Linux. † 1 † 2

Jim O'Gorman (afterwards, J) & Marty Aharoni (afterwards, M): Thank you for the opportunity.

R Stepping right into things, can you offer an simple introduction to Offensive Security?

J Offensive Security is Enterprise Security. Outside of security analysis, which starts with penetration testing, we conduct development of the open source tool Kali Linux as well as training using Kali Linux. With Kali Linux, although there are previous distributions like BackTrack, Whax, and Whoppix, we have incorporated all of those.

R I see. Now I understand the background behind distribution.

J With Offensive Security, we also utilize another Exploit Database site. † 3 We boast that our public vulnerability database is generally the largest of its kind, and whenever exploits are included in public vulnerability intelligence, we make an effort to publish them on our site as well. Furthermore, in recent years as warnings for mobile devices increase, we have released Kali Linux NetHunter, which is a Kali Linux targeted at mobile devices. † 4

Jim O'Gorman "Elwood" (pictured left)
A penetration testing expert. In addition to leading training courses, he also works in Offensive Security consulting. He has knowledge in Network Intrusion Simulation, Digital Forensics, and Malware Analysis.

Marty Aharoni "muts" (pictured right)
A co-member of the Kali Linux development team. A network security expert, he works in both military and government industry. Though his major work is in vulnerability surveying, exploit development, and penetration testing, he also instructs training in tools and methods used by attackers.

R Is this also open source?

J Yes it is. Now, if we're speaking about business, we conduct hands on training to develop specialists who use Kali Linux. There are also recognized certifications in Offensive Security, so we receive support from throughout the industry for this.

R Why is it you think you receive such support?

J There are plenty of written tests for security qualifications, but as for hands-on style training, really there is only us. Further, we conduct a practical test to assess the qualifications of our

† 1 **Offensive Security** https://www.offensive-security.com/
† 2 **Kali Linux** https://www.kali.org/
† 3 **Exploit Database** https://www.exploit-db.com/
† 4 **Kali Linux NetHunter** https://www.kali.org/kali-linux-nethunter/

trainees and in reality, passing this test is not easy. In the last 8 years, training has continued but, during this time, I think that people who have earned certification on Offensive Security are seeing their recognition grow within the industry.

M To add one more thing, I think the situation where there are not enough security specialists is related to this. As organizations bring in human resources, our certifications have become one indicator of their qualifications.

J We offer security technologies and skill, but as time passes, these become obsolete. However, the approach to try to solve problems directly through hands-on trial and error will not become obsolete. So the heart of what we deliver is the acquisition of this attitude.

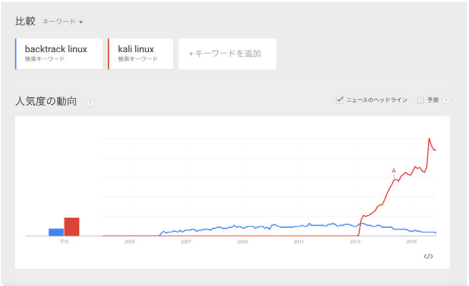
R What an excellent opinion. We've discussed that you began offering training 8 years ago, but what was your initial motivation for doing so?

M As stated earlier, there are many distributions that serve as Kali Linux's ancestors. When we originally made Live DVD Linux which consolidated numerous tools into one, the intent in developing it was the idea that we'd become free from the difficult labor of rebuilding environments. After that, in 2007 we had the opportunity to participate in BlackHat USA. At the time it was BackTrack, but I was surprised at how many people were using it. The idea to offer security knowledge to so many people just became stronger, so the following year, in 2008, we began training.

R I see, there is an importance to master the many types of penetration tests isn't there.

The Evolution of Kali Linux continues

R Moving on, I'd like to ask you about Kali Linux. Why did you switch to Kali Linux even as BackTrack was very popular?



