Sicurezza in rete: vulnerabilità, tecniche di attacco e contromisure

Alessandro Bulgarelli
bulgaro@weblab.ing.unimo.it

Riccardo Lancellotti
riccardo@weblab.ing.unimo.it

WEB Lab Modena

Black hat vs. White hat

- Qualsiasi apparato collegato ad Internet si espone a migliaia di potenziali attaccanti (black hat).
- Chi difende da queste minacce è definito white hat.
- In genere i black hat vincono!!!
- L'unico modo per contrastarli è studiarne costantemente le attività e le innovazioni.

Sicurezza in rete: vulnerabilità, tecniche di attacco e contromisure

Black side

Defacement

- Il defacement consiste nella modifica della homepage (e a volte anche delle pagine interne) di un sito web, effettuata ottenendo un accesso al server che lo ospita
- I contenuti originari vengono sostituiti con testi e/o immagini irridenti e critici, a volte nonsense (o apparentemente tali)
- Un defacement mina la credibilità del sito colpito, che dimostra di essere vulnerabile

Defacement

- Per ottenere l'accesso ad un sistema come "superuser" ed effettuare un defacement, l'attaccante utilizza:
  - exploit e bug noti che sfruttano vulnerabilità nel software (in particolare presenti nel server Web, ma non solo)
  - tattiche di social engineering
  - password cracking

Defacement

Todays reported and verified attacks: **676** of which **234** are single IP and **442** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
★ - Special defacement

Time	Attacker		Domain	OS	View
10:55	Fatal Error	H	zatec-gmbh.de	Win 2000	view | mirror
10:55	Fatal Error	H	schmid-fischerbach.de	Win 2000	view | mirror
10:55	Fatal Error	H	ruoff-raumausstattung.de	Win 2000	view | mirror
10:54	Fatal Error	H	drapp.de	Win 2000	view | mirror
10:54	Fatal Error	H	wolfgang-staiger.de	Win 2000	view | mirror
10:53	Fatal Error	H	bisinger.de	Win 2000	view | mirror
10:52	Fatal Error	H	weinmann-aach.de	Win 2000	view | mirror
10:52	TechTeam	H	serverge.net	Linux	view | mirror
10:51	SPYKIDS	H	sestakava.cz	Linux	view | mirror
10:51	SpyKids	H	emergencias.com.mx	Linux	view | mirror
10:50	SPYKIDS	H	vdi.cz	Win 2000	view | mirror
10:50	Fatal Error	H	lacker.de	Win 2000	view | mirror
10:50	TechTeam	H	kerbeck.com	Linux	view | mirror
10:50	Fatal Error	H	busam-online.de	Win 2000	view | mirror
10:49	Fatal Error	H	amd-germany.de	Win 2000	view | mirror
10:49	r00t_System	H	thehacker.com.br	Linux	view | mirror
10:49	Fatal Error	H	gewa-balkone.de	Win 2000	view | mirror
10:49	SPYKIDS	H M	vanik.borec.cz	Linux	view | mirror
10:49	Fatal Error	H	bukara.de	Win 2000	view | mirror
10:48	Fatal Error	H	hotel-sonnenhof.de	Win 2000	view | mirror
10:48	TechTeam	H	bahgladyfashions.com	Linux	view | mirror
10:48	Fatal Error	H	wagner-spielwaren.de	Win 2000	view | mirror
10:47	TechTeam	H	7south.com	Linux	view | mirror
10:47	Fatal Error	H	frankplastic.de	Win 2000	view | mirror

Defacement


www.ironsheeps.de - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://www.ironsheeps.de/
Search
Home Bookmarks The Mozilla Org... Latest Builds
Ironsheeps
Funclan
Nick: Pass: login Join Search: SEARCH Topics: Alle Überschriften
Start Themen Downloads _ACCOUNT News schreiben Top 10
Hauptmenü
Startseite
Members
Forum
Gästebuch
Hello Hacker !
Thank you for your nice posting :) And a real thanks that you damaged nothing . Cu , Mino
Geschrieben von Mino am Saturday, 08.May. @ 16:52:02 CEST (3 mal gelesen)
(Kommentare? |)
This Site Defaced By Kieger - HACKED - OWNED - GOT
r00t_System - AFROM4N - amarelo - Spofs - kieger - MC_KiNNeY - r00t_System Hack u Box !! irc.brasnet.org - #Ry - r00tSystem@hush.com

Ispezione della rete

- L'ispezione della rete, in genere, è utilizzata come vero e proprio preludio ad un vero attacco.
- È la combinazione di:
  - Raccolta dati
  - Ricerca di informazioni
  - Controllo delle policy di sicurezza adottate

Footprinting

- Il termine anglosassone footprint significa “impronta”
- Lo scopo è di raccogliere il maggior numero di informazioni riguardanti gli aspetti della situazione di protezione di una struttura.
- Si vuole determinarne il footprint, il profilo della presenza su Internet, degli accessi remoti e di eventuali Intranet/Extranet del sistema obiettivo.

