



UNIVERSITA' DEGLI STUDI DI
NAPOLI FEDERICO II

Scuola Politecnica e delle Scienze di Base
Corso di Laurea in Ingegneria Informatica

Elaborato di Network Security

Honeypots in ambiente DSP

Anno Accademico 2022/2023

Professore
Simon Pietro Romano

Studenti
Francesco Gianpio Palmieri M63001297
Daniele Marfella M63001365

Indice

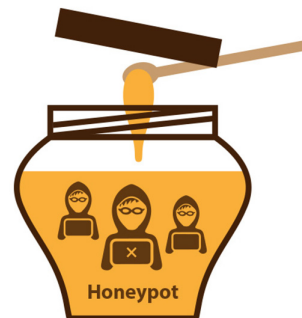
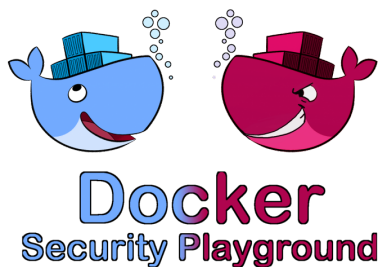
1	Sommario	2
2	Introduzione	3
2.1	Introduzione alle honeypot	3
2.2	Tassonomia	4
2.3	Deployment	5
2.4	Vantaggi e svantaggi	6
2.5	Honeypot data analysis	7
3	Laboratorio DSP	9
3.1	Honeypot utilizzati	9
3.1.1	Dionaea	9
3.1.2	Cowrie	9
3.2	Configurazione laboratorio	11
3.3	Scenari di attacco	14
3.3.1	Scenario 1: attaccante "ingenuo" e honeypot a bassa interazione	15
3.3.2	Scenario 2: attaccante poco "ingenuo" e honeypot a media interazione	17
3.3.3	Scenario 3: attaccante medio e honeypot ad alta interazione	20
4	Conclusioni	22
	Bibliografia	23

Capitolo 1

Sommario

In questo elaborato svolto per l'esame di Network Security, approfondiamo l'argomento relativo alle honeypots e a diversi scenari a cui possono essere coinvolti. Il contributo dell'elaborato può essere suddiviso in due paragrafi: nella prima parte si ha un approfondimento teorico che introduce l'argomento e ne descrive le caratteristiche fondamentali, dopodiché si ha una parte più pratica con la creazione di un semplice laboratorio su Docker Security Playground in cui vengono mostrati i diversi scenari.

Lo scopo finale risulta essere quindi quello di approfondire in che modo l'attaccante cade "in tentazione" delle honeypots, e, di utilizzare le funzionalità di questi ultimi per ottenerne il tracciamento delle attività svolte.



Capitolo 2

Introduzione

2.1 Introduzione alle honeypot

Una honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici. Solitamente consiste in un computer o un sito che sembra essere parte della rete e contenere informazioni preziose, ma che in realtà è ben isolato e non ha contenuti sensibili o critici; potrebbe anche essere un file, un record, o un indirizzo IP non utilizzato [1] (in questo caso si parla di honey tokens).

Le honeypot sono in grado di individuare gli attacchi zero-day e di fornire informazioni sulle azioni e sulle motivazioni degli attaccanti. L'obiettivo principale di una honeypot è quello di distrarre gli aggressori dal loro obiettivo reale e allo stesso tempo raccogliere informazioni su di essi e sugli schemi di attacco [5].

L'utilizzo di honeypot semplifica il rilevamento degli attacchi in quanto esse non sono interessate dal traffico di produzione. Tipicamente una honeypot non è accessibile mediante i canali classici, ma solo in seguito a una scansione che ne rivela la presenza. Per questo tutte le connessioni verso le honeypot sono considerate malevole. Inoltre, tali meccanismi consentono anche di migliorare la risposta agli attacchi, permettendo di studiarne i vari aspetti e ideare, così, delle contromisure adeguate.

2.2 Tassonomia

Esistono diverse tipologie di honeypot; in genere esse vengono classificate in base a tre criteri: campo di applicazione, livello di interazione, direzione dell'interazione.

Per quanto riguarda il campo di applicazione si distingue tra production honeypot e research honeypot. Le honeypots di produzione sono quelle tipicamente utilizzate nelle reti aziendali; sono caratterizzate da facilità di implementazione e di utilizzo, ma le informazioni raccolte sugli attaccanti e sulle tipologie di attacco sono limitate. Al contrario, le honeypots di ricerca forniscono informazioni complete sugli attacchi, ma sono più difficili da implementare. Di solito sono utilizzate da organizzazioni di ricerca per analizzare gli attacchi e sviluppare contromisure generali contro le minacce. Le honeypot di ricerca aiutano a comprendere le motivazioni, il comportamento, gli strumenti e l'organizzazione dei black-hats, permettendo di definire un profilo di attacco abbastanza dettagliato.

