Security Architecture

From Matchi Wiki

Contents

Access Matrix of Matchi's Sub-Systems

High-level summary of access levels to content and sub-systems, with authentication method:

Sub-System Access Matrix											
	Use Case:										
Access Area	**Public/Guest**	**Content Manager**	**Innovators**	**Buyers**	**Sponsors**	**Challenge Owner**	**Challenge Admin**	**Challenge Judge**	**Developer**	**Tester**	**System Administrator**
Website public pages	Open	Open	Open	Open	Open	Open	Open	Open	Open	Open	Open
Website own innovation			Password						Password	Password	Password
Website others' innovations				Password	Password	Password	Password	Password	Password	Password	Password
Website content management		Password							Password	Password	Password
Website functional development									Password	Password	Password
Website functional administration									Password	Password	Password
Challenge Entry			Password							Password	Password
Challenge Scoring								Password		Password	Password
Challenge Management							Password			Password	Password
Challenge Reports						Password			Password	Password	Password
Server development									PPK	PPK	PPK
Server operations									PPK	PPK	PPK
Sever administration											PPK+SUDO
Database development									Password	Password	Password
Database operations									Password	Password	Password
Database administration											Password
Business systems development									Password	Password	Password
Business systems operations									Password	Password	Password
Business systems administrations											Password

Notes on simplifications

1. Business Support Systems have been grouped together and currently have the same access model and methods and consist of:

- Self-hosted:
  - JIRA Issue Management
  - TEMPO Timesheet management
  - Wiki system documentation
  - OwnCloud file storage documentation system (in the process of replacing DropBox)
- Cloud-hosted:
  - ZoHo CRM and tactical reporting system
  - DropBox tactical file storage and sharing system
  - GMail Email and Calendaring system
  - Slack Communications

- BitBucket configuration management

2. Both System Administration roles and Developer and Tester roles span over the following:

- Business Support sub-system
- Server Backend sub-system
- Website

Technical Details on Authentications

- **Password**: Joomla password authentication mechanism, uses various password saltings, hashes and the BCrypt library.
- **PKK**: Public/Private key authentication with 1024-bit RSA encryption and using the OpenSSH library. It is only possible to connect as user *madman*.
- **SUDO + PKK**: Same as PKK, but a `sudo` command is required to escalate the user to user *root*, since it has been made impossible to directly connect as user *root*.

Security Overview

Common Weaknesses in an enterprise

The top weaknesses in the security chain in an enterprise are the staff / employees who work for the enterprise. This is why they are the commonest attack vector.

Origins of Attacks

Types of Attacks

Sophisticated attacks

A sophisticated attack can take a long time to plan and is executed over a number of days. The planning usually involves profiling a selection of individuals in the company. They are usually aimed at high-value companies. The average cost to cyber-criminals of a planned attack averages at about $1300. The most common attacks are:

- **Spear Phishing attack**: This is mostly done via a plausible-looking email that can contain booby-trapped attachments that unleashes malware on the victim's machine if the attachment is opened or viewed, or an instruction to go to a website that the victim sheepishly follows - however the website is a plausible copy of a real website and armed with malware or information-capturing features.

- **Watering Hole attack**: By offloading mal-ware from a peripheral site that is known to be visitid by an individual, the mal-ware executes its attack when the individual subsequently visits the target site.

Brute Force attacks

These are simple in nature and are aimed at public-facing systems, such as websites and email servers. The cost of these attacks are trivial, as the attackers simply run a never-ending script that scans random IP addresses until a possible victim is found. The most frequently-encountered attacks are:

- **Dictionary attacks**: These are aimed at servers themselves, websites logins, and email logins.
- **Distributed Denial of Service**: Many compromised computers can be instructed to send resource-consuming IP packets to the targeted server or domain, and so rendering the server incapable of performing its intended function

Attack Vectors

Direct server attack on specific ports

Attack on port 21/22: SSH secure shell

This is usually committed by opportunistic "script-kiddies" who deploy as password dictionary attack against the user 'root'. This is the simplest form of attack, which is why it is so popular. Once a server has been compromised and a server session is obtained, much local damage can be committed, and the server can be used as a launching point to compromise more servers, thus further obfuscating the attacker's origins.

Attack Surface area

All Matchi servers are visible on the public Internet, and there is little point in changing the stadard SSH port from 22 to something else, since a port-scan will show the few open ports and making the guessing of the SSH port trivial.

It is planned to place SSH-access to the servers behind a VPN in future as a further precaution.

Potential damage

Dictionary attacks waste bandwidth and computation resources. Even though password authentication is not possible on Matchi servers, not all attack scripts are sophisticated to detect this and cease the dictionary attack.

Should an SSH attack have been successful, an attacker could have

- Vandalised the system
- Added spamming or DDoS processes to run on the server
- Opened up ports to the public for internal services
- Installed a root-kit in order to access the server at leisure at the later time
- Uploaded illegal or incriminating content
- Host a phishing site
- etc...

