

Home > Editorial Boards >

## IJSPS News

March 8th, 2023 News! IJSPS Vol. 11, No. 1 has been published online.

November 30th, 2022 News! IJSPS Vol. 10, No. 4 has been published online.

Agusut 27th, 2022 News! IJSPS Vol. 10, No. 3 has been published online.

June 30th, 2022 News! IJSPS Vol. 10, No. 2 has been published online.

## Submissions

Please send your full manuscript to: [ijsp@ejournal.net](mailto:ijsp@ejournal.net)

## Useful Documents

[Paper Template](#)

[Copyright Statement](#)

[Application For Reviewers](#)

## FAQs

### 1. How to submit my research paper? What's the process of publication of my paper?

The journal receives submitted manuscripts via email only. Please submit your research paper in .doc or .pdf format to the submission email: [ijsp@ejournal.net](mailto:ijsp@ejournal.net).

### 2. Can I submit an abstract?

The journal publishes full research papers. So only full paper submission should be considered for possible publication...[Read More]

## Editorial Boards

### Editor-in-Chief



Prof. Houssain Kettani  
Dakota State University, USA

### Executive Editor

Prof. Zhusheng Kang  
University of Electronic Science and Technology of China, China

### Editorial Board

Assoc. Prof. Kun Hua

Department of Electrical and Computer Engineering,  
Lawrence Technological University, E220 Southfield, MI,  
USA

Assoc. Prof. Brian Kelley

Department of Electrical and Computer Engineering,  
The University of Texas at San Antonio, USA

Assoc. Prof. Ignacio Bosch Roig

Departamento de Comunicaciones, Universidad  
Politécnica de Valencia, Spain

Dr. Fernando Soares Schindwein

Department of Engineering, University of Leicester, UK

Assoc. Prof. Jun Qin

Department of Electrical and Computer Engineering,  
Southern Illinois University Carbondale, Carbondale,  
IL 62901, USA

Prof. Youngwook Kim

Department of Electrical and Computer Eng.,  
California State University, Fresno, USA

Asst. Prof. Mario Flores

Department of Electrical and Computer Engineering,  
The University of Texas at San Antonio, USA

Prof. Jérôme Antoni

University of Lyon, France

We welcome experts and professionals to join our Editorial Board. If you are interested in becoming an Editor, please complete the [Application Form](#) and send it to [ijsp@ejournal.net](mailto:ijsp@ejournal.net).

We will review your information and if appropriate, we will place you on our list of Editorial Board.

## IJSPS News

March 8th, 2023 News! IJSPS Vol. 11, No. 1 has been published online.

November 30th, 2022 News! IJSPS Vol. 10, No. 4 has been published online.

Agustus 27th, 2022 News! IJSPS Vol. 10, No. 3 has been published online.

June 30th, 2022 News! IJSPS Vol. 10, No. 2 has been published online.

## Submissions

Please send your full manuscript to: [ijsp@ejournal.net](mailto:ijsp@ejournal.net)

## Useful Documents

[Paper Template](#)

[Copyright Statement](#)

[Application For Reviewers](#)

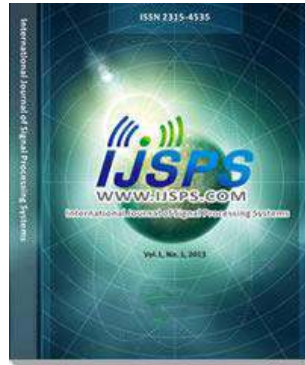
## FAQs

**1. How to submit my research paper? What's the process of publication of my paper?**

The journal receives submitted manuscripts via email only. Please submit your research paper in .doc or .pdf format to the submission email: [ijsp@ejournal.net](mailto:ijsp@ejournal.net).

**2. Can I submit an abstract?**

The journal publishes full research papers. So only full paper submission should be considered for possible publication...[\[Read More\]](#)



## International Journal of Signal Processing Systems

IJSPS aims to provide a high profile, leading edge forum for academic researchers, industrial professionals, engineers, consultants, managers, educators and policy makers working in the field to contribute and disseminate innovative new work on Signal Processing Systems. All papers will be blind reviewed and accepted papers will be published biannual, which is available online (open access) and in printed version.

2022

### Recently Published Papers



#### Dynamic Channelization Model Based on Non-maximally Decimated Filter Bank

Tong Liu, Fangming Shi, Wenxu Zhang, and Jianbo Hu

**Abstract**—A model is proposed, called dynamic channelization model based on non-maximally decimated filter bank, to solve the uncertainty and time-varying nature of subband signals' number, bandwidth and location distribution. The structure divided the receiving signal into several sub bands evenly based on signal reconstruction theory. We input the adjacent subbands signals...[\[Read more\]](#)

ISSN: 2315-4535 (Print)

Abbreviated Title: Int. J. Signal Process. Syst.