Per quanto riguarda il livello di interazione, si hanno tre categorie principali:

- **Low-interaction honeypots (LIHP):** simulano solo una piccola serie di servizi (come SSH o FTP) e non forniscono all'attaccante alcun accesso al sistema operativo. La raccolta di informazioni è limitata, per questo tale tipologia di honeypots viene utilizzata principalmente per la valutazione statistica. Le LIHP tendono a essere honeypots di produzione.
- **Medium-interaction honeypots (MIHP):** emulano più servizi rispetto alle LIHP, ma non forniscono ancora nessuna funzionalità del sistema operativo.
- **High-interaction honeypots (HIHP):** sono le più sofisticate. Sono le più complesse in quanto forniscono all'attaccante un sistema operativo vero e proprio che non è limitato. Gli HIHP raccolgono la maggior quantità possibile di informazioni, tra cui i log completi degli attacchi, l'accesso ai dati, l'attraversamento di alberi di file, codici byte eseguiti, ecc. Ciò comporta una maggiore complessità dell'analisi. Gli HIHP tendono a essere honeypots di ricerca.

Infine, considerando la direzione in cui avviene l'interazione si distingue tra server honeypot e client honeypot. Le honeypots lato server aspettano che siano gli aggressori a iniziare la comunicazione, mentre le honeypots lato client cercano attivamente potenziali entità dannose e richiedono una interazione. Un'ulteriore classificazione potrebbe essere fatta sulla fisicità delle honeypot, distin-

guendo tra physical honeypots (macchina reale presente nella rete) e virtual honeypots (macchina simulata) [5].

Criterio	Tipologie
Campo di applicazione	Production, Research
Livello di interazione	Low, Medium, High
Direzione dell'interazione	Client, Server
Fisicità	Reale, Virtuale

2.3 Deployment

Una honeypot può essere posizionata in vari punti all'interno della rete di un'organizzazione, in base allo scopo che si vuole raggiungere. Possono essere dislocate anche più honeypot all'interno della stessa rete; in questo caso si parla di honeynet. Tipicamente, la rete di un'organizzazione è suddivisa in tre aree: una parte esterna; una zona demilitarizzata in cui sono disposti i server che devono essere accessibili dall'esterno; una LAN interna a cui possono accedere solo coloro che appartengono all'organizzazione. Una honeypot può essere installata in tutte e tre le aree descritte e in base a tale scelta raccoglierà dati di un certo tipo. Per questo è importante definire l'obiettivo da raggiungere prima di compiere la scelta sulla tipologia di honeypot e sulla sua posizione all'interno della rete.

Ad esempio, una honeypot a bassa interazione può servire come un sensore di rilevamento delle intrusioni se posizionata dietro il perimetro difensivo dell'organizzazione (zona demilitarizzata). Quando sono collocate al di fuori del firewall dell'organizzazione, le honeypots a bassa interazione sono utili per catturare dati statistici sulla frequenza, il volume, il tipo e l'origine dei tentativi di attacco [4].

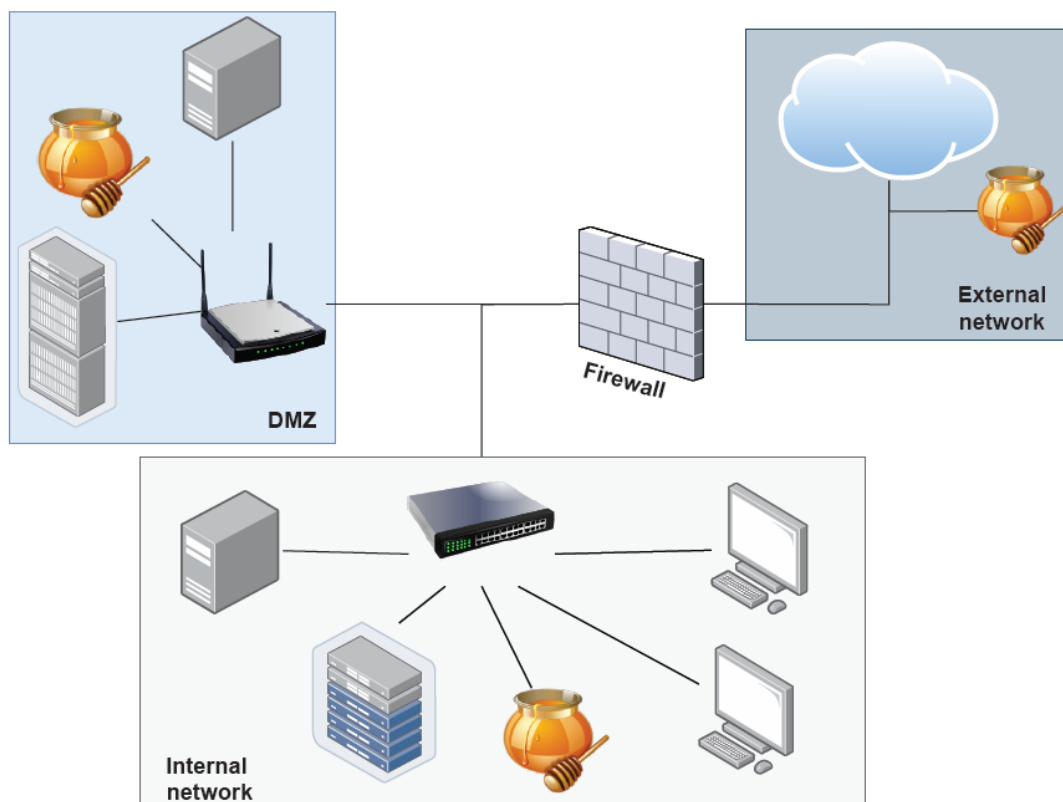


Figura 2.1: Immagine tratta da [2]

