Modulo 1 – Unidad 1

Introducción sobre Ethical Hacking

Ejercicio Número 1 Unidad 1:

Seleccionar 1 técnica de ataque y hacer una breve descripción de la misma, por ejemplo, detallar de qué se trata la técnica de Phishing, no se pide realizar la técnica, únicamente explicar que entienden por la misma.

Subirlo en el foro de la unidad correspondiente por favor, exponer con capturas o pantallas.

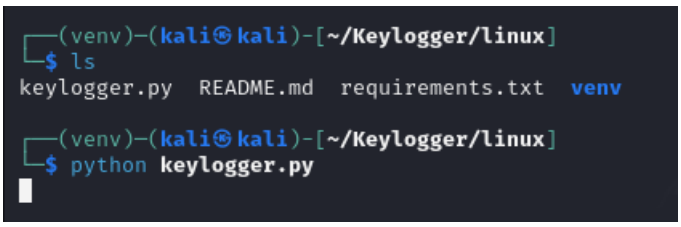
Técnica seleccionada: Keylogging.

El Keylogging es la captura de toda entrada de texto que se inserta desde un teclado a través de un software (Keylogger). Algunos Keyloggers pueden ser configurados para que realicen otras funciones además de la captura de la entrada de texto por teclado, como por ejemplo: Capturas de pantalla, envío de logs a direcciones de correo, etc.

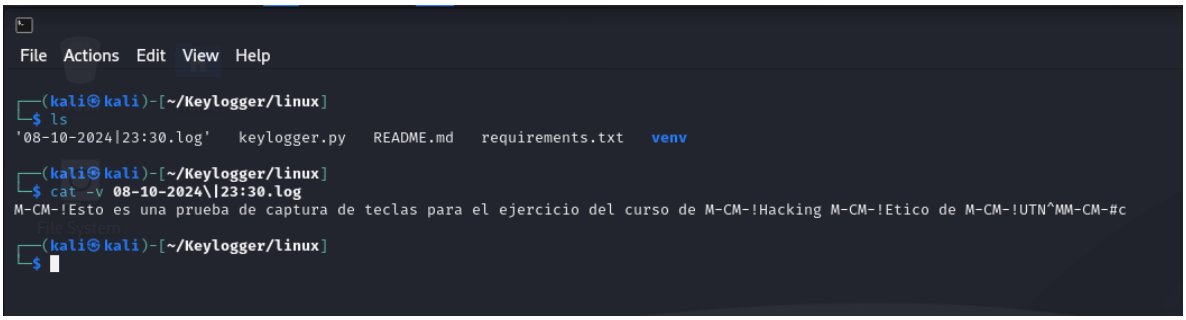
El uso más común es para controlar o espiar lo que hace una persona en su PC, o la obtención de datos sensibles como usuarios y contraseñas.

Voy a ilustrar el ejercicio con algunas capturas de pantalla de la utilización de PyKeyLogger en un entorno controlado:

Ejecución del KeyLogger:



Visualización del log obtenido:



Ejercicio Número 2 Unidad 1:

Buscar en Internet, un modelo de pentest o un informe de pentest realizado, exponerlo en el foro y en lo posible, dar su punto de vista de que es lo que se entiende.

Es un ejercicio de entendimiento, no es necesario ser específico con técnicas o tareas, la consigna se refiere más a la presentación del informe.

Procedo a exponer en capturas de pantalla un reporte de pentest realizado por la empresa “NCC Group Security Services” para el cliente “phpMyAdmin” expuesto públicamente en la fuente: https://pentestreports.com/reports/

1) En primer lugar tenemos una carátula, donde se muestran las partes implicadas, fecha y versión del reporte:

phpMyAdmin
Web Application Security Assessment

phpMyAdmin
May 18, 2016 – Version 1.2

Prepared for
Michal Čihař
Gervase Markham

Prepared by
Cara Marie
Valentin Leon

2) Tenemos un disclaimer / descargo de responsabilidad:

3) En el sumario ejecutivo resalto como información más relevante la fecha del testeo, la versión del software testeado, el objetivo de la necesidad del testeo:

This assessment was performed remotely by two NCC Group consultants, Cara Marie and Valentin Leon, over a period of two weeks from April 25th to May 6th. The assessment was conducted as a code-assisted penetration test of phpMyAdmin version 4.6.0 (current release as of this writing). phpMyAdmin provided access to key members of the development team and was committed to making this project a success.