Editor-in-Chief: Prof. Houssain Kettani

Associate Executive Editor: Ms. Cherry L. Chen

DOI: 10.18178/ijsp

Abstracting/Indexing: Ulrich's Periodicals Directory, Google Scholar, Crossref, etc.

E-mail questions or comments to [IJSPS Editorial Office](mailto:ijsp@ejournal.net).



**Dr. Houssain Kettani**

Dakota State University, USA

I am very excited to serve as the first Editor-in-Chief of the International Journal of Signal Processing Systems (IJSPS) and hope that the publication can enrich the... [\[Read More\]](#)



## Contact Us

International Journal of Signal Processing Systems

E-mail: [ijsp@ejournal.net](mailto:ijsp@ejournal.net)

Home > Published Issues > 2016 > Volume 4, No. 3, June 2016 >

### IJSPS News

- March 8th, 2023 News! IJSPS Vol. 11, No. 1 has been published online.
- November 30th, 2022 News! IJSPS Vol. 10, No. 4 has been published online.
- Agustus 27th, 2022 News! IJSPS Vol. 10, No. 3 has been published online.
- June 30th, 2022 News! IJSPS Vol. 10, No. 2 has been published online.

### Submissions

- Please send your full manuscript to: [ijsp@ejournal.net](mailto:ijsp@ejournal.net)

### Useful Documents

- Paper Template
- Copyright Statement
- Application For Reviewers

### FAQs

#### 1. How to submit my research paper? What's the process of publication of my paper?

The journal receives submitted manuscripts via email only. Please submit your research paper in .doc or .pdf format to the submission email: [ijsp@ejournal.net](mailto:ijsp@ejournal.net).

#### 2. Can I submit an abstract?

The journal publishes full research papers. So only full paper submission should be considered for possible publication...[Read More]

Article#	Article Title & Authors (Volume 4, No. 3, June 2016)	Page
<b>CONTENT</b>		
1	On Enhancement of Reading Brain Performance Using Artificial Neural Networks' Modeling <i>Hassan M. H. Mustafa, Mohamed Abdulrahman, Shahinez Mahmoud, Ayesha Sohail, and Nosipho Dladu</i>	177
2	On a New Competence Measure Applied to the Combining Multiclassifier System <i>Marek Kurzynski</i>	185
3	Network Element Simulation Based on Log Files <i>Bahadır Taşdemir, İzzet Çelik, Ferit Ünlü, Caner Reşber, and Ömer Sönmez</i>	192
4	A Supervised Learning Approach for the Fusion of Multiple Classifier Outputs <i>C. Ulas, B. Koroglu, C. Bekar, O. Burcak, and O. Agin</i>	198
5	Vulnerability Research and Mapping of Campus Network <i>Justinus Andjarwirawan, Agustinus Noertjahyana, and Devi C. Angi</i>	204
6	Parallel Processing of Ray Tracing on GPU with Dynamic Pipelining <i>Mekhriddin Rakhimov Fazliddinovich and Yalew Kidane Tolcha</i>	209
7	Obstruent Consonant Landmark Detection in Thai Continuous Speech <i>Siripong Potisuk</i>	214
8	Review of Parameter Estimation Techniques for Time-Varying Autoregressive Models of Biomedical Signals <i>A. R. Najeeb, M. J. E. Salami, T. Gunawan, and A. M. Aibinu</i>	220
9	Reduction of Impulsive Noise in OFDM Systems Using a Hybrid Method <i>Alina Mirza, Sumrin Mehak Kabir, and Shahzad Amin Sheikh</i>	226
10	An Efficient Turbo Equalization for Faster than Nyquist Signal <i>Chang-Uk Baek and Ji-Won Jung</i>	231
11	Solving the Problem of the Accents for Speech Recognition Systems <i>Irakli Kardava, Jemal Antidze, and Nana Gulua</i>	235
12	Location Selection for Versatile Characters of Image Based CAPTCHA <i>Chen-Chiung Hsieh, Yu-Chen Lin, Kai-Miao Cha, and Chao-Wei Huang</i>	239
13	Partially and Fully Constrained Least Squares Linear Spectral Mixture Models for Subpixel Land Cover Classification Using Landsat Data <i>Uttam Kumar, Cristina Milesi, Ramakrishna R. Nemani, S. Kumar Raja, Weile Wang, and Sangram Ganguly</i>	245
14	The Technology of Parallel Processing on Multicore Processors <i>Musaev Muhammadjon Mahmudovich and Berdanov Ulug'bek Abdumurodovich</i>	252
15	Human Ear Localization: A Template-Based Approach <i>Alaa Halawani and Haibo Li</i>	258