2.4 Vantaggi e svantaggi

Esaminiamo qui i vantaggi e gli svantaggi derivanti dall'utilizzo di honeypot. Tra i vantaggi si ha:

- Raccolta di dati preziosi che non sono contaminati dal traffico benigno e quindi sono di dimensioni ridotte e più facili da gestire e analizzare.
- Sono indipendenti dal carico di lavoro dei sistemi di produzione.
- Permette di catturare attacchi zero-day.
- Riduzione dei falsi positivi, ovvero di dati che si pensano malevoli ma in realtà non lo sono (questo è un problema molto ricorrente negli Intrusion Detection Systems).
- Flessibili, ovvero possono essere adattati a diversi ambienti.

Per quanto riguarda gli svantaggi:

- Le honeypot lato server sono inutili se nessuno le attacca.
- Le honeypot a bassa interazione emulano dei servizi e non li implementano veramente; da ciò scaturisce che il comportamento di tali emulazioni può essere diverso dal protocollo reale e questo potrebbe rivelare all'attaccante la vera natura di quel sistema.
- Se le honeypot vengono bucate, possono essere sfruttate dall'attaccante per condurre un attacco verso altri nodi della rete dell'organizzazione target. In questo caso più alto è il livello di interazione più alto sarà il rischio. Per compromettere il computer host, l'aggressore dovrebbe accorgersi della presenza dell'honeypot e prendere di mira il sistema operativo dell'host o vulnerabilità impreviste nell'implementazione dei sistemi e dei servizi emulati.

2.5 Honeypot data analysis

I dati registrati da una honeypot sono fondamentali e permettono di creare quello che è un profilo di attacco, ovvero un insieme di informazioni che ci permettono di capire elementi quali:

Motivazione: descrive la ragione dell'attacco. Spesso può essere solo indovinata. Tipiche motivazioni di un attacco sono il guadagno, la notorietà o la vendetta.

Ampiezza/profondità: l'ampiezza è descritta dal numero di macchine colpite; la profondità dal grado in cui è stato analizzato un bersaglio specifico.

Sofisticazione: descrive il livello di competenza necessaria per eseguire un attacco specifico. All'estremo inferiore di questa scala si trovano gli attacchi che utilizzano software o exploit che sono pubblicamente disponibili di cui l'attaccante ha una scarsa conoscenza di come funzionano realmente; all'estremo superiore ci sono attacchi che mostrano un certo livello di competenza nello sviluppo o modifica di strumenti personalizzati per gli attacchi.

Occultamento: misura la capacità di nascondere le prove dell'attacco.

Fonte e causa principale dell'attacco: occorre, per quanto possibile, identificare l'attaccante e capire da dove ha avuto origine l'attacco (ad esempio da un worm). L'individuo, il gruppo o il malware dietro l'attacco meritano un profilo a sé stante, che descriva tutte le caratteristiche che si possono ricavare dall'attacco. Indirizzi e-mail, soprannomi, frasi comuni, o il confronto tra le

tecniche di diversi attacchi può aiutare a identificare gli aggressori, o almeno identificare un gruppo di attacchi come provenienti da una fonte comune.

Vulnerabilità: individuare la falla nel sistema che ha permesso l'attacco.

Tools: capire quali strumenti sono stati utilizzati per eseguire l'attacco.

Le informazioni fornite dalle honeypots sono preziose, ma non sono immediatamente utili senza un'attenta analisi da parte di persone esperte nel campo della sicurezza informatica. È fondamentale, pertanto, riservare delle risorse allo scopo di effettuare un'analisi accurata di questi dati per poter sfruttare al meglio le informazioni raccolte e implementare le dovute misure di sicurezza.

Capitolo 3

Laboratorio DSP

In questo capitolo mostriamo il funzionamento delle honeypots in uno scenario di attacco su Docker Security Playground [3]. Nello scenario implementato abbiamo utilizzato tre honeypot, uno per ogni livello di iterazione, e mettendoci nei panni dell'attaccante, ignaro della loro reale natura, abbiamo cercato di interagire con essi e di sfruttarne le vulnerabilità.

Alla fine di ogni interazione abbiamo riportato i dati raccolti.