From Google Trends - A comparison of the popularity of BackTrack Linux and Kali Linux. Compared to BackTrack (blue), since 2013 Kali Linux has become the major version in use. https://www.google.co.jp/trends/explore#q=backtrack%20linux%2C%20kali%20linux&cmpt=q&tz=Etc%2FGMT-9

M It was 2 years ago. At the time, BackTrack was popular but there was a trend where there were issues with packet management, capacity was swelling, etc. So we decided to rebuild the distribution. We changed the Linux base from Ubuntu to Debian, and rebuilt the development environment from scratch using new technologies. We also removed the outdated tools from BackTrack. This made Kali Linux both more stable and secure than BackTrack. Here I can show you some interesting data (referring to graph). This is a comparison of BackTrack and Kali Linux using Google Trends. Kali Linux has become the overwhelming topic. It is thought that interest and demand for penetration testing has risen, and if the success of this transfer has come from us then it is definitely a good feeling.

R Absolutely. That is very interesting data. Incidentally, what is the significance of the "Kali" in Kali Linux?

M Well, first, we want to bring about a meaning

in the relation to distribution. In the Swahili language, Kali means "fearlessness." It also has various meanings in other languages as well. For example, in the Philippines, it is the name of an offensive, attack-based martial art. In India, Kali is the name of a Hindu female God who oversees the destruction and creation of the world as I understand it. The Hindu significance is especially interesting considering the image of Kali Linux being born from BackTrack.

R I understand. In Japanese, "Kari" (カリ・狩り : Japanese pronunciation of Kali) means "Hunting."

M Really? That's amazing. Such a perfect image. Well definitely add that to our documents.

R What kinds of standards have you selected for the editing tool in Kali Linux?

M Excellent question. Basically, we are using the same ones normally used. Additionally, we share user and bug info on our Kali Linux Bug Tracker (bugs.kali.org), but as a reflection of user demand, we also have a editing tool.

R My next question comes from a user. With regards to the requests on your forums, is there a means for editor tool writers to get feedback from you?

M Generally, no there is not. On the forums, tool writers can insert links to their homepages. Perhaps, if there is a request to improve a tool, I recommend contacting the author directly.

R Is there a list of tools written for Kali Linux? † 5

M On the website that information is available (tools.kali.org). I believe it has 99% of available tools listed. In addition to an explanation, there is also a simple introduction on each tools' use.

R Okay, thank you. Kali Linux 2.0 will soon be released. Can you offer any insight on its characteristics?

M In Version 1, we added big changes in the Linux base. In version 2 as well, there are some major changes in this same manner. The most major change is that it will be a "rolling release." As a rolling release, it's not a set period version update, but rather there will be frequent updates to the software system. For this reason we'll be able to respond to the particulars of things like package updates, and the thought is that this will make it a major improvement to the user experience.

R I'll ask another question from a user related to user-support. This person hears that you're planning to upgrade Metasploit in Kali Linux. Not the professional version but the community version. However even if you do so, due to a warning about a different Ruby version, you may not be able to upgrade. So what measures would you propose in this situation.

M Actually, that is an improvement in Kali Linux 2.0. Since Ruby is an important part of the Metasploit package, for example even if you download the package to access GitHub, due to the differences in the Kali Linux-installed Ruby and that version, you couldn't really set it up very well. However, with the rolling release, because you're now able to appropriately time your Ruby upgrade, from here out I don't think you would have this problem.

R An excellent understanding of the improvements that Kali Linux 2.0 will bring. I'm sure that will make this user very happy! Thank you very much for your time today.

† 5 Note: This interview was conducted on August 6th, 2015, just before the release of Kali Linux 2.0 on August 11th.

SECCON 2015 Hiroshima Tournament Report

Ken-ichi Saito

SECCON 2015 Regional Preliminary, 2nd Event

SECCON † is an initiative which seeks to find and develop human resources who can act globally in the field of Information Security. The executive committee organized by JNSA (Japan Network Security Association), has functioned since 2012. In 2015, it officially started the Yokohama tournament in June.

The second regional preliminary SECCON 2015 Hiroshima tournament took place on October 24th at the Hiroshima University Satellite Campus. SECCON conducts regional competitions which focus on specific themes. For the Hiroshima event, it was a competition to run exploits against various architectures by hitting scripts and "Nekketsu" Shellcodes. Here, the shellcode targeted an assembly program that aimed to start up a shell.

