

Building the Automation Sandbox



Gus Khawaja

Gus.Khawaja@guskhawaja.me www.ethicalhackingblog.com



Module Overview

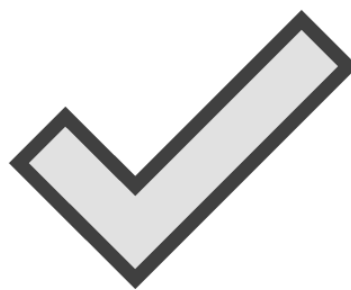


Typical PenTest Workflow

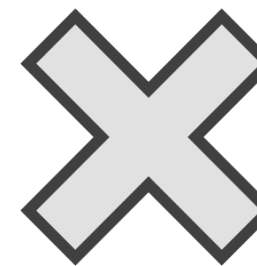


Terminal

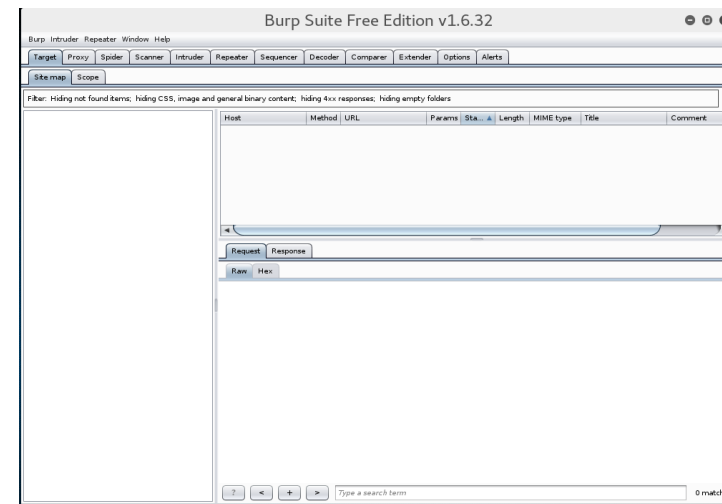
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping webserver.home.lan  
PING webserver.home.lan (10.0.0.101) 56(84) bytes of data:  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=1  
ttl=128 time=1.54 ms  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=2  
ttl=128 time=1.22 ms  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=3  
ttl=128 time=0.940 ms  
^C  
--- webserver.home.lan ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 0.940/1.237/1.545/0.247 ms  
root@kali:~#
```



Web browser



GUI



Our Application

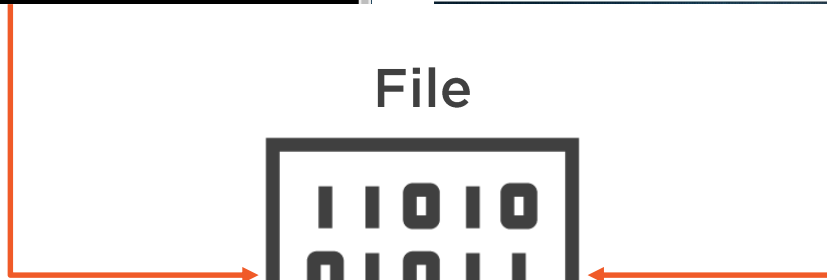
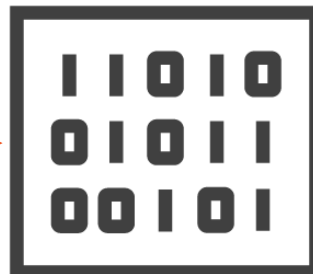
Terminal

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping webserver.home.lan  
PING webserver.home.lan (10.0.0.101) 56(84) bytes of data  
.  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=1  
ttl=128 time=1.54 ms  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=2  
ttl=128 time=1.22 ms  
64 bytes from webserver.home.lan (10.0.0.101): icmp_seq=3  
ttl=128 time=0.940 ms  
^C  
--- webserver.home.lan ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 0.940/1.237/1.545/0.247 ms  
root@kali:~# █
```

Web browser




File




GitHub

GusKhawaja/pat: Penteste... X +

https://github.com/GusKhawaja/pat Search

 This repository Search

Pull requests Issues Gist

+ - 

GusKhawaja / pat

Unwatch 1 Star 0 Fork 0

Code

Issues 0

Pull requests 0

Wiki

Pulse


Graphs

Settings

Pentester Automation Tool <http://www.ethicalhackingblog.com> — Edit

4 commits 1 branch 0 releases 1 contributor

Branch: master New pull request New file Upload files Find file HTTPS https://github.com/GusKhawaja/pat Download ZIP

 GusKhawaja Creating the version Latest commit 2e081a9 15 hours ago


README.md Update README.md 15 hours ago

pat.py Creating the version 15 hours ago

README.md

pat v0.1

This application will be the next generation for automating penetration testing tasks. The work is in progress.



Executing Commands from the Terminal



Opening the Browser



Saving the Results



Putting It All Together



Summary



Building the automation application infrastructure

Overview

- Built the terminal automation
- Built the open browser automation
- Saving the results
- Refactoring (pat.py)