3.1 Honeypot utilizzati

3.1.1 Dionaea

È un honeypot a bassa interazione che emula diversi protocolli come HTTP, FTP, TFTP, SMB, MSSQL, MySQL e SIP. Emula un sistema Windows 2000. Il suo scopo è quello di ottenere una copia dei malware usati dagli attaccanti. Nel nostro elaborato usiamo l'immagine `dinotools/dionaea` presente su Docker Hub, lasciando la configurazione di default.

3.1.2 Cowrie

Cowrie è un honeypot SSH e Telnet a media/alta interazione progettato per registrare gli attacchi di forza bruta e l'interazione della shell eseguita dall'attaccante. In modalità media interazione (shell) emula un sistema UNIX in Python. Questa è la modalità di default e prevede un file system falso con la possibilità di aggiungere e rimuovere file; questi file possono essere scaricati con `curl/wget` o

caricati tramite SFTP. I file aggiunti dall'attaccante vengono salvati per una successiva ispezione. In modalità alta interazione (proxy) funziona come proxy SSH e telnet per osservare il comportamento dell'attaccante su un altro sistema. In questo caso è possibile impostare un server reale a cui reindirizzare il traffico o lasciare che cowrie gestisca un pool di macchine virtuali generate dinamicamente (una per ogni attaccante in base all'ip). Per l'utilizzo a media interazione abbiamo installato Cowrie su un container docker Ubuntu 22.04 e mappato le connessioni sulle porte 22 e 23 per ssh e telnet rispettivamente. Per quanto riguarda l'utilizzo di Cowrie ad alta interazione abbiamo utilizzato l'immagine docker di Cowrie e cambiato la configurazione come indicato di seguito.

```
[honeypot]
backend = proxy

[proxy]
backend = simple
backend_ssh_host = 193.20.1.3
backend_ssh_port = 22
backend_user = dsp
backend_pass = dsp

[ssh]
listen_endpoints = tcp:22:interface=0.0.0.0
```

Figura 3.1: Configurazione Cowrie ad alta interazione

3.2 Configurazione laboratorio

Il laboratorio ha lo scopo di simulare una rete di honeypots che serve a "confondere" l'attaccante il cui bersaglio sono gli host su tale rete. La configurazione proposta presenta 5 nodi di rete, ovvero:

- **Dionaea** come honeypot a bassa interazione.
- **Cowrie** implementato su Ubuntu come honeypot a media interazione.

Per avviarlo vanno eseguiti i seguenti comandi dalla Shell:

```
$ sudo su - cowrie  
$ cowrie/bin/cowrie start
```

- **Cowrie_High** come honeypot ad alta interazione.
- **Server** che corrisponde ad un punto di atterraggio delle connessioni indirizzate a Cowrie_High.
- **Kali** invece rappresenta l'attaccante.

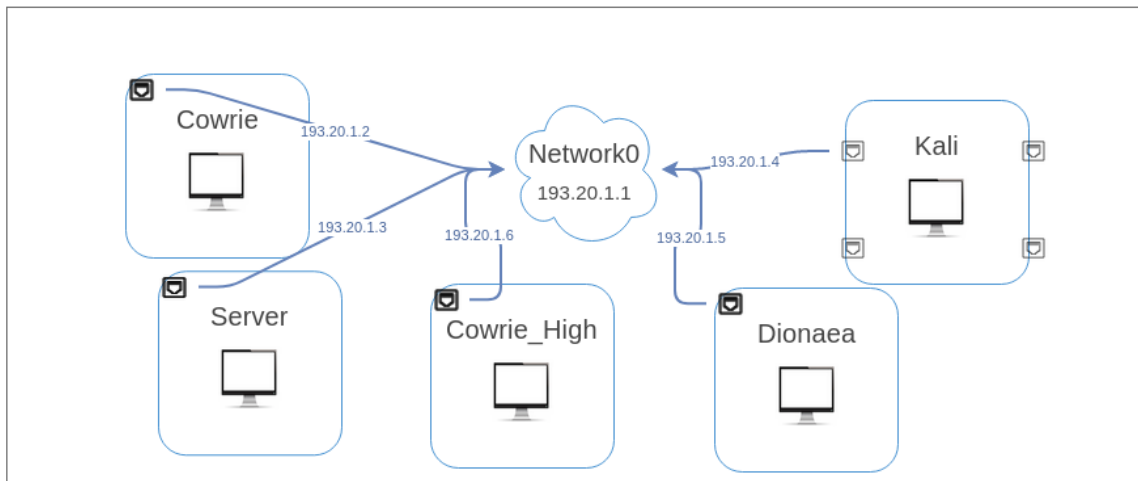


Figura 3.2: Grafico di rete su DSP

Docker-compose file:

```
version: '2'

services:
  Cowrie:
    image: 'xmarf/honeypot_ubuntu:latest'
    stdin_open: true
    tty: true
    networks:
      Network0:
        ipv4_address: 193.20.1.2

  Dionaea:
    image: 'dinotools/dionaea:latest'
    stdin_open: true
    tty: true
    networks:
      Network0:
        ipv4_address: 193.20.1.5

  Server:
    image: 'nsunina/ssh-server:1.0'
    stdin_open: true
    tty: true
    networks:
      Network0:
        ipv4_address: 193.20.1.3
    cap_add:
      - ALL

  Cowrie_High:
    image: 'fgipa246/cowrie_high:latest'
    stdin_open: true
    tty: true
```

```
networks:
  Network0:
    ipv4_address: 193.20.1.6
Kali:
  image: 'dockersecplayground/kali:v1.0'
  stdin_open: true
  tty: true
  networks:
    Network0:
      ipv4_address: 193.20.1.4
  cap_add:
    - ALL
  privileged: true
networks:
  Network0:
    ipam:
      config:
        - subnet: 193.20.1.1/24
```