# Vulnerability Research and Mapping of Campus Network

Justinus Andjarwirawan

Petra Christian University/Informatics Department, Surabaya, Indonesia

Email: justin@petra.ac.id

Agustinus Noertjahyana and Devi C. Angi

Petra Christian University/Informatics Department, Surabaya, Indonesia

Email: agust@petra.ac.id, m26411163@john.petra.ac.id

**Abstract** — Vulnerability of computer systems in campus-wide network has been an issue for years, since networks were open to allow anonymous access. It will take many studies of computer security to protect. A vulnerability research and mapping of a network is a step to address the issue, as well as minimizing security breach in the future.

Evaluation of a network security can be done by many tools available and also guidelines based on CEH (Certified Ethical Hacker) module and Acunetix for web specific security.

With CEH and Acunetix guidelines, the evaluation shows many common security weaknesses and therefore this evaluation leads to security recommendations based on the weaknesses and security holes found.

**Index Terms** — vulnerability, penetration testing, vulnerability scanning, certified ethical hacker, acunetix

## I. INTRODUCTION

Network security evaluation is done inside Petra Christian University, Surabaya, Indonesia, as the target. The chosen test object has a very common university network configuration. Common configuration also delivers common attacks such as computer virus, trojan, backdoors, spams, as well as cross-site scripting and SQL injection.

Universities today still manage their own web servers, mail servers and databases. The focus of monitoring intrusions are on these servers, besides the routers and firewalls.

Penetration test or pentest is one method to evaluate a computer network security parameter. Most reports of the penetration test are used to define protections against possible future attack.

### A. Problem Statements

Monitoring campus-wide computer network and servers. The first step to evaluate this wide network is collecting all information about the existing network and active servers in the area.

Expected solutions to secure a campus-wide network are based on the evaluation. Mapping is given after a full scan of the entire network. A report of the whole scanning, penetration test and test tools results is given at

the end of the test. CEH (Certified Ethical Hacker) by EC-Council will be the guideline to analyze and implement a security policy, as suggested (K. Graves, 2010)[5].

Acunetix is a software as a tool to analyze vulnerabilities of web sites and web based applications. Cross-site Scripting (XSS) and SQL injection are the top security vulnerabilities found.

ints after.

### B. Methodology

Surveys of the existing Local Area Networks (LANs), servers, infrastructure are done both by interviews and own scanning. Accessing to the campus network is available through wireless network, wired network, and also the Internet.

Filter and limitation of the network access through a router or firewall are easily detected by doing a port scanning with nmap tool. A firewall test must be done both ways, from inside the campus network to the Internet and from the Internet to the demilitarized zone (DMZ) of campus network.

## II. THEORIES

### A. Network Security

There is no network that is capable of anti tapping nor computer network that is completely secure. The nature of a computer network is for communication. Each communication can fall into the hands of others and can be misused. Security systems help secure the network without blocking the user and puts anticipation when the network successfully penetrated. In addition, it is important to make sure that the users in the network have sufficient knowledge about the safety and that they accept and understand how the security plans are made.

There are two main elements of forming a secure network, they are:

1. Firewall, both physical and virtual, which is placed between the device and network services used and the people who may misbehave.

2. The security plan, which will be implemented together with the users to keep the system from penetration from outside.

In addition to those described above, network security can be aimed for information system owners that can keep their information system from compromised by others, which in turn can damage the system.

The type of intruder may include:

- The Curious: this type of intruder is basically interested in finding the type of system and data owned by a person or company.
- The Malicious: type of intruder is trying to ruin someone else's system or modify a webpage.
- The High-Profile Intruder: this type is trying to use someone else's system to gain popularity and fame.
- The Competition: this type of intruder is interested in what data you have in the system of organization or others.

Computer security is one important aspect of an information system. Meanwhile, a network itself can also be secured from attacks. In terms of the types of existing network security, they are: Confidentiality, Integrity, Availability, Non-repudiation, Authentication and Accountability.

### B. Hacking

Hacking is a common term that is usually negative, but in the definition itself hacking is a way of someone who manipulates things to perform better or useful for another purpose. A negative person doing a bad hacking is known as a cracker, or those who do cracking a system.

A computer hacker term may mean either bad or good depending on the purpose of hacking. A hacker may damage confidential information, steal confidential information, and also modify them.

But a hacker may do good things for good purposes, that they were called white hat hackers. Also a good hacker term is used for the certification such as CEH.

### C. Penetration Test

The purpose of penetration testing is to find vulnerabilities of a system. There are two types of testing, they are: external testing and internal testing.

External testing is to test all available information and access that is available to public or without any kind of authentication.

