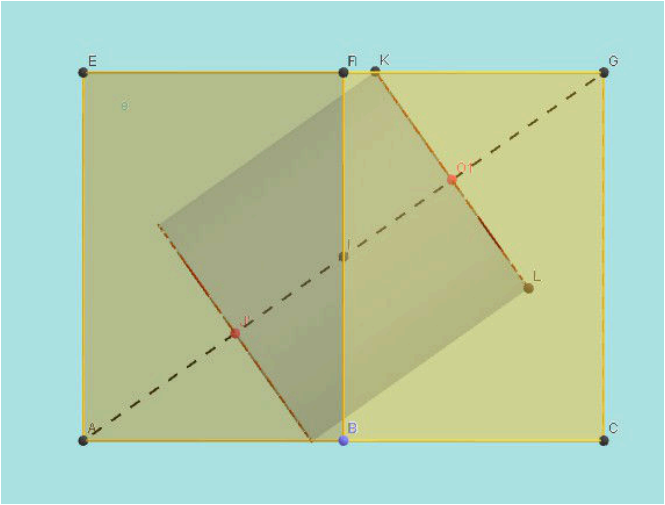

Рис 2: Діагональний переріз

Тепер розв'язання задачі зводиться до визначення радіуса основи циліндра із подібності трикутників GO1K та GEA.

Водночас, область застосування ілюстративних моделей обмежена. Вони допомагають краще зрозуміти визначення, формулювання теорем і задач. Але розвитку просторової уяви вони сприяють лише на першому етапі. Більш того, постійно постачаючи учня готовими, нехай дуже красивими і правильними малюнками, тим більше 3D-моделями, ми зрештою починаємо гальмувати подальше вдосконалення цієї навички, а деякі завдання взагалі майже втрачають сенс, якщо дати до них готовий малюнок.

Тестування на проникнення за допомогою open-source OS Linux і SHELL скриптів

Піскозуб А.З., Стефінко Я.Я., Банах Р.І.

Кафедра захисту інформації, НУ "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 1 , E-mail: azpiskozub@gmail.com , banakh.ri@gmail.com
Кафедра безпеки інформаційних технологій, НУ "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail: jarik.bit@gmail.com

This article discuss the security threats to computer networks and systems, and one of the ways to protect it - penetration testing. Most powerful thing for this purpose are OS LINUX and its shell scripts. We describe the methods and ways of implementation of these scripts to assist us in success pentest. We have been analyzing the current free software for pentest and demonstrating examples for using

special bash script of OS Kali Linux.

Вступ

Технологія тестування на проникнення сьогодні рясніє спрощеними графічними інтерфейсами для користувача. Незважаючи на простоту у використанні, вони часто пропонують дуже мало контролю над операціями і не пропонують дуже інформативний досвід для своїх користувачів. Ще одним недоліком є те, що багато з цих рішень оцінки безпеки розроблені тільки для ідентифікації та автоматизації експлуатації у найбільш очевидних і традиційних випадках вразливостей. Для будь-якого іншого практичного прикладу уразливості, пентестеру потрібно покладатися на свої власні сценарії та інструменти оцінки.

Основний набір навичок хорошого пентестера проникнення включає, щонайменше, елементарні навички в сценаріїв або мов програмування, таких як Баш сценаріїв, Python, Ruby, Perl і так далі. Це пояснюється тим, що вони можуть впоратися з особливими і винятковими екземпляри вразливостей з їх власними персоналізованими засобами і здатні до автоматизації тестування безпеки відповідно до їх власної точки зору. [3]

Тестування на проникнення і shell скрипти

Тест на проникнення (пентест) дозволяє моделювати несанкціонований доступ в інформаційні системи, а також інші дії, які дозволяють порушити нормальне функціонування систем і бізнес-процесів. По суті, це метод оцінки захищеності інформаційних систем та/або інформації, та об'єктів, де вона зберігається або обробляється від несанкціонованого використання [1].

Bourne Again Shell (Bash) є, можливо, одним з найважливіших частин програмне забезпечення за історію існування розробки ПЗ. Без багатьох утиліт оболонки Bash і потенціалом, що дається користувачам шляхом об'єднання і взаємодії системних утиліт в програмований спосіб (так звані Bash сценаріїв чи скрипти), багато з важливих проблем безпеки в сучасному світі було б дуже накладно вирішити[3]. Утиліти, такі як Grep, Wget, VI, і AWK дозволяють своїм користувачам робити дуже потужну обробку рядків, видобуток даних і управління інформацією. Системні адміністратори, розробники, інженери безпеки, тестери на проникнення по всьому світу протягом багатьох років покладаються на цей потенціал вирішення проблем і ефективність у забезпеченні їм вирішувати їхні щоденні технічні проблеми.

Принципово оболонка bash є найбільш стандартизованою, і, як правило, відносно найбільш популярних операційних систем, реалізованих з одного одного джерела – офіційного відкритого вихідного коду. Це означає, що можна гарантувати певний базовий набір поведінки для bash скриптів або набору команд незалежно від операційної системи і реалізації башу.

Загальна культура і конвенцій Linux / Unix часто буває важко оцінити для початківців і, можливо, через відсутність підказок, натяків, і багатого

графічний дизайну взаємодії та користувальницької привабливості ззовні.