3.3 Scenari di attacco

La soluzione proposta presenta tre differenti scenari d'attacco che differiscono in base all'"astuzia" dell'attaccante e al livello d'interazione delle honeypots. Prima di procedere alla scelta degli scenari, ogni attaccante esegue una scansione in rete con il tool Nmap eseguendo il comando sulla rete:

```
$ nmap 193.20.1.0/24
```

```
Nmap scan report for honeypots_Cowrie_1.honeypots_Network0 (193.20.1.2)
Host is up (0.00016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
MAC Address: 02:42:C1:14:01:02 (Unknown)

Nmap scan report for honeypots_Server_1.honeypots_Network0 (193.20.1.3)
Host is up (0.00015s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C1:14:01:03 (Unknown)

Nmap scan report for honeypots_Dionaea_1.honeypots_Network0 (193.20.1.5)
Host is up (0.00015s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
1723/tcp  open  pptp
3306/tcp  open  mysql
5060/tcp  open  sip
9100/tcp  open  jetdirect
MAC Address: 02:42:C1:14:01:05 (Unknown)

Nmap scan report for honeypots_Cowrie_High_1.honeypots_Network0 (193.20.1.6)
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C1:14:01:06 (Unknown)

Nmap scan report for d042e21f68d9 (193.20.1.4)
Host is up (0.00019s latency).
All 1000 scanned ports on d042e21f68d9 (193.20.1.4) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 204.64 seconds
root@d042e21f68d9:/#
```

Figura 3.3: Risultato di Nmap

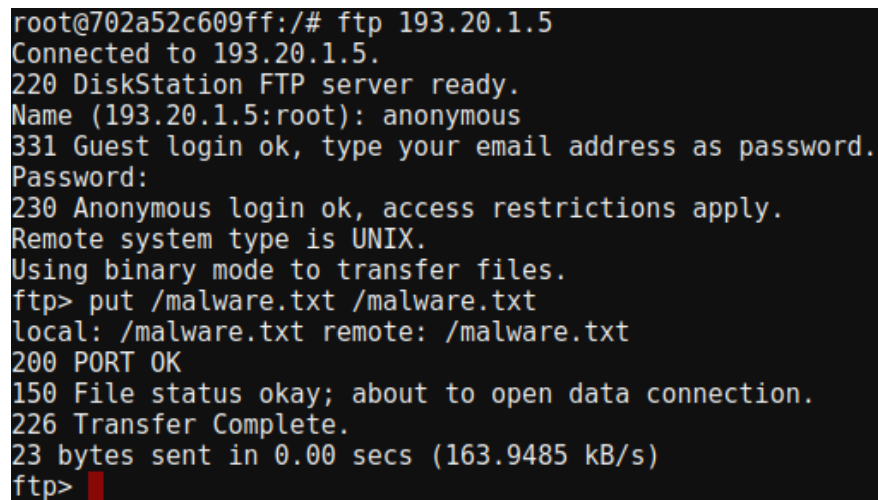
3.3.1 Scenario 1: attaccante "ingenuo" e honeypot a bassa interazione

La prima cosa che viene subito notata durante la scansione di Nmap è il grande numero di porte aperte presso l'host *193.20.1.5*. Il malintenzionato non esita due volte ad interagire con quel nodo di rete e lo fa sfruttando la porta legata ad *FTP*.

FTP consente infatti il login "anonimo" presso tale nodo in modo da poter inviare, o ottenere, file dalla destinazione.

Dopo aver generato il proprio file malware (nel nostro caso un semplice file txt) il malintenzionato effettua il login anonimo e lo invia alla destinazione eseguendo:

```
$ ftp root@193.20.1.5
$ put /malware.txt /malware.txt
```



```
root@702a52c609ff:/# ftp 193.20.1.5
Connected to 193.20.1.5.
220 DiskStation FTP server ready.
Name (193.20.1.5:root): anonymous
331 Guest login ok, type your email address as password.
Password:
230 Anonymous login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put /malware.txt /malware.txt
local: /malware.txt remote: /malware.txt
200 PORT OK
150 File status okay; about to open data connection.
226 Transfer Complete.
23 bytes sent in 0.00 secs (163.9485 kB/s)
ftp> █
```