Scansione delle porte

- Consiste nell'invio di pacchetti alle porte TCP e UDP del sistema obiettivo per stabilire quali servizi siano in esecuzione (o in stato di LISTENING)
- Conoscere i servizi attivi fornisce importanti informazioni che possono essere sfruttate in sede di attacco al sistema
  - Identificazione del tipo di sistema operativo
  - Identificazione di particolari applicazioni o di versioni di uno specifico servizio

Nmap

- Dalla semplice scansione eseguita risulta che l'host ha diverse porte “well-known” aperte
- Tra i risultati si noti la presenza di un Web server, della porta dedicata all'HTTPS ed il servizio ssh attivo
- È importante determinare la versione dei servizi e delle applicazioni installati

Identificazione dei servizi

- Identificate le porte aperte sul sistema obiettivo, è fondamentale determinare quali sono i servizi attivi “dietro” quelle porte
- È indispensabile in quanto i report forniti dai tool di scan eseguono automaticamente una associazione tra numero porta e servizio ad essa associata
- Es. Se viene trovata aperta la porta 25, nmap segnala la presenza di un server SMTP sull'host

Fingerprinting dello stack

- Con fingerprinting (dello stack) si intende quella tecnologia che consente di identificare con grande precisione il sistema operativo di un host

- Ciò che rende possibile questa analisi è la differente implementazione dello stack TCP/IP per ciascun OS

Attacco al sistema

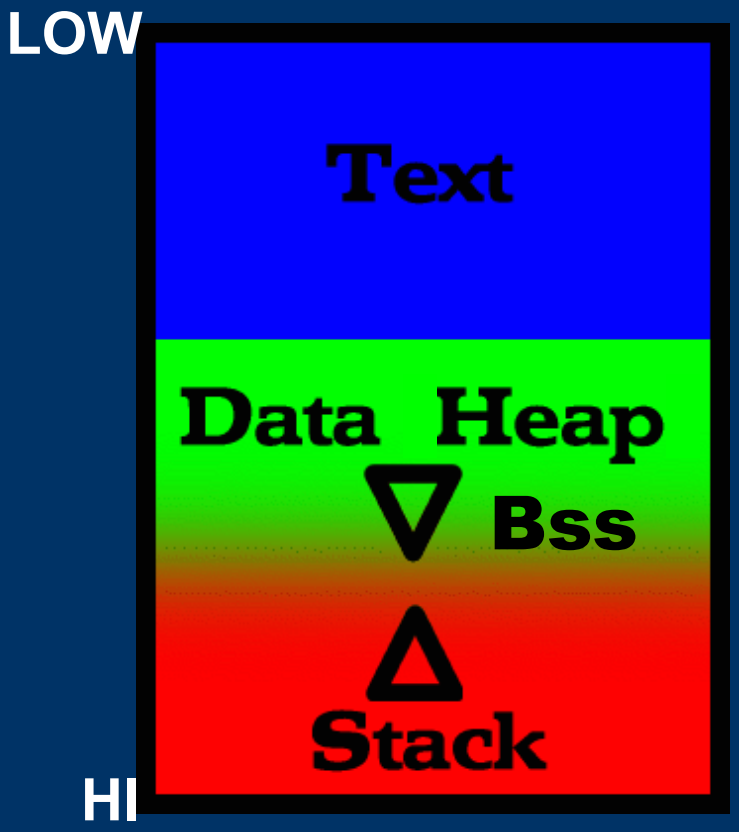
Una volta identificato l'obiettivo, per eseguire il defacement del sito Web, l'attaccante interverrà per:

- sfruttare vulnerabilità ⟶ buffer overflow
- compiere escalation di privilegi ⟶ ptrace bug