El “Scope” o “alcance” (los sistemas, aplicaciones y redes que se someterán a pruebas, así como las metodologías y técnicas a utilizar):

Scope

NCC Group's evaluation included:

- Main application portal: This portal is a MySQL web administration tool. The interface supports user and database management, and a console for direct SQL statement and query execution.
- Setup portal: Provides an interface for phpMyAdmin application configuration, including security, import, export, and SQL query settings.
- Source code: While the focus of the assessment was not purely code review, NCC Group reviewed sections dealing with authentication, input validation, and command execution.

Test environments were created using the precompiled phpMyAdmin packages hosted on https://launchpad.net/~nijel/+archive/ubuntu/phpmyadmin.

Los “Key Findings” o hallazgos más importantes resultados del test:

Key Findings

The assessment uncovered several application flaws. Some of the more notable were:

- A lack of filtering on user CSV output that could allow an attacker to run arbitrary code on an administrator's computer.
- Improper cookie invalidation that could allow an attacker to unset internal global variables.

- Unauthenticated exposure of the Cross-Site Request Forgery (CSRF) protection token that could allow an attacker to perform various attacks against phpMyAdmin users.
- Several traffic flows that expose sensitive data or make use of plaintext HTTP communications. This could allow an attacker to man-in-the-middle, perform CSRF, or various other attacks against phpMyAdmin users.

Recomendaciones de seguridad luego del test:

Security Recommendations

In addition to the recommendations specified in each of the vulnerability details , implementing the following high-level recommendations will allow phpMyAdmin to gain a stronger security stance.

- Update phpMyAdmin to support modern security-related headers – HTTP Strict Transport Security and a stricter Content Security Policy. To enable a stricter Content Security Policies (CSP) (see Vulnerability 002), NCC Group recommends removing all legacy scripts inserted as inline JavaScript and move them to script files separate from the HTML source.
- Restrict all state changing actions to occur via HTTP POST. Allowing state changing requests to be sent via GET can leak sensitive data (see Vulnerability 001) and allow attackers to perform numerous attacks against phpMyAdmin. This violates security best practices.
- Provide users with hardening guides at install time and warn users about potential misconfigurations, to reduce the risk of insecure installations.
- Consider requiring installations to use TLS by default. If users have not already acquired certificates, then the installation process should direct them through the process for acquisition via Let's Encrypt.[2]
- Consider implementing an out-of-date software warning to aid users in maintaining up-to-date and secure phpMyAdmin instances.

Información detallada sobre las vulnerabilidades identificadas (descripción, como ejecutarla y recomendaciones de mitigación):

Vulnerability Details

nccgroup

Vulnerability	**CSV Export Allows Arbitrary Command Execution in CSV File**
Risk	**Medium** Impact: Medium, Exploitability: High
Identifier	NCC-1604_MOSS_phpMyAdmin-006
Category	Data Validation
Location	The CSV Export functionality[3]
Impact	A malicious user can change a database field so that when an administrator uses the Export functionality and opens the exported CSV in a spreadsheet editor such as Excel, code may be run on the administrator's computer. Alternatively, a malicious or compromised administrator can add or modify users with formulas in various fields to target other application administrators and users.
Description	The CSV Export functionality does not properly escape exported CSV field values. This can lead to code execution on a user's computer. This is done by including a formula in the CSV file that a spreadsheet editor similar to Excel will evaluate – the formula can include commands to be run on the user's computer. For example, if a user changes a database name or column value to be `=cmd|' /C calc'!A0` and the database is then exported in CSV format by another user, `calc.exe` will run when the file is evaluated by a spreadsheet editor. The victim user will be prompted with a warning, but since the user has downloaded the CSV from a trusted source, they are likely to allow the functionality. It should be noted that encapsulating the values with quotation marks (") does not mitigate the issue.
Reproduction Steps	1. Log into phpMyAdmin and insert `=cmd|' /C calc'!A0` into a database column value. 2. Export the database in CSV format. 3. Open the exported CSV file that was exported in Windows Excel and click through the warnings. 4. Observe the calculator application now running on the computer.
Recommendation	When performing a CSV Export, for any cell that starts with an `=`, `-`, `"`, `@`, or `+`, add a space to the beginning and remove any tab characters (`0x09`) in the cell. Alternatively, prepend each cell field with a single quote, so that their content will be read as text by the spreadsheet editor.

[3] https://github.com/phpmyadmin/phpmyadmin/blob/RELEASE_4_6_0/libraries/plugins/export/ExportCsv.php

El informe completo lo adjunto como comentario en el post de este ejercicio.

Rodrigo Vila.-