Figura 3.4: Accesso tramite FTP e passaggio di un file malware.txt

A questo punto l'attaccante "stupido" non sa di aver colpito un Honeypot e di conseguenza viene tracciato da Dionea, i cui file di Log sono presenti al path `opt/dionaea/var/lib/dionaea/bistreams/`

```
root@5bd232ac8cab:/opt/dionaea/var/lib/dionaea/bistreams/2023-07-13# ls
ftpd-193.20.1.5-21-193.20.1.4-55398-2023-07-13T17:03:13.908685-Mcc1im
ftpd-193.20.1.5-21-193.20.1.4-60188-2023-07-13T17:03:13.486456-zXYdh1
B.20.1.5-21-193.20.1.4-60188-2023-07-13T17:03:13.486456-zXYdh107-13# cat ftpd-193
stream = (('out', b'220 DiskStation FTP server ready.\x0d\x0a'),
('in', b'USER anonymous\x0d\x0a'),
('out', b'331 Guest login ok, type your email address as password.\x0d\x0a'),
('in', b'PASS anonymous\x0d\x0a'),
('out', b'230 Anonymous login ok, access restrictions apply.\x0d\x0a'),
('in', b'SYST\x0d\x0a'),
('out', b'215 UNIX Type: L8\x0d\x0a'),
('in', b'TYPE I\x0d\x0a'),
('out', b'200 Type set to I.\x0d\x0a'),
('in', b'PORT 193,20,1,4,233,83\x0d\x0a'),
('out', b'200 PORT OK\x0d\x0a'),
('in', b'STOR /malware.txt\x0d\x0a'),
('out', b'150 File status okay; about to open data connection.\x0d\x0a226 Transfer Complete.\x0d\x0a'),
('in', b'TYPE A\x0d\x0a'),
('out', b'504 Not implemented for parameter \x27A\x27.\x0d\x0a'),
('in', b'PORT 193,20,1,4,179,245\x0d\x0a'),
('out', b'200 PORT OK\x0d\x0a'),
('in', b'LIST\x0d\x0a'),
('out', b'150 File status okay; about to open data connection.\x0d\x0a226 Transfer Complete.\x0d\x0a'),
('in', b'QUIT\x0d\x0a'),
('out', b'221 Goodbye.\x0d\x0a')]root@5bd232ac8cab:/opt/dionaea/var/lib/dionaea/bistreams/2023-07-13#
```

Figura 3.5: Log di Dionea

Le informazioni registrate da Dionea in fig.3.5 si riferiscono sia all'identità dell'attaccante, che alle attività da lui svolte. In particolar modo possiamo notare la tracciatura dell'indirizzo IP *193.20.1.4*, del login "anonimo" tramite *FTP* e del file malware passato mediante il comando *put*.

DinoTools/dionaea

Home of the dionaea honeypot



3.3.2 Scenario 2: attaccante poco "ingenuo" e honeypot a media interazione

L'attaccante, insospettito dai numerosi servizi offerti dall'host *192.20.1.5*, decide di scagliare l'attacco all'host *193.20.1.2*. Questo server presenta le porte 22 e 23 aperte, relative ai servizi SSH e telnet. Il primo passo consiste in un attacco a dizionario in modo da scoprire tutte le combinazioni username e password valide. Per questo attacco viene sfruttato il tool Hydra, a cui passiamo due dizionari: *username.txt* e *password.txt*. Il comando è il seguente:

```
$ hydra -L username.txt -P password.txt 192.20.1.2 ssh -t 5
```

```
root@f6f2e4c0da7:~# hydra -L usernames.txt -P passwords.txt 193.20.1.2 ssh -t 5
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2023-07-13 12:20:48
[DATA] max 5 tasks per 1 server, overall 5 tasks, 576 login tries (l:18/p:32), ~116 tries per task
[DATA] attacking ssh://193.20.1.2/
[22][ssh] host: 193.20.1.2 login: root password: blondes
[22][ssh] host: 193.20.1.2 login: root password: broncos
[22][ssh] host: 193.20.1.2 login: root password: private
[22][ssh] host: 193.20.1.2 login: root password: skippy
[22][ssh] host: 193.20.1.2 login: root password: marvin
[STATUS] 322.00 tries/min, 322 tries in 00:01h, 254 to do in 00:01h, 5 active
[22][ssh] host: 193.20.1.2 password: broncos
[22][ssh] host: 193.20.1.2 password: private
[22][ssh] host: 193.20.1.2 password: skippy
[22][ssh] host: 193.20.1.2 password: marvin
[22][ssh] host: 193.20.1.2 password: blondes
[22][ssh] host: 193.20.1.2 password: enjoy
[22][ssh] host: 193.20.1.2 password: girl
[22][ssh] host: 193.20.1.2 password: apollo
[22][ssh] host: 193.20.1.2 password: parker
[22][ssh] host: 193.20.1.2 password: qwert
[22][ssh] host: 193.20.1.2 password: time
[22][ssh] host: 193.20.1.2 password: sydney
[22][ssh] host: 193.20.1.2 password: women
[22][ssh] host: 193.20.1.2 password: voodoo
[22][ssh] host: 193.20.1.2 password: magnum
[22][ssh] host: 193.20.1.2 password: juice
[22][ssh] host: 193.20.1.2 password: abgrtyu
[22][ssh] host: 193.20.1.2 password: 777777
[22][ssh] host: 193.20.1.2 password: dreams
[22][ssh] host: 193.20.1.2 password: maxwell
[22][ssh] host: 193.20.1.2 password: music
[22][ssh] host: 193.20.1.2 password: rush2112
[22][ssh] host: 193.20.1.2 password: russia
[22][ssh] host: 193.20.1.2 password: scorpion
[22][ssh] host: 193.20.1.2 password: rebecca
[22][ssh] host: 193.20.1.2 password: tester
[22][ssh] host: 193.20.1.2 password: mistress
[22][ssh] host: 193.20.1.2 password: phantom
[22][ssh] host: 193.20.1.2 password: billy
[22][ssh] host: 193.20.1.2 password: 6666
[22][ssh] host: 193.20.1.2 password: albert
1 of 1 target successfully completed, 37 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-07-13 12:22:34
root@f6f2e4c0da7:~#
```