Buffer overflow

- La causa dei principali problemi di overflow del buffer è da individuare nell'intrinseca mancanza di sicurezza del linguaggio di programmazione
- Non vi è alcun controllo sui limiti degli array e dei riferimenti di puntatore, e ciò significa che uno sviluppatore deve assumersi l'onere di questo tipo di controlli

Segmentazione della memoria

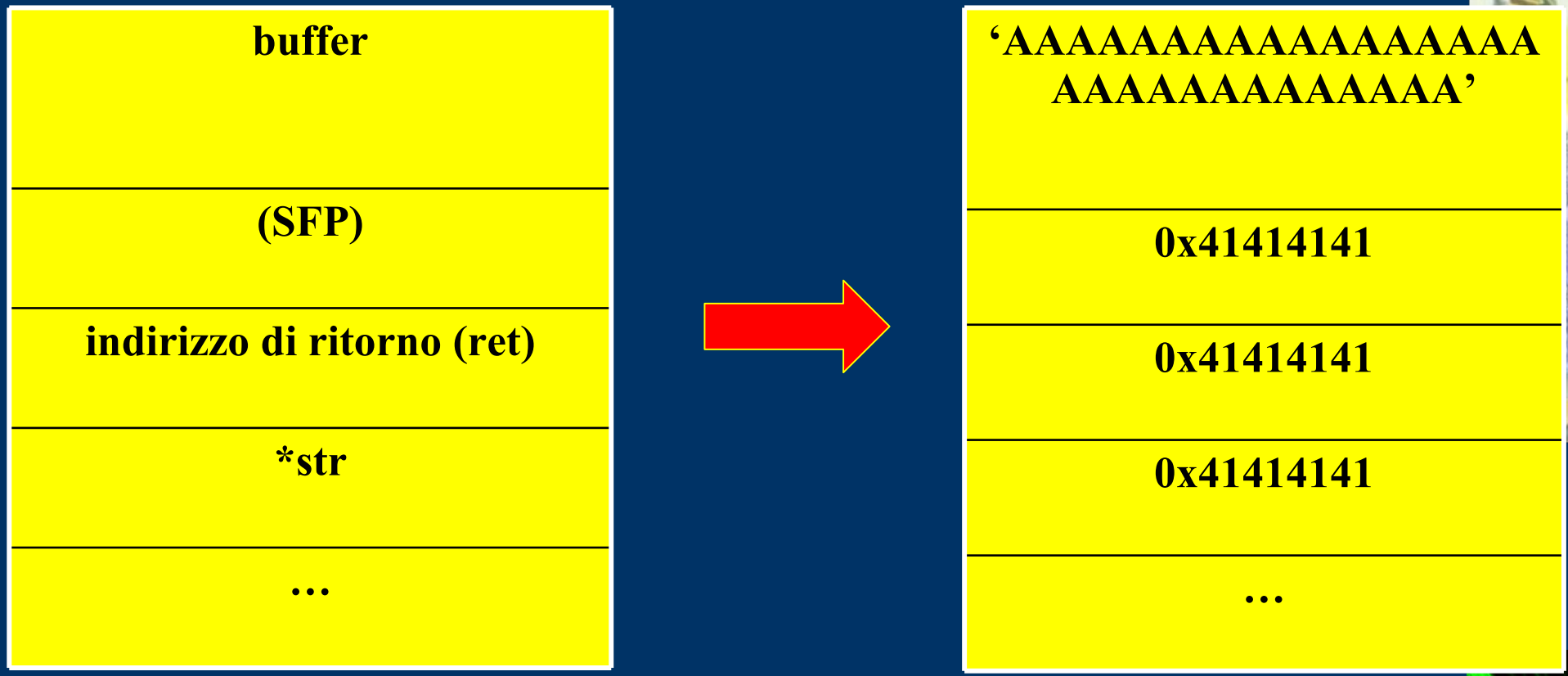


Codice e dati *read-only*

Dati inizializzati e non

Stack delle operazioni

Buffer overflow



- Una volta superata la dimensione del buffer, le informazioni vengono scritte all'interno di altri registri. In particolare può essere sovrascritto il registro EIP

Bytecode

- Il bytecode è un “pezzo” di codice autonomo, progettato in modo astuto, che può essere inserito all'interno dei buffer
- Diverse restrizioni:
  - Autonomo
  - Non contenere determinati caratteri speciali
- Il più comune bytecode è lo shellcode