Internal testing is to recognize the number of network access points internally.

The analysis done in this research to the objective campus is by using the external testing.

The three methods of penetration testing are: Passive, Active and Aggressive. Passive test will test inside web applications, logins and configurations. Active test will do input manipulations, possess access rights and test all known vulnerabilities. Aggressive test will do the vulnerability exploits, reverse engineer a software or system, putting a backdoor, steal codes and manipulate finance related information.

The campus object test is done with the passive type of penetration test.

The penetration phases are: discovery, enumeration, vulnerability mapping, exploitation, as also found in many campus wide penetration tests[3][4], and finally report generation.

## III. ANALYSIS

The purpose of this research is to find weaknesses, that is the vulnerabilities of the network and systems, then also to deliver solutions to secure those vulnerabilities.

The tools used for the test are penetration tools softwares that are suggested by CEH.

The first tool is for footprinting, using Angry IP Scanner, and then scanning with Acunetix, and finally enumeration with Softperfect Network Scanner. Some tools that are suggested by CEH are paid commercial applications. The rest are open source applications.

According to CEH, 90% of the time a hacker spends their time is to collect information. The rest are to take over the target.

Footprinting which is the first thing to do as a hacker is to define the target by doing port scanning to all available IP addresses of the target network, to find available services and active hosts.

Footprinting the campus network finds information:

- target IP addresses
- live services: web (http & https), ftp, ssh
- host names
- application version (e.g. web server version)

The Acunetix tool delivers a report that counts the numbers of vulnerabilities and the level of the security vulnerability, from low, medium, to high; as in Microsoft[1]. Table I shows major vulnerabilities found in the testing.

TABLE I. VULNERABILITY SUMMARY

Description				
No.	Attacks	Vulnerability	Total alerts	Level
1	Cross Site Scripting (XSS)	Cross site scripting (verified)	12	High
		jQuery cross site scripting	8	High
2	SQL Injection	Blind SQL Injection	7	High
3	CSRF (Cross Site Request Forgery) protection	HTML form without CSRF protection	18	Medium

## IV. CONCLUSION

Port scannings were not completely tested on all available ports, which may miss a few known services that changed their default ports.

Many web sites and web applications are found to be vulnerable to Distributed Denial of Service (DDoS).

Old versions of web servers are also spotted. Many web applications are found to have using old versions and deprecated functions which could cause a Cross-Site Scripting and SQL injection attacks. These are the most vulnerabilities found commonly in other organizations[2].

The suggestions are to always keep an up to date versions of operating systems and applications. Also to do periodic tests. It is also suggested to classify port penetration attempts and in percentage values[1] and weights, therefore administrators will have priorities to anticipate future attacks based on the most probable attempts.

#### ACKNOWLEDGMENT

The author wish to thank the ICCCV committees for accepting this paper, and also Agustinus Noertjahyana and Devi C. Angi for supporting the research.

#### REFERENCES

- [1] Yeu-Pon Lai, Po-Lun Hsia, "Using the vulnerability information of computer systems to improve the network security", *Computer Communications* Volume 30, issue 9, Elsevier, 30 June 2007, pp. 2032-2047.

- [2] Mvungi, N.H., Mfinanga, D.A., Mwinyiwiwa, B.M.M., "Intrusion detection by penetration test in an organization network", in *Adaptive Science & Technology*, IEEE, Jan 2009, pp. 226-231.
- [3] Zulazeze Sahri, Muhd Eizan Shafiq Abd Aziz, Khairul Ikhwan Zolkefley, Roslan Sadjirin, Mohd Ikhsan Md Raus, "Implementing IT Security Penetration Testing in Higher Education Institute", in *Australian Journal of Basic and Applied Sciences*, ISSN: 1991-8178, 2014, pp. 67-72.
- [4] Arya Sedigh, Kapilan Radhakrishnana, Carlene E-A Campbella, Dhananjay Singh, "Trust Evaluation of the Current Security Measures Against Key Network Attacks", *MAGNT Research Report*, ISSN 1444-8939, 2014.
- [5] Kimberly Graves, "CEH Certified Ethical Hacker Study Guide", Sybex, 2010.



**Justinus Andjarwirawan** is a lecturer in the Informatics Engineering department of Petra Christian University. It is based in Surabaya city, Indonesia. Born in Central Java, Indonesia in 1972.

He has a bachelor degree of Electrical Engineering from Petra Christian University, Indonesia, and a master degree in Computer Science from Asian Institute of Technology, Thailand. His current interest and teaching subjects are Open Source Programming, Mobile Programming, and Web Programming. Research interest in subjects of computer networking, user experience, user interface, human-computer interaction, web technology, and mobile applications.