Figura 3.6: Output Hydra

Con le combinazioni ottenute, l'attaccante effettua l'accesso al server ssh e va a leggere il file delle password:

```
$ cat ./etc/passwd
```

```

root@6f6f2ee4c0da7:/# ssh root@193.20.1.2
The authenticity of host '193.20.1.2 (193.20.1.2)' can't be established.
ECDSA key fingerprint is SHA256:VUWBenKZ5qozA1rwKGX51lgSKVj7qYnt7RSqC0cghDIU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '193.20.1.2' (ECDSA) to the list of known hosts.
root@193.20.1.2's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# cd .. /etc
root@svr04:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail list Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
phil:x:1000:1000:Phil California,,,:/home/phil:/bin/bash

root@svr04:/etc#
```

Il report di tutte le attività svolte dall'attaccante può essere consultato sotto forma di file *json* al path *cowrie/var/log/cowrie/cowrie.json*:

[illegible]

```
[{"eventid":"c0wrie_login.failed","username":"guest","password":"tigger","message":"login attempt [guest/tigger] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:38.331837Z","src_ip":"193.20.1.4","session":"a93215eeffb8"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"robert","message":"login attempt [guest/robert] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:39.277040Z","src_ip":"193.20.1.4","session":"d3e019a1f646"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"access","message":"login attempt [guest/access] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:39.287851Z","src_ip":"193.20.1.4","session":"fba62fb9b721"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"love","message":"login attempt [guest/love] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:39.314677Z","src_ip":"193.20.1.4","session":"53d18691afec"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"buster","message":"login attempt [guest/buster] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:39.324820Z","src_ip":"193.20.1.4","session":"d7d6fd7a14f"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"1234567","message":"login attempt [guest/1234567] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:39.335264Z","src_ip":"193.20.1.4","session":"a93215eeffb8"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"soccer","message":"login attempt [guest/soccer] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:40.281871Z","src_ip":"193.20.1.4","session":"d3e019a1f646"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"hockey","message":"login attempt [guest/hockey] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:40.292304Z","src_ip":"193.20.1.4","session":"fba62fb9b721"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"killer","message":"login attempt [guest/killer] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:40.318704Z","src_ip":"193.20.1.4","session":"53d18691afec"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"george","message":"login attempt [guest/george] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:40.329898Z","src_ip":"193.20.1.4","session":"d7d6fd7a14f"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"sexy","message":"login attempt [guest/sexy] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:40.339582Z","src_ip":"193.20.1.4","session":"a93215eeffb8"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"andrew","message":"login attempt [guest/andrew] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:41.285883Z","src_ip":"193.20.1.4","session":"d3e019a1f646"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"charlie","message":"login attempt [guest/charlie] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:41.296779Z","src_ip":"193.20.1.4","session":"fba62fb9b721"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"superman","message":"login attempt [guest/superman] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:41.322314Z","src_ip":"193.20.1.4","session":"53d18691afec"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"asshole","message":"login attempt [guest/asshole] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:41.334401Z","src_ip":"193.20.1.4","session":"d7d6fd7a14f"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"fuckyou","message":"login attempt [guest/fuckyou] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:41.344005Z","src_ip":"193.20.1.4","session":"a93215eeffb8"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"dallas","message":"login attempt [guest/dallas] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:42.288519Z","src_ip":"193.20.1.4","session":"d3e019a1f646"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"jessica","message":"login attempt [guest/jessica] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:42.300893Z","src_ip":"193.20.1.4","session":"fba62fb9b721"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"admin","message":"login attempt [guest/admin] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:42.325791Z","src_ip":"193.20.1.4","session":"53d18691afec"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"panties","message":"login attempt [guest/panties] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:42.337346Z","src_ip":"193.20.1.4","session":"d7d6fd7a14f"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"pepper","message":"login attempt [guest/pepper] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:42.347494Z","src_ip":"193.20.1.4","session":"a93215eeffb8"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"lilli","message":"login attempt [guest/lilli] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:43.293267Z","src_ip":"193.20.1.4","session":"d3e019a1f646"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"austin","message":"login attempt [guest/austin] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:43.302861Z","src_ip":"193.20.1.4","session":"fba62fb9b721"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"william","message":"login attempt [guest/william] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:43.329568Z","src_ip":"193.20.1.4","session":"53d18691afec"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"daniel","message":"login attempt [guest/daniel] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:43.339732Z","src_ip":"193.20.1.4","session":"d7d6fd7a14f"},
{"eventid":"c0wrie_login.failed","username":"guest","password":"golfer","message":"login attempt [guest/golfer] failed","sensor":"b8d2c80db824","timestamp":"2023-07-14T11:48:43.349406Z","src_ip":"193.20.1.4","session":"a93215eeffb8"}]
```