Shellcode

- Questo bytecode genera una shell
- Se si riesce a manomettere un programma suid root in maniera che esegua uno shellcode, si disporrà di una shell utente con privilegi di root
- Complicazioni (per l'attaccante!!!):
  - L'indirizzo reale dello shellcode deve essere noto
  - I 4 Byte nei quali è memorizzato l'indirizzo di ritorno devono essere sovrascritti con l'indirizzo dello shellcode

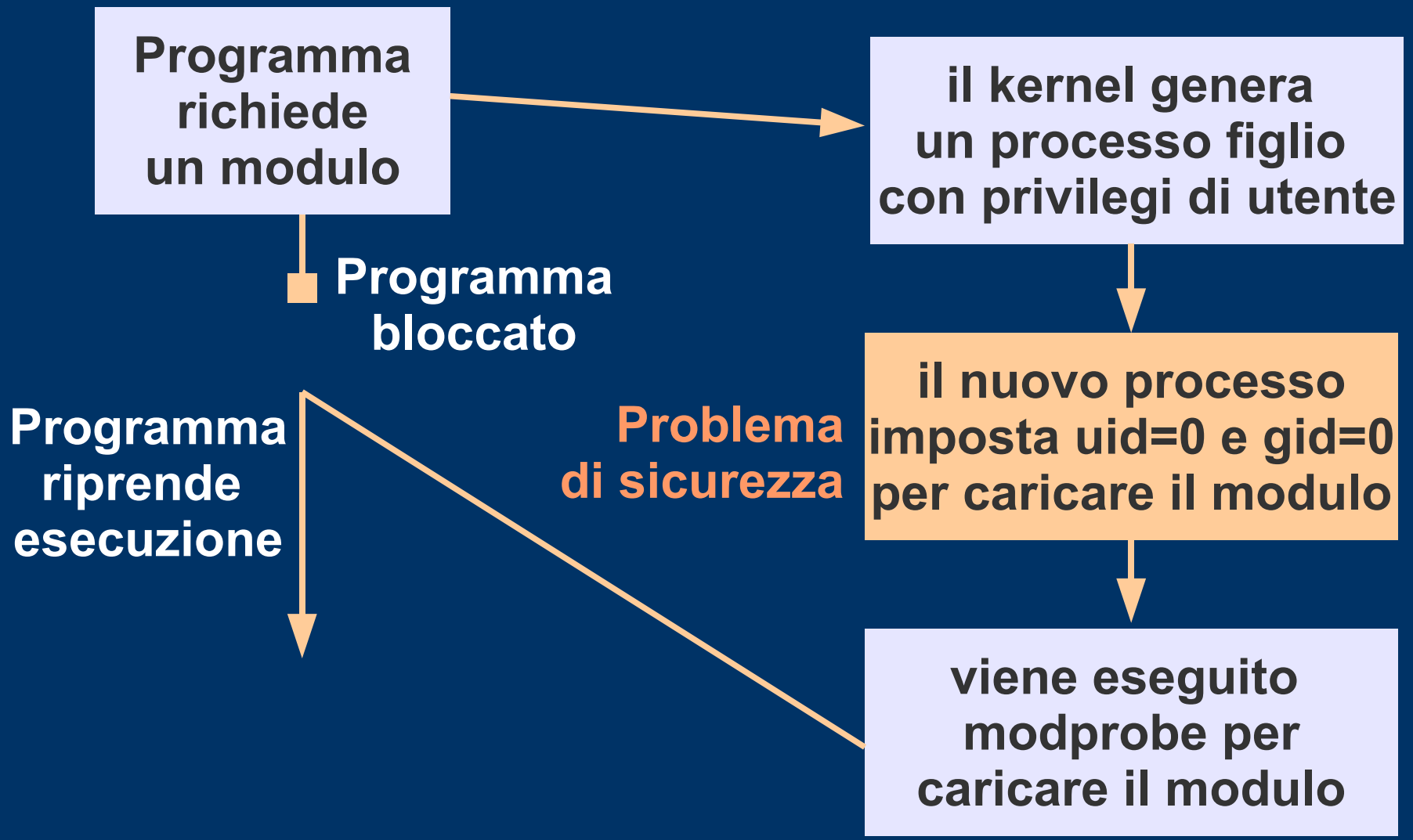
System call ptrace

- Usata principalmente dai debugger
- Consente di:
  - tracciare le system call di un processo
  - leggere e modificare lo spazio di memoria e i registri di un programma
  - inserire breakpoints
- Prevede un modello di sicurezza:
  - un processo può interferire solo con processi dello stesso utente
  - il modello non è perfetto...