Defences

SSH Daemon Configuration The SSH Daemon has been configured in each server such that:

- Access via SSH is not possible using password
- It is impossible to log in to any servers as user *root*
- It is only passible to log as one single nominated account. Subsequent escalation to user *root* is possible once logged in, where required.

Fail2Ban Fail2Ban daemon runs on each server:

- Fail2Ban immediately bans an IP address after one failed attempt to connect. The ban is lifted after 24 hours to stop the blacklist on the server's firewall from growing out of control.

RKHunter The RKHunter daemon (Root-Kit Hunter) runs on each server:

- Detects if any of the binary files have been altered, and if so, it sends out an email alert to security@matchi.biz
- Looks for file signatures in files that match those of known root-kits. If one is found, it sends out an email alert to security@matchi.biz

Automated Detection

A daily digest of banned IP addresses detected by the Fail2Ban daemon is sent to security@matchi.biz.

Manual Detection

- Log files can be analysed to see which sessions were disconnected.*

```
root@mweb02 /var/log # grep "disconnect" secure |awk '{print $9}' | grep '[1-9]' | sort -u | sed -e 's/:$//'
112.216.65.78
112.85.42.107
112.85.42.46
112.85.42.99
113.195.145.13
115.146.123.162
116.31.116.43
etc...
```

The IP addresses are inevitably shown to originate from unusual locations, like Vietnam below:

```
root@mweb02 /var/log # whois 115.146.123.162
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html
% Information related to '115.146.120.0 - 115.146.127.255'
inetnum:        115.146.120.0 - 115.146.127.255
netname:        CMCTELECOM-VNNIC-VN
descr:          CMC Telecommunications Services Company
descr:          273 Doi Can str, Ba Dinh, Ha Noi
etc...
```

- Check who is currently logged on to the server*

It would only be one, sometimes two sessions on a server.

```
root@mweb02 /var/log # w
 23:11:30 up 108 days,  5:53,  1 user,  load average: 1.53, 1.80, 1.53
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
madman   pts/1    97e4a9a1.skybroa Mon22    2.00s  0.20s  0.00s sshd: madman [priv]
```

Recovery

Recovery from a successful SSH attack if root access was obtained is risky and if possible, a full server rebuild is preferred.

Possible recovery steps after an attack like this are, in order of increasing effort:

- If only a root-kit was discovered, the adulterated files can be replaced by just re-installing the relevant packages
- The server needs to go into fail over mode (if a fail-over server exists for the attacked server)
- All packages on the compromised are re-installed, if the package manifest has not been corrupted
- Capture all access logs for later analysis and evidence if a server rebuild is required (see next steps)
- The compromised server needs to be rebuilt from a recent diskimage that is known to not be compromised
- The compromised server needs to be rebuilt from scratch

Attack on port 25: Postfix SMTP mail service

An attacker can attempt to send or relay spam emails via the SMTP services that on services.

Attack Surface area

Each server runs an SMTP service that acts as a relay for locally-generated emails to the GMail email service.

Potential damage

- Reputational damage
- If sufficient complaints are lodged, the matchi.biz domain may be repoted to one of many spam-prevention offices such as Spamhaus. This will cause most outgiong emails from Matchi to automatically get rejected by the recipient.

Defences

- Post 25 is only accessible from with the server.

Detection

It is currently only possible to detect SMTP-service abuse by studying the SMTP/Postfix log files

Recovery

After having determined which anti-span offices deem the matchi.biz domain to be a spam originator, it is possible to appeal to each of them to them in order to remove the blacklisting. This is a very time-consuming process and the request will only be effected after 24 hours at least, since email servers typically update their local spam domain blacklists once per day.

Attack on port 80/441: Apache Webserver

A whole range of attacks are possible the Apache attacks in order to compromise its integrity, slow it down, or crash it.

Attack Surface area

- The public-facing website at http://matchi.biz
- The administration website at http://matchi.biz/administrator

Potential damage

Most of the attack types results in a loss of performance or loss of integrity of the presented data on a browser. Ultimately, reputation suffers followed by the inevitable loss of revenue.

Defenses

- Keep the patch-level of Apache up to date
- Cloudflare prevents a number of typical attacks types on Apache

Detection

Recovery

Distributed Denial of Service (DDoS) attack on servers

Attack Surface area

Any of the Matchi servers in the data centre. DDoS attacks are usually focussed on webservers, however.

Potential damage

Loss of service to users, that can range from being annoying through to being detrimental to revenue. A DDoS usually results in a loss of reputation.

Defenses

All traffic to the webserver is bound to the domain matchi.biz and is routed via the Cloudflare Content Delivery Service. Cloudflare additionally offers a low-level DDoS prevention. On experiencing a DDoS attack, Cloudflare can manually be set to actively repel DoS agents.

Detection

- When access to the website is slow
- Observing the session count on Apache management console

- Keeping abreast with current DDoS attacks on http://www.digitalattackmap.com/

Recovery

Matchi's reputation needs to be restored. It may be prudent to send an email to all users who are believed to have a session open on the website at the time of the attack, depending on the severity of the impact - should the defense have failed for whatever reason.