Figura 3.9: Contenuto del file di log a media interazione

Possiamo notare che vengono registrate informazioni quali l'indirizzo IP da cui proviene l'attacco, tutte le combinazioni usate nell'attacco a forza bruta e tutti i comandi eseguiti dall'attaccante sull'honeypot.



HoneyPot

3.3.3 Scenario 3: attaccante medio e honeypot ad alta interazione

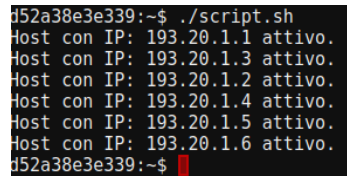
Il malintenzionato sceglie come bersaglio l'host *193.20.1.6* che presenta la sola porta 22 aperta. Una volta effettuato l'accesso, l'attaccante sfrutta quel nodo per eseguire un semplice script bash che effettua tramite ping la scansione di rete ottenendo informazioni sugli altri nodi.

script.sh:

```
#!/bin/bash

#
ls_ping()
{
    ping -c 1 $1 > /dev/null
    [ $? -eq 0 ] && echo Host con IP: $i attivo.
}

for i in 193.20.1.{1..255}
do
    ls_ping $i & disown
done
```



```
d52a38e3e339:~$ ./script.sh
Host con IP: 193.20.1.1 attivo.
Host con IP: 193.20.1.3 attivo.
Host con IP: 193.20.1.2 attivo.
Host con IP: 193.20.1.4 attivo.
Host con IP: 193.20.1.5 attivo.
Host con IP: 193.20.1.6 attivo.
d52a38e3e339:~$
```

Figura 3.10: Output script

Nel nostro esempio è stato eseguito un semplice Scanning della rete, ma un'alternativa poteva essere eseguire del codice malevolo dal nodo destinazione verso i nodi scoperti dallo Scanning. L'attaccante però non sa che quest'ultimo è una honeypot ad alta interazione che funge da Proxy verso un altro server SSH della rete. E' possibile quindi ottenere le informazioni di tracciatura di quest'attività copiano l'apposito file dal container Docker istanziato da DSP, utilizzando il comando seguente:

[illegible]

Figura 3.11: Dati registrati dallo scenario 3

Capitolo 4

Conclusioni

Lo scopo principale del laboratorio è stato quello di creare un "Playground" di honeypots in modo da poter sperimentare diverse tipologie di interazione con essi. L'idea è stata quella di simulare una rete il cui scopo risulta essere proprio quello di essere visibile e confondere i malintenzionati che puntano ad attaccare i diversi nodi su di essa. Fra le numerose soluzioni che si possono adottare quella presentata nel seguente elaborato risulta fra le più semplici, ma, riesce a dimostrare come le attività malevole possono essere tracciate a diversi livelli di interazione.

Per i primi scenari è stato mostrato come leggere la tracciatura presso le honeypots di bassa e media interazione attraverso protocolli come FTP, e attacchi di tipo forza bruta su SSH. Inoltre, è possibile notare come all'aumentare del livello di interazione con cui la honeypot lavora, aumenta la pericolosità di quest'ultimo di essere utilizzato per scopi secondari.

Nel nostro ultimo scenario è stato lanciato un semplice script per la scansione di rete dall'honeypot, ma non si esclude la possibilità che un attaccante riesca a far eseguire del diverso codice malevolo. In conclusione le honeypots sono potenti strumenti utili per il tracciamento dei malintenzionati, ma il loro posizionamento e il loro livello d'interazione sono fondamentali per la sicurezza in rete.

Bibliografia

- [1] <https://it.wikipedia.org/wiki/Honeypot>.
- [2] <https://webthesis.biblio.polito.it/21285/1/tesi.pdf>.
- [3] <https://github.com/DockerSecurityPlayground/DSP>.
- [4] Robert McGrew. Experiences with honeypot systems: Development, deployment, and analysis. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, volume 9, pages 220a–220a. IEEE, 2006.
- [5] Marcin Nawrocki, Matthias Wählisch, Thomas C Schmidt, Christian Keil, and Jochen Schönfelder. A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249*, 2016.