Caricamento di un modulo

- Moduli del kernel: funzioni aggiuntive caricate e scaricate dinamicamente
- Quando un processo deve usare delle funzioni di un modulo si invoca il module loader
- Per un breve attimo il processo assume i privilegi di superutente ed esegue modprobe
  - potenzialmente rischioso

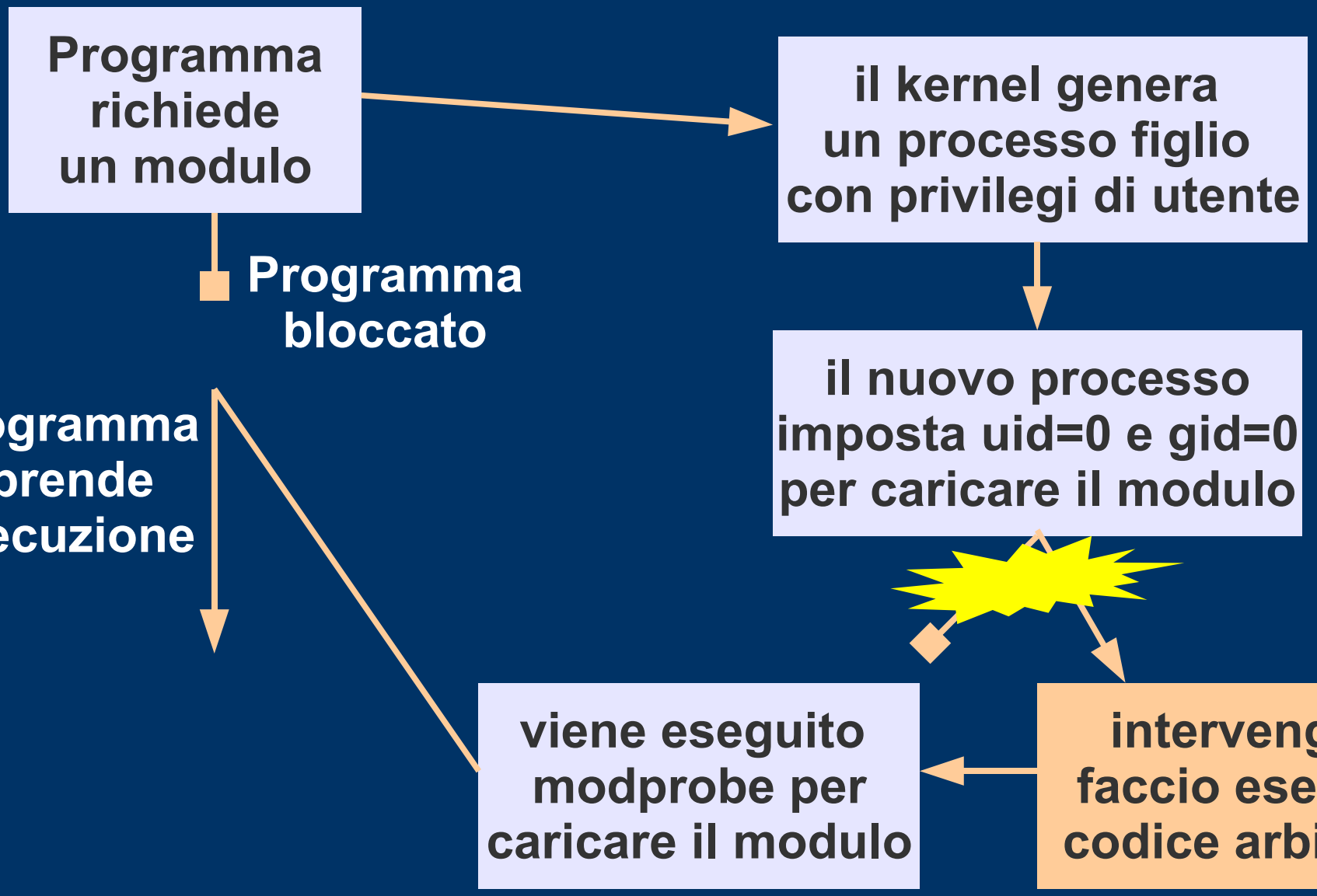
Caricamento di un modulo



Privilege escalation con ptrace

- Si traccia il flusso di un programma
- Quando viene richiesto un modulo è possibile
  - tracciare il processo figlio che deve caricare il modulo
  - intercettare la system call che esegue modprobe
- Attraverso ptrace possiamo controllare un processo che ha guadagnato privilegi di superutente

Caricamento “ritoccato”



Sicurezza in rete: vulnerabilità, tecniche di attacco e contromisure

White side

Il processo della sicurezza

- Non esistono sistemi informatici intrinsecamente sicuri ed è necessario adattarli continuamente alle esigenze ed alle politiche delle organizzazioni.