There were 34 participants. From their self-introductions at the start of the tournament, 30-40% were students, while 60-70% were made up from other factions including programming and security. There were also others who gave lectures on themes such as malware analysis at security conferences. Compared to other tournaments, it appeared the skill level was quite high.

Competition Rules

The competition server ran virtual server programs from various architectures, and on these servers current directory was a file named Flag.txt. Each of these server programs had vulnerability, and thus it became possible to run several executable files or downloads.

The participants found vulnerabilities in the server programs through disassembling the executable files, then using this they wrote exploit code to show the contents of the Flag.txt file and sent it to the server. The contents shown in each Flag.txt files were recorded on the score server and became a point. The team with the most points at the end of the competition became the winner. The competition took place over 3 hours.

On the competition server, in addition to two problems about architecture of differing difficulty on (each worth 100 points), there were also trivia questions (10 points each) used (ex. What is a CTF?).
in the event.

Strategy Points

The adopted architecture for this competition was as follows+

† **SECCON 2015** http://2015.seccon.jp/

The tournament room setup at Hiroshima University's satellite campus

ARM	H8	MIPS
Power PC	SH	CRIS
FR-V	M32R	M-CORE
MN-10300	SH64	V850
Thumb	MIPS16	Blackfin
CR16	M32C	RX

The representative architecture x86 was not used. In all honesty, there were fewer architectures whose names were known to the author. There were likely lots which were unfamiliar to many of the participants as well.

Before the competition, there was an orientation from Makoto Iwamura (NTT) and the writer of the tournament problem, Hiroaki Sakai (Fujitsu). Mr.Iwamura explained the importance of running a system call in order to read the Flag. txt file's contents, and as the info inquired upon in the competition, brought up how to make the system call, return value functions, character strings, buffers and other rules.

He recommended to view the GDB simulation source code in order to investigate the system call rules, as the competition server ran on a GDB simulation. As a further strategy point, Mr. Iwamura alluded to the close compiler environment that was distributed to the participants. This environment was also used in Mr. Sakai's writing of the problem set. One could also consult this, because within the environment it contained sample programs that ran the system call.

However, in Mr. Sakai's orientation, with the V850 architecture as an example, he introduced a hint for writing shell code while making a comparison of output assembly code and the sample program's source code in C language. According to Mr. Sakai, if you could successfully analyze one architecture, you could likely guess the characteristics of other architectures.

Additionally, in the orientation, he gave a demo of the exploit execution. Within the distributed materials there was a V850 Exploit Code sample, and this sample was used in the demonstration. In other words, with the V850 issue, if participants could build their code and send it to the server, they could score some points.

A tough competition and the outcome

After the start of competition, the service and trivia problems were successively resolved by the

The scores projected on the tournament main screen. The various circles represent the participants.

"nubia" holds his award certificate and prize earned as the winner of the tournament.

participants, and there was vigorous movement on screen displaying the scoreboard. However, the movement gradually slowed, and soon it reached a stalemate.

Participants searched for the vulnerability in the architecture program, and writing the exploit code was proving to be a tall hurdle to overcome.

However, as time passed participants who earned points outside of the service and trivia problems intermittently appeared. It was "Nubia" and "El." In fact, among the 34 participants in the competition, they were the only two to resolve issues outside of the service and trivia problems.

From beginning to end, Nubia held the lead and went on to win the event by, acquiring 1220 points. This was 400 more than el, who took second place el. Nubia now advances to the SECCON Championship tournament which will take place in late January. As an additional prize, he received an autographed copy of Mr. Sakai's book, "Hello World."

Afterwards, Nubia stated that while he progressed with program analysis, he achieved victory when he became able to guess the architecture characteristics, as stated by Mr. Sakai in the orientation.

