FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Banners & Scripts

Agenda

- Review of Lab Activities
- Banner Grabbing
- Scripting
- Metasploitable2
- Lab 07 details

Lab Review

Backdoor Connections

One way to connect to the backdoor is from the attacking system

- Set up a netcat server on the target VM, listening for an incoming connection on port 1234
  - What options let you know it is a server instance you are setting up?
- This allowed us to connect at will, but it also lets anyone else connect
- Seen by vulnerability scanners

Backdoor Connections

Another way is to modify your registry entry so the target machine will phone home to a netcat server listening on Kali

- This is a more realistic use of netcat as a backdoor
- It won’t be seen by vulnerability scanners
- It will only attempt to connect to the Kali machine
- You aren’t leaving a hole in the defenses of the target machine that others could connect to
  - Very bad in a production environment
  - Hackers don’t stop trying to get in when you are doing a pentest

msfvenom

- msfvenom replaced msfpayload and msfencode
  - The functionality of both msfpayload and msfencode have been combined into a single tool
- msfvenom still has the same two primary functions
  - Creating a payload
    - Generating the executable binary from the payload
  - Encoding the payload
    - Changing the binary structure of the payload to avoid detection by antivirus programs

msfvenom Options

Some of the most commonly used options:

- **l** used to generate a list of payloads, encoders, etc.

- **p** specifies the payload to use

- **e** specifies the encoder to use

- **b** allows you to specify bad characters to avoid (\x00)

  – \x00 represents a null byte

- **a** specifies the architecture (x86, x64, etc.)

-- **platform** specifies the target platform

-- **payload-options** lists the payloads options

- **f** specifies the output format

-- **help-formats** lists the possible formats

Banner Grabbing

Banner Grabbing

- Can be used by system administrators to obtain information about their networks
  - Inventory
  - Open ports
  - Running services
  - Network services

Banner Grabbing

- Can be used by attackers to obtain the same information as administrators
- In addition to what is up and running, the version of these services is important
  - Is it vulnerable?
  - Are there exploits currently available?

Banner Grabbing

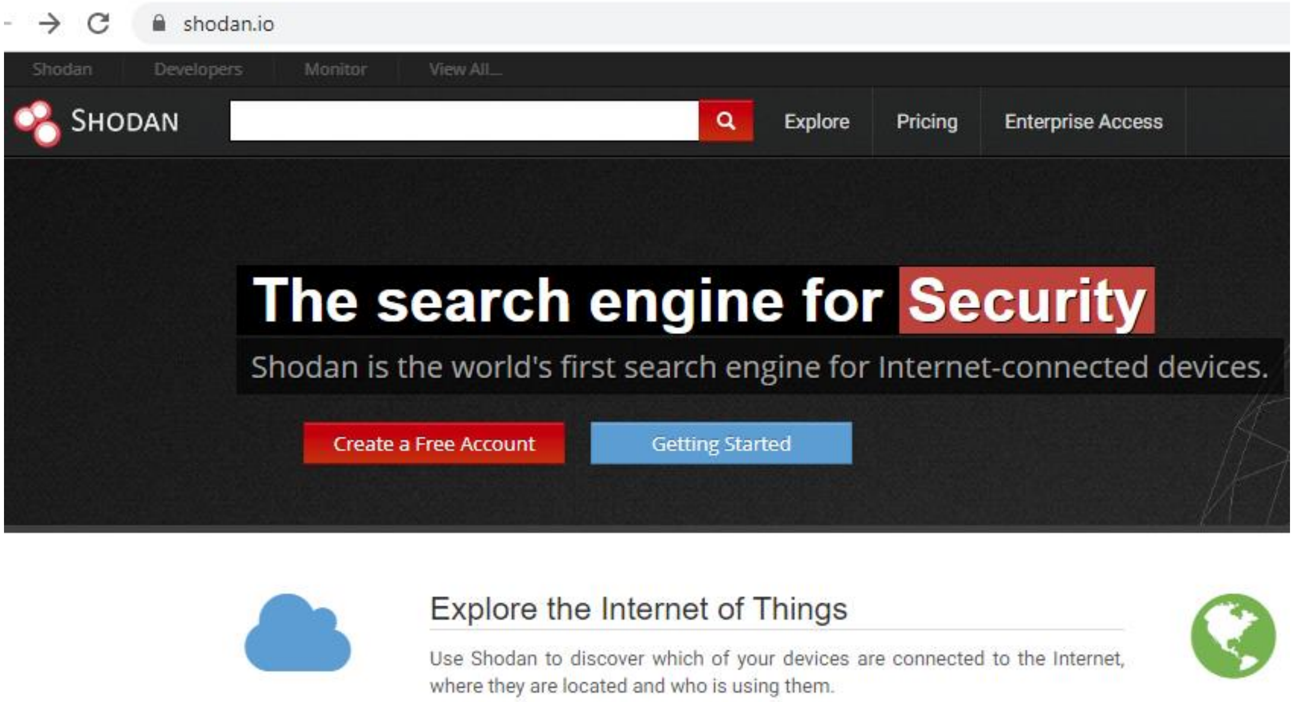
- Common services used for banner grabbing include:
  - FTP
  - SMTP
  - HTTP
  - Remote Execution Protocol
  - Etc.
- These are referred to as ‘r’ services