- La sicurezza non è un prodotto, bensì è un processo che integra dispositivi, tecnologie, politiche e soprattutto buonsenso!!!

Il processo della sicurezza

- Differenza tra prodotto e processo:
  - un prodotto è il risultato conclusivo di un ciclo di lavorazioni
  - un processo è un ciclo continuo di elaborazioni e modifiche
- Negli ultimi anni vi è stato un cambiamento di visione radicale per quanto riguarda la sicurezza:
  - da modello statico (sicurezza è installare un antivirus ed un firewall)
  - A modello dinamico (sicurezza è un ciclo continuo di azioni necessarie per evitare incidenti informatici)

Interventi sul caso di studio

- Il sistema precedentemente violato presenta alcuni problemi di sicurezza
  - mancanza di politiche di sicurezza
  - mancanza di tecnologie per la sicurezza

MANCANZA DI BUONSENSO

Politiche di sicurezza

Quadro generale di riferimento definito dal management contenente:

- – i principi base di sicurezza informatica cui attenersi relativamente a riservatezza, integrità, disponibilità, controllo degli accessi, …
- – le normative di riferimento relative alla sicurezza informatica
- – le responsabilità
- – …

Alla policy si devono attenere gli obiettivi, le soluzioni progettuali, i processi e le procedure

Politiche di sicurezza

Nel caso in esame si sono verificati almeno tre problemi:

- obsolescenza di più applicazioni
- obsolescenza del kernel
- mancanza di un controllo degli accessi

È fondamentale definire politiche di aggiornamento dei sistemi, dei servizi e delle applicazioni nonché di controllo degli stessi e nominare i responsabili di questo tipo di interventi

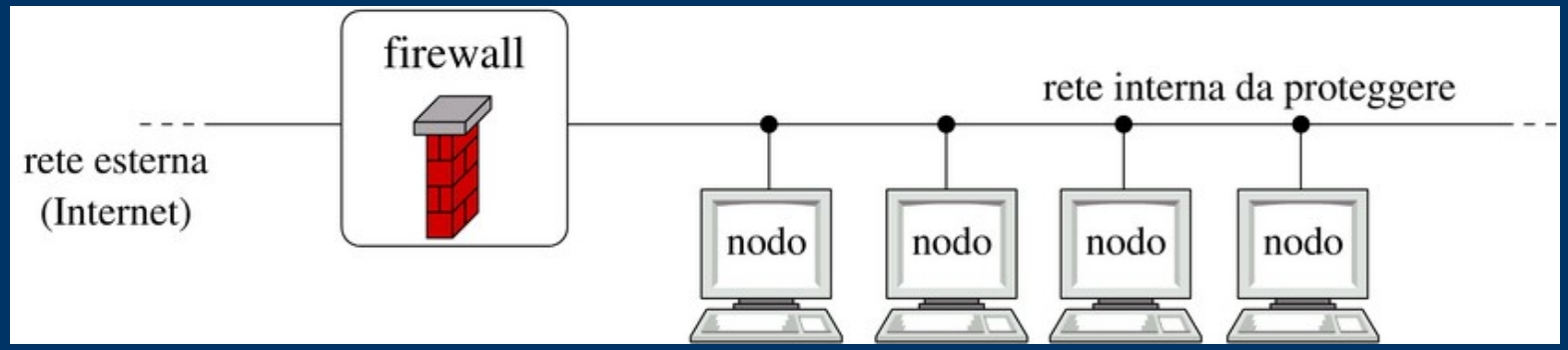
Tecnologie per la sicurezza

Tra le tecnologie dedicate alla protezione dei sistemi informatici sono da annoverare:

- Firewall
- Intrusion Detection System
- Virtual Private Network
- Honeypot

Firewall

Il firewall è un dispositivo di sicurezza che si interpone tra due diverse reti per controllare e limitare il traffico.



