### **Security Incident Report**

**Title:** Apply Operating System (OS) Hardening Techniques

**Analyst:** jose Escamilla  
**Date:** 26/07/2024

#### **1. Identified Network Protocol**

One of the network protocols identified during the investigation is **HTTP (HyperText Transfer Protocol)**, used for transmitting web pages.

#### **2. Incident Documentation**

**Incident Summary:** The website YummyRecipesForMe.com, which sells recipes and cookbooks, was compromised by a disgruntled baker. The attacker executed a brute force attack to access the administrative account by using known default passwords. After gaining access, they modified the website's source code by embedding a malicious JavaScript script that prompted visitors to download an executable file to "update their browser." Upon executing the file, users were redirected to a fraudulent site, GreatRecipesForMe.com, where the company’s recipes were offered for free.

**DNS and HTTP Traffic Logs:**

**DNS Resolution for YummyRecipesForMe:**makefile  
Copiar código  
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)

14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)

**HTTP Request to YummyRecipesForMe:**wasm  
Copiar código  
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0

14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0

14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.] ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

**DNS Resolution for GreatRecipesForMe:**makefile  
Copiar código  
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)

**HTTP Request to GreatRecipesForMe:**wasm  
Copiar código  
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0

14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.] ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0

14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1

**Incident Details:**

* **DNS (Domain Name System):** Used for resolving domain names to IP addresses.
* **HTTP (HyperText Transfer Protocol):** Used for transmitting web pages.
* **TCP (Transmission Control Protocol):** Used to establish connections and ensure reliable data transmission.

The attacker exploited inadequate security policies, such as weak passwords and lack of mechanisms to prevent brute force attacks.

#### **3. Recommended Security Measure**

**Implement Strong Password Policies and Brute Force Attack Prevention Mechanisms:**

1. **Strong Password Policies:**
   * Require complex passwords that include a mix of uppercase letters, lowercase letters, numbers, and special characters.
   * Avoid using default or easily guessable passwords.
2. **Brute Force Attack Prevention Mechanisms:**
   * Implement an account lockout policy after a certain number of failed login attempts.
   * Use intrusion detection mechanisms to identify and block brute force attempts in real-time.
   * Consider implementing multi-factor authentication (MFA) to add an additional layer of security.
3. **Continuous Audits and Monitoring:**
   * Perform regular security audits to identify and rectify vulnerabilities.
   * Continuously monitor access logs and login attempts to detect suspicious activities.

#### **Conclusion**

Implementing strong password policies and mechanisms to prevent brute force attacks is crucial for protecting systems and data from unauthorized access and brute force attacks. These measures, along with continuous audits and monitoring, will significantly enhance the security of the website and protect user-sensitive information.

### **Informe de Incidente de Seguridad (spanish)**

**Título:** Aplica Técnicas de Reforzamiento del Sistema Operativo (SO)

**Investigador:** Jose Escamilla  
**Fecha:** 26/07/2024

#### **1. Protocolo de Red Identificado**

Uno de los protocolos de red identificado durante la investigación es **HTTP (HyperText Transfer Protocol)**, utilizado para la transmisión de páginas web.

#### **2. Documentación del Incidente**

**Resumen del Incidente:** El sitio web YummyRecipesForMe.com, que vende recetas y libros de cocina, fue comprometido por un panadero descontento. El atacante llevó a cabo un ataque de fuerza bruta para acceder a la cuenta administrativa mediante contraseñas predeterminadas conocidas. Tras obtener acceso, modificó el código fuente del sitio web, insertando un script de JavaScript malicioso que solicitaba a los visitantes que descargaran un archivo ejecutable para "actualizar su navegador". Al ejecutar el archivo, los usuarios eran redirigidos a un sitio web fraudulento, GreatRecipesForMe.com, donde las recetas se ofrecían gratuitamente.

**Registro de Tráfico DNS y HTTP:**

**Resolución DNS para YummyRecipesForMe:**makefile  
Copiar código  
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)

14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)

**Solicitud HTTP a YummyRecipesForMe:**wasm  
Copiar código  
14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0

14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0

14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [.] ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0

14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1

**Resolución DNS para GreatRecipesForMe:**makefile  
Copiar código  
14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)

**Solicitud HTTP a GreatRecipesForMe:**wasm  
Copiar código  
14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0

14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0

14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags [.] ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 0

14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1

**Detalles del Incidente:**

* **DNS (Domain Name System):** Se utilizó para resolver nombres de dominio a direcciones IP.
* **HTTP (HyperText Transfer Protocol):** Utilizado para la transmisión de páginas web.
* **TCP (Transmission Control Protocol):** Utilizado para establecer conexiones y asegurar la transmisión fiable de datos.

El atacante explotó la falta de políticas de seguridad adecuadas, como contraseñas fuertes y mecanismos para prevenir ataques de fuerza bruta.

#### **3. Medida de Seguridad Recomendada**

**Implementar Políticas de Contraseñas Fuertes y Mecanismos de Prevención de Ataques de Fuerza Bruta:**

1. **Políticas de Contraseñas Fuertes:**
   * Requerir contraseñas complejas que incluyan una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
   * Evitar el uso de contraseñas predeterminadas o fáciles de adivinar.
2. **Mecanismos de Prevención de Ataques de Fuerza Bruta:**
   * Implementar una política de bloqueo de cuentas después de un número determinado de intentos fallidos de inicio de sesión.
   * Utilizar mecanismos de detección de intrusiones para identificar y bloquear intentos de fuerza bruta en tiempo real.
   * Considerar la implementación de autenticación multifactor (MFA) para agregar una capa adicional de seguridad.
3. **Auditorías y Monitoreo Continuo:**
   * Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.
   * Monitorear continuamente los registros de acceso y los intentos de inicio de sesión para detectar actividades sospechosas.

#### **Conclusión:**

La implementación de políticas de contraseñas fuertes y mecanismos de prevención de ataques de fuerza bruta es crucial para proteger los sistemas y datos contra accesos no autorizados y ataques de fuerza bruta. Estas medidas, junto con auditorías y monitoreo continuo, mejorarán significativamente la seguridad del sitio web y la protección de la información sensible de los usuarios.