Banner Grabbing

- We create our own scripts using Bash and Python, but there are other commonly available tools
  - Netcat
  - Nmap
  - Telnet
  - zmap
- Most come pre-installed on Kali Linux

Shodan

- Shodan is a commercial tool that scans for services running on machines connected to the internet



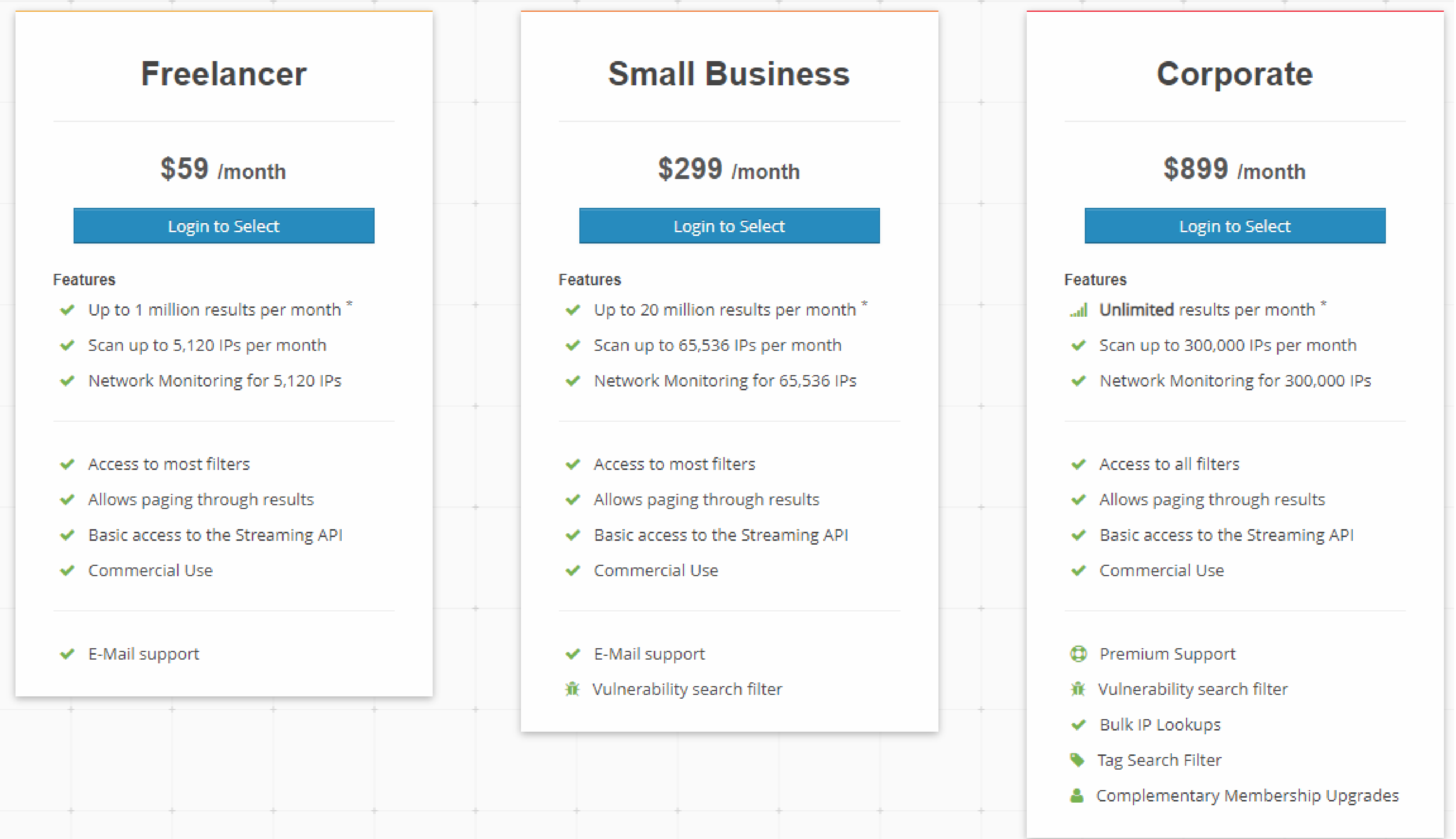
The search engine for Security

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Shodan Pricing



Freelancer

$59 /month

Login to Select

Features

- ✓ Up to 1 million results per month *
- ✓ Scan up to 5,120 IPs per month
- ✓ Network Monitoring for 5,120 IPs

- ✓ Access to most filters
- ✓ Allows paging through results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- ✓ E-Mail support

Small Business

$299 /month

Login to Select

Features

- ✓ Up to 20 million results per month *
- ✓ Scan up to 65,536 IPs per month
- ✓ Network Monitoring for 65,536 IPs

- ✓ Access to most filters
- ✓ Allows paging through results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- ✓ E-Mail support
- Vulnerability search filter

Corporate

$899 /month

Login to Select

Features

- **Unlimited** results per month *
- ✓ Scan up to 300,000 IPs per month
- ✓ Network Monitoring for 300,000 IPs

- ✓ Access to all filters
- ✓ Allows paging through results
- ✓ Basic access to the Streaming API
- ✓ Commercial Use

- Premium Support
- Vulnerability search filter
- ✓ Bulk IP Lookups
- Tag Search Filter
- Complementary Membership Upgrades

Bash Scripting

Bash Scripting

- At their simplest from, they allow you to run several terminal commands one after another