In genere i compiti sono svolti da un PC munito di almeno due interfacce di rete.

Firewall - Tipologie

In base alle funzionalità si possono identificare due tipologie di firewall:

- Packet Filtering
- Application Gateway (o Proxy Firewall)

Il Kernel Linux aggiunge alle funzionalità di packet filtering la trasformazione degli indirizzi e delle porte (NAT/PAT).

Firewall – Packet Filtering

I filtri di pacchetto bloccano o abilitano il traffico che attraversa il firewall definendo i protocolli, gli indirizzi IP e le porte utilizzate.

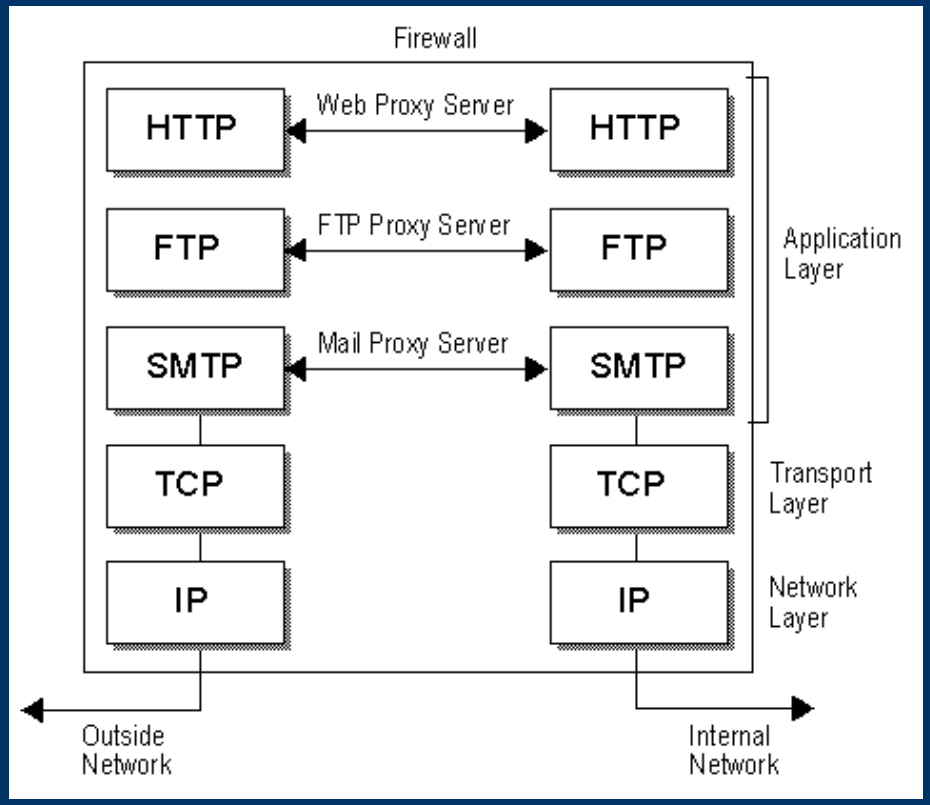
Questo tipo di firewall, di norma, agisce a livello 2 (network).

Quando un pacchetto arriva al packet filter, vengono estratte alcune informazioni dall'header e, in base alle regole definite, è inoltrato o scartato.

Proxy Firewall

Un firewall proxy è una applicazione che agisce da intermediaria tra due sistemi.

Agisce a livello applicazione (da qui l'appellativo *Application Gateway*).



IDS: Definizione

- Un Intrusion Detection System (IDS) è un sistema di rilevazione, segnalazione e logging delle attività di intrusione, utilizzo illecito dei dispositivi di rete (workstation, server, router, ...) e delle applicazioni che deve controllare in base alla configurazione.

- Esistono diversi tipi di IDS:
  - basati sulla rete: Network IDS (NIDS)
  - basati sull'host: Host IDS (HIDS)
  - ibridi: Hybrid IDS

IDS: Funzionalità

- Analisi
  - del traffico di rete a vari livelli dello stack TCP/IP
  - dei log di sistema
  - degli eventi (trasferimento, apertura file, ...)
- Rilevamento delle attività sospette e/o illegali
- Logging dettagliato delle attività rilevate (valore legale dei log)

Falsi positivi e falsi negativi

