```
[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

by Michael DeHaan, a developer who has been working with configuration management and infrastructure orchestration in one form or another for many years. He has worked with Puppet, Chef, Cfengine, server deployment (Capistrano, Fabric,) and ad-hoc task execution (Func, plain SSH), and wanted to see if there was a better way. Ansible wraps up all three of these features into one tool, and does it in a way that's actually simpler and more consistent than any of the other task-specific tools.

Ansible is a automation and provisioning tool that makes it easy to configure systems with the needed software, configuration options and even content. It is a command line tool, written in Python, that uses SSH connections to run these actions. This means that all you need to do is have a SSH connection to a machine and Ansible will run any actions you want to run.

Using Ansible it's easy to deploy — and most importantly, it uses a very simple language (YAML, in the form of Ansible Playbooks) that allow you to describe your automation jobs in a way that approaches plain English.

Cfengine, Chef and Puppet are fantastic and can be used to manage extremely large infrastructures but there is no denying that they have a large learning curve and can be difficult to setup and configure. Ansible aims to be simpler and easier to understand while still maintaining the efficiency and power of others tools.

References:

- Jeff Geerling , 2014, "Ansible for DevOps "
- http://docs.ansible.com/

Програмне забезпечення IT-компанії

Скоропад О.

Компанія EPAM, sko@ukr.net

Software development company is a factory for the production of IT products. Like any factory, this company has complex structure and big set of processes with a lot of the necessary tools. All these tools are special applications for software development. This article describes a simple software landscape of modern IT company and explains major functionality of components. Particular attention is paid to free software.

Сучасна IT компанія – це фабрика з випуску програмних продуктів. Як і кожна фабрика, така компанія має свою структуру та налагоджений складний виробничий процес з великою кількістю необхідних інструментів. В ролі інструментів виступають програмні продукти призначені для розробки на всіх його етапах програмного забезпечення, а оскільки таких етапів є багато, то і перелік продуктів є дуже широким.

Спробуємо класифікувати програмне забезпечення для розробки:

1. Інструменти програмної архітектури та аналітики призначені для візуалізації ідеї програмного проекту та візуалізації блок-схеми та основних