Additional reading

- https://f5.com/Portals/1/PDF/security/2016_DDoS_Attack-Trends.pdf

Website fake user account creation

Attack Surface area

The Matchi website: An adversary would attempt to create an account (either automatically or manually) in the hope that the account would be approved and access to the Matchi Innovation Database be obtained.

Potential damage

- This adds an unnecessary workload on the load on member management staff, who need to remove this person.
- Should an attacker accidentally be given access as an innovator, the attacker can only see his own innovation and not that those of others.
- There is no limit to the number of innovations that an innovator can create, and an adversary who has obtained access could automate the creation of unlimited innovations, which will consume system resources.

Defenses

- The sign-up process is protected by Google's "I am not a robot" reCAPTCHA. This is a very successful measure, although there are reports that it can be circumvented in automated attack scripts.
- The sign-up process includes an email verification step
- Every user who applies to become a member (Innovator, Buyer, Sponsor, Challenge Owner), is manually vetted. A failed applicant can summarily be rejected. Each member approval event or rejection event is notified to other member management staff.
- Members' email addressed that belong email domains known to be favourited by attackers, are scrutinised and if the email has not been verified within a certain period, or the applicant has not been accepted within a certain period, then the applicant is summarily rejected. The applicant is not notified of this event. A list of all automated rejections is emailed in a daily digest to security@matchi.biz.
- New email domains that are used can be added to the configuration of automated rejection process.

Detection

- Invalid sign-ups that pass the initial scrutiny can only manually be detected, which number on average one per month.
- An adversary who has obtained access and who automates the creation of unlimited innovations will draw attention on completing the innovation entry.

Recovery

Any (fake) innovations that an attacker may have created are automatically removed when that user is removed from the Matchi members' database.

Dictionary attack agaisnt the Matchi website

Attack Surface area

The Matchi website: An adversary would attempt to access the site with random user names and passwords (either automatically or manually) in the hope that access to the Matchi Innovation Database be obtained.

Potential damage

- Consumes network and system resources
- A successful attack to the correct user account allows access to all Matchi Innovations.

Defenses

Successive, repeated failures with a given time frame to gain access is detected and the attacker's origin IP address is permanently banned. The number of repeats and time frame duration is configurable.

Detection

The list of banned IP addresses can be viewed through the "Brute Force Stop" Joomla component in the Matchi Administration website.

Recovery

It is not possible to undo any data-theft damage done by an adversary who has gained unlawful access to the system.

Website SQL injection

By manipulating a URL on a database-driven website and adding SQL commands, it can be possible to effect data changes on the database.

The favourite motive for an attack is to replace website content in order to espouse some ideology or to brag amongst peers.

Attack Surface area

The Matchi webserver

Potential damage

The potential damage from such an attack is limitless. If the

Defenses

All SQL operations on the Matchi site are performed via the Joomla database API, which offers a very solid protection against this. The Joomla Framework is regularly updated as new vulnerabilities are discovered. Most vulnerabilities are "zero-day", which means that they have not yet been know to be used "in the wild" by attackers.

Detection

It is not possible to detect a SQL Injection attack as such: Data will either be observed as incorrect or deleted, or parts of the Matchi website will not work correctly.

Immediate action

Ban the attacking IP address from all the Matchi servers

Recovery

- Restore the most recent backup know to now have been subjected to this attack
- Switch over to the fail-over system, if it can be ascertained that the fail-over database does not contain a replication of the production database's attack.

Website data slurping

It is in theory possible to slurp attachment documents and customers' corporate logos.

Attack Surface area

Matchi webserver

Potential damage

- An adversary can infer what innovations are on the Matchi Innovation Database by looking at the collection of innovation-related documents and the corporate logos.

Defenses

- The Matchi website is front-ended by Cloudflare, which detects unusual content downloads to a single IP address and will stop it.
- There are .htaccess files that are configured to prevent access to directories that contain collections of images and documents

Detection

This can manually be detected by looking at server logs and the volume that is downloaded to an IP address.

Recovery

It is not possible to recover from an attack like this.

Uploading Malware in Attachments

Attack Surface area

Innovators only can upload files to further support their innovations. These are typically brochures and white papers. It is possible that an attachment can contain a specially-crafted piece of malware that executes when the file is opened again in the right environment.

Potential damage

- Since we are running Linux, it is unlikely that our system can be damaged from malware that is hidden in attachments.

- We do allow innovation buyers and innovation sponsors to download attachment files, and we would effectively be distributing the malware to our clients. This can lead to reputational damage.

Defenses

New attachments to innovations are scanned for malware using *maldet*.

A daily update of malware signatures is updated to *maldet*.

Detection

Detection is automated. A notification email is sent to security@matchi.biz when an attachment with malware is found.

Recovery

The offending file is moved to a safe directory, from where it can either be manually cleansed or deleted and the file uploader can be asked to resubmit the attachment.