  - The commands are specified in a file
  - You need to make the file executable to run it
- Allows you to create useful scripts to perform common tasks
- Automates simple tasks to save time
- It is good practice to specify the shell you want the terminal to run the script in
  - #!/bin/bash

Bash Scripting

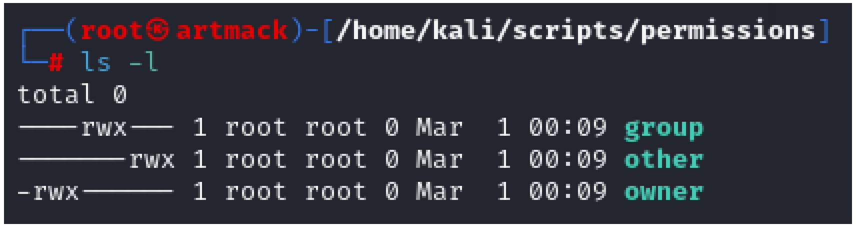
We discussed that a bash script basically takes commands you would normally run in the terminal and automates them

- A good thing about automating scripts is that you can time them
- On Linux operating systems you can use cron jobs to schedule a time when a script will run
  - Windows equivalent to Task Scheduler

Bash Scripting

A Bash script can have permissions set to it just like any other file in Linux

- RWX
  - Read
  - Write
  - Execute
- This means you can control who has access to the script and what type of privileges they have



```
┌──(root㉿artmack)-[/home/kali/scripts/permissions]
└─# ls -l
total 0
----rwx--- 1 root root 0 Mar  1 00:09 group
-------rwx 1 root root 0 Mar  1 00:09 other
-rwx------ 1 root root 0 Mar  1 00:09 owner
```

Bash Scripting

- A Bash script essentially a text file so commands will need to be placed in the same order in which they would normally run in a terminal window
- In addition to this, it supports variables, conditional statements, loops, and functions

Bash Scripting

- **Bash** (Bourne again shell) replaced **sh** (Bourne shell)
- When executing a Bash script inside a shell, remember that the script itself is $0 and any further arguments are $1, $2, $3, etc.