The reason for using various architectures

We spoke with SECCON executive committee member Yoshinori Takesako (Recruiting Marketing Partners) about the tournament. We tried to throw the question of whether the competition architecture was too much but according to Mr. Takesako, any architecture can be attached to regular use items such as electronics or cars, and is used by those controls. So he wanted to create a mechanism to shift attention to architecture security as we move towards the era of IoT (Internet of Things).

Additionally, if you say Exploit, most people seem to think of Black Boxing, but Mr. Takesako added he also wants people to know that you can Exploit using examinations of architecture as well.

The SECCON Regional Tournament will continue with events in Fukushima and Osaka. HISYS Journal plans to report on those competitions as well.

Reference
The SECCON 2015 Problem Set is available on Mr. Sakai's personal website at http://kozos.jp/seccon

CODE BLUE 3 Report, Part One

Ken-ichi Saito

A new challenge for CODE BLUE

As introduced in our previous issue, the 3rd CODE BLUE was held over two days from October 27th-28th at the Bellesalle Grand Shinjuku. Over the next few issues, we'll deliver articles on the event. This time, let's take a bird's eye view into CODE BLUE.

As many are already aware, CODE BLUE is an international conference where top class information security specialists gather and share information that transcends languages and borders. In addition to lectures from well-known researchers from the U.S. And Europe, it seeks out excellent researchers from across Asia, starting with Japan. The goal is to spread the results of their research across the world.

At the opening of the meeting, Executive Committee Chairman Ryouichi Sasaki from Tokyo Denki University announced several new initiatives for CODE BLUE. First, was the change from a one track system to two tracks, generating a large increase in the amount of sessions. Another one targeting development of young talent, was the establishment of a framework for lecturers 24 years old and under (U-25). Mr. Sasaki stated that through these initiatives CODE BLUE could touch on more information, and rather than simply collecting more information from participants, he wanted to build a true exchange of information.

CODE BLUE Executive Committee Chairman and Tokyo Denki University Teacher Ryouichi Sasaki

CODE BLUE Administration Representative Shinoda Kana

Shinoda Kana, a representative from the administration offices then took the podium. She announced that this CODE BLUE had far surpassed it's planned 500 participants with over 600 registrations. Further, she elaborated on the U-25 initiative that Mr. Sasaki had mentioned previously. Although there were applicants from across the world, research from two Japanese students had been selected. Additionally, among other inititaives in regard to young talent development, he added that thanks to cooperation from several industry partners, they

were able to invite 12 students to participate in CODE BLUE at no cost to them.

A Lineup Rich In Diversity

One characteristic of CODE BLUE is the wide range of lectures it provides. Over the two days there were over 24 presentations. Although there can be a tendency at information security conferences to stick with only technical topics, at CODE BLUE there were many themes of interest. Within the timetable discussions human resource development and community trends, dealing with zero-day vulnerabilities, and IoT security for health care device and smart grid research, were line up. Thanks to the establishment of the two-track system , participants were able to choose presentations that fit their own interests.

Of course there were plenty of participants who came out of their interest in technology, and the web-themed presentations were particularly popular among them. In fact, the Web presentation drew so many attendees that although it had been scheduled to take place in the smaller of the two halls used for the conference, larger one at the last-minute!

We plan to delve further into each of the lectures in the next issue with a summary of each of the presentations.

An Energetic Exchange Among Colleagues

Following the two days of presentations, a Networking Party was held in the smaller hall to allow a relaxed exchange among colleagues. The alcohol flowed and participants enjoyed a frank and relaxed discussion among each other. Throughout the event, student volunteers helped with participants, meal set-up, etc. At the Networking Party these volunteers had the chance to participate and could be seen enthusiastically speaking with many of the event speakers.

After the party, many of the pictures taken will be publicly available on the CODE BLUE Flickr account.† Participants can check the site to see if their phot ograph is on the site, and those who did not make CODE BLUE can look to see what the event was like. We asked several of the participants from overseas about their thoughts on CODE BLUE and the majority responded with statements of how well-organized the conference was.

As the 2020 Tokyo Olympics approach, the importance of Cyber Security continues to be stressed. Events like CODE BLUE are truly significant in this aspect. Each CODE BLUE event continues to grow in scale, and the expectation is that the future events will be no different.