Середовище bash буде представлене тут на прикладі спеціалізованої операційної системи, Kali Linux. Калі це дистрибутив взятий з Debian, і він упакований з утилітами, орієнтованих виключно на вирішення технічних проблем безпеки і тестування на проникнення.

II. Bash shell як універсальне вирішення задач пентесту

Наведемо приклади найбільш корисних команд bash для ефективного виконання ваших подальших технічних задач в Kali Linux. По-перше, для навігації по системі чи файлах ми використовуємо cd, pwd, ls, find , man, grep. Перенаправлення вводу-виводу(I/O) дозволяє насправді в 80% побачити всі результати роботи скриптів і краще зрозуміти процеси. Наприклад, ви можете шукати через вивід від Nmap або TCPdump або кейлоггерів шляхом подачі її output в інший файл або програму для аналізу. Для пере направлення виводу потрібно тільки додати в кінці команди символ > , а для введення з файлу чи програми , навпаки < . Для аналогічних цілей обміну виведенням між процесами використовують pipe, тобто | . Також в Linux доступна можливість кастомізувати для себе bash, а саме підлаштувати консоль під свої особисті вимоги(колір, шрифт тощо).[4]

Також ми покажемо як використовувати утиліти , такі як Nmap, Whois, Dig, та інші мережеві «Swiss Army» ножі, щоб вивчити стан безпеки на конкретних хостах чи в певних локальних мережах.

Whois servers містять інформацію про IP адреси, доменні назви та іншу відповідну інформацію про певні організації, якими ми можемо бути зацікавлені в ході пентесту. За допомогою команди dig, ми можемо отримати всю можливу інформацію про певний домен чи IP адресу з всесвітньої павутини. Для більш конкретної інформації також часто використовують dnsmap і dnsenum.

Для оглядання і окреслення цільового хоста ми будемо використовувати Network mapper (Nmap) та Arping. Nmap став де-факто стандартом для мережевої оцінки , і може робити значно більше ніж Hping, Fping, and Arping. В різних випадках, часто для оцінки між мережевих екранів, пентестери потребують більш налаштовувані менеджери мережевих пакетів у різних протоколах мережевого рівня. Саме тут і пригодяться Hping, Fping, and Arping.

Ось приклад ICMP сканування з Nmap:

```
nmap -sn -v --reason 192.168.10.0/24
```

Metasploit це очевидно найбільш використовувана платформа для тестування на проникнення та розробки експлойтів. Ця утиліта необхідна і достатня для тестування, пошуку і розробки експлойтів для вразливостей ОС чи додатків. Основним середовищем виконання для Metasploit є утиліта bash – msfcli [5]:

```
msfcli [MODULE] [OPTIONS] [MODE]
[MODULE] := [exploit/* | auxiliary/* | payload/* | post/* ]
```

```
[OPTION] := [ [option_name] = [value] <space> ]*
[MODE] := [A | AC | C | E | H | I | O | P | S | T ]
```

Linux і bash скрипти дозволяють нам дуже вдало комбінувати деякі команди,щоб отримати дуже зручний вивід даних з застосуванням до них, одразу ж, певних можливостей Metasploit.Для прикладу,використаємо MSFcli, Nmap та awk [3]:

```
for ip in `nmap -v -T5 -p[PORT] [HOST] | awk -F\ '/[PORT]\/[tcp|udp]
on/ { print $6 }'`; do msfcli [MODULE] RHOST=$ip E; done
```

Також до пакету утиліт Metasploit входять msfconsole, msfpayload, meterpreter тощо. Важливими утилітами bash на етапі експлуатації в процесі пентесту є також arpspoof, macchanger, tcpdump, ettercap, sslyze, w3af, arachni, sqlmap, john-the-ripper і smtpwalk.

Висновки

В теперішніх умовах, ми бачимо, як щоденно виявляються нові вразливості у всесвітньо відомих і широко використовуваних протоколах і системах (Bash shellshock, SSL heartbleed etc.). Отож зараз bash та скриптинг взагалі є ключовими інструментами для здійснення ефективних тестів на проникнення та для виявлення нових вразливостей, адже вони дозволяють заглибитись в найдрібніші деталі певних протоколів.

Література

[1]Піскозуб А.З. Використання тестування на проникнення в комп'ютерні мережі та системи для підняття їх рівня захищеності // Матеріали третьої міжнародної науково-практичної конференції FOSS Lviv 2013,. – Львів,2013.
[2] D.Kennedy, J.O'Gorman. Metasploit.The penetration tester's guide. - No starch press, San Francisco, 2011. 332c.
[3] Keith Makan .Penetration Testing with the Bash shell. Birmingham – Mumbai,Packt Publishing,2014,151c.
[4] Jason Andress, Ryan Linn. Coding for Penetration Testers.London,Elsiever,2012,321c.
[5] Kali Linux. https://kali.org

Ansible - IT automation engine for configuration management and cloud provisiong

M. Salo

UK2 Limited t/a VPS.NET michael.salo@uk2group.com

Automatic provisioning of infrastructure as well as deployment is a cornerstone of DevOps. It brings the benefits of version control, reproducibility, and a central place to consolidate (executable) knowledge about infrastructure setups. Best known provisioning systems are Chef and Puppet. A newcomer to this game is Ansible with goal are foremost those of simplicity and maximum ease of use and with strong focus on security and reliability, featuring a minimum of moving parts.

Ansible is an radically simple IT automation engine was that released in 2012