Bash Scripting

- When you create a Bash script, keep in mind the arguments being passed…
- You can modify a bash script to accept arguments
  - ./Banners.sh 10.0.0.60
  - Wherever $1 occurs in the script, it will be replaced with 10.0.0.60
    - This helps avoid the need to edit the script every time the IP of a target changes

Bash Scripting

- Redirecting stdout and stderr to the same location
  - We wanted all the output that would normally be sent to the screen to get redirected to our file for logging purposes
  - The &> redirection operator sends both stdout and stderr to the same location
    - 2>&1 and >& are supported by some shells
  - You could individually control where stdout and stderr go
    - > on its own redirects stdout
    - 2> on its own redirects stderr

Bash Scripting

- A Bash script essentially a text file so commands will need to be placed in the same order in which they would normally run in a terminal window
- In addition to this, it supports variables, conditional statements, loops, and functions

Python Scripting

Python Scripting

- Python is widely used in the security field
- Just like Bash, it can be used to run a series of commands and be executed from a shell
- Doesn’t require to be compiled prior to execution and is interpreted on run time
  - Converted to machine language

Python Scripting

Python is popular with developers since it has simpler syntax than other programming languages and it easily integrated into web applications

Attackers like using Python because of the same reasons

- Easier to learn
- Easier to write exploits with

Python Scripting

Vast number of libraries, modules, and frameworks available

- Makes it easy to develop complex cybersecurity tools and applications quickly
- Libraries provide various functionalities, including network analysis, cryptography, penetration testing, and vulnerability scanning

Python Scripting

Cross-platform

- It can run on different operating systems, including Windows, macOS, and Linux

Scalable

- Can handle large-scale projects
- Can integrate with other languages and technologies, such as C/C++, Java, and more

Python Scripting

Has the ability to do things like socket programming

- Connect to remote machines and parse the results

The best part is that it’s free!

- Python is an open-source programming language which has led to a vast community of developers who contribute

Metasploitable2

Metasploitable2

- Intentionally vulnerable version of Ubuntu
- Designed as a testing platform for hacking tools and to demonstrate common vulnerabilities
- Compatible with VMWare, VirtualBox and a variety of other virtualization platforms
- Comes with a wide variety of services up and running in a misconfigured state
  - We got a sense of the number of open ports when we did our scans

Metasploitable2

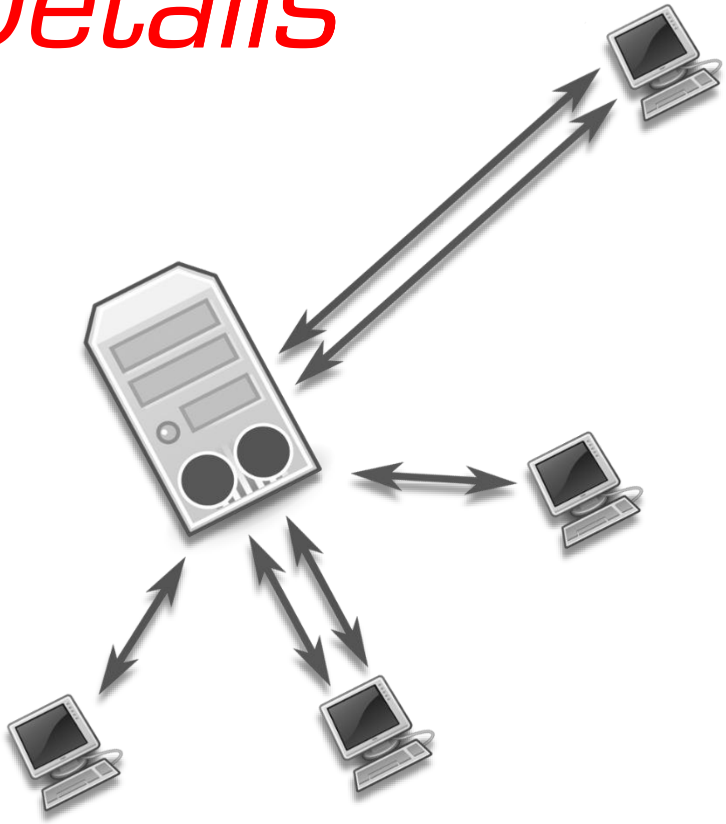
- Most of the open ports can be used as a remote entry point to the system
- Ports 512, 513 and 514 (the "r" services) have been misconfigured to allow remote access from any hosts
- The NFS service is configured to allow direct probing via portmapper, and showmount
- Comes with services such as vsftpd and UnrealIRCD that both shipped with a backdoors

Metasploitable2

- Weak Passwords on both the system and many of the services
  - These are common problems that administrators don’t fix
- Mutillidae for practicing Web Application Vulnerabilities
- Damn Vulnerable Web Application for similar testing (dvwa)
- TWiki web based collaboration platform
- Many More Vulnerabilities

FANSHAWE

Lab 07 Details



Lab 07

- Banner Grabbing
- Python scripting
  - LAN scan
  - Socket programming
- Exploiting Metasploitable2