† **CODE BLUE Flickr account** https://www.flickr.com/photos/119351343@N04/albums

A column on the current events in Cybersecurity news from an independent viewpoint

Threat Scope

#13 What is the real role of cyber intelligence?

By El Kentaro

In Cyber countermeasures, Intelligence is crucial

In the last few years, "intelligence" has become the keyword focused on in the Cybersecurity industry. But in its true meaning, what really is cyber threat intelligence?

Presently, the answer to this brings about widely varying definitions and explanations across security solutions vendors, client businesses, and government and other organizations.

In a previous column, we heard from Michael Peterson of the U.S. Central Intelligence Agency. † He touched on the state of intelligence rooted in his 40 years of experience with the agency. This time, I'd like to introduce the blog written by Greg Day, Vice President and Chief Security Officer for Europe, Middle East & Africa at Palo Alto Networks, in which he discusses cyber threat intelligence.

In a threat situation that continues to change each day, what really is Cyber Threat Intelligence? Further, is a vast amount of information really "intelligence?" In asking these questions, Mr. Day speaks on his own experience and viewpoint about the role that Cyber Intelligence should hold.

Seek quality over quantity!

Speaking on his experience after participating in a certain leadership event, Mr. Day stated that the majority of what he heard on "intelligence" from management levels was really just noise with little actual value.

Certainly, when vulnerabilities surface, technological information related them grows massively, just as when cyber attacks are confirmed, raw data on things like domain names and IP addresses also increases rapidly. However, in what ways can we analyze this raw data to produce real intelligence that has value? Mr. Day points out that recently the change from "data" to "intelligence" is what is being sought after in Cyber Intelligence.

Next, in discussing the rapid increase in vulnerabilities, he mentioned that the number of CVE registered incidents in 2014 grew to 9751, meaning that each day an average of 27 vulnerabilities and threats are revealed. As such, Mr. Day notes that you can compare statements such as Sociologist Edward Osborne Wilson's remark that "we are drowning in information, while starving for wisdom," or the U.S. FBI's definition of intelligence, "information that has been analyzed and refined so that it is useful to policymakers in making decisions." In doing so, he notes that we have surpassed the amount

† **HISYS Journal Vol.8** http://www.shield.ne.jp/ssrc/contents/doc/SSRC-HJ-201504.pdf

of information that security experts can handle within the time available to make decisions.

However, Day points out that in this situation, there is still a chance to to produce real Intelligence. He stresses the importance of the following three opportunities for intelligence to add value.

1) Ensuring protection against as many threats as possible, as rapidly as possible..
2) Be able to identify which high risk attacks are likely to impact your organization.
3) Be able to analyze from Indicators of Compromise which attacks to be proactive against within your organization.

Particularly, it is #3 which is the problem that troubles security experts. As in cases of large scale information leaks in the media where IOCs were discovered but not acted upon stand out, even when a compromise is suspected it can be difficult to decide on exactly what kind of attack it is or what it indicates. Of course, as a countermeasure to this problem the majority of organizations engage in information sharing but the information is often limited only to members within the organization.

Towards increasing the quality of intelligence

In order to make possible valuable intelligence from the aforementioned three points, the practical use of appropriately timed, practical decisions and disposition methods, few false detections, and a complete overhead view of the organization is critical, according to Mr. Day.

The current state of security in cyberspace is thought of in terms in winning and losing. As threats and events continue to increase, even though tools that use SIEM (Security Information and Event Management) can support in the threat countermeasure process, it is critical to combine both internal and external information in developing intelligence.

As a final last point on the importance of cyber countermeasures, Day wraps up with a note on the layout of human resources. In each organization there are a limited number of people to work threats, and to keep up with the increasing speed of attacks and threats. The more we can automate activity, the more we can use those human resources to focus on the activities where we need them.

Reference
Bland Information Overload or Business-Critical Intelligence?
http://researchcenter.paloaltonetworks.com/2015/11/bland-information-overload-or-business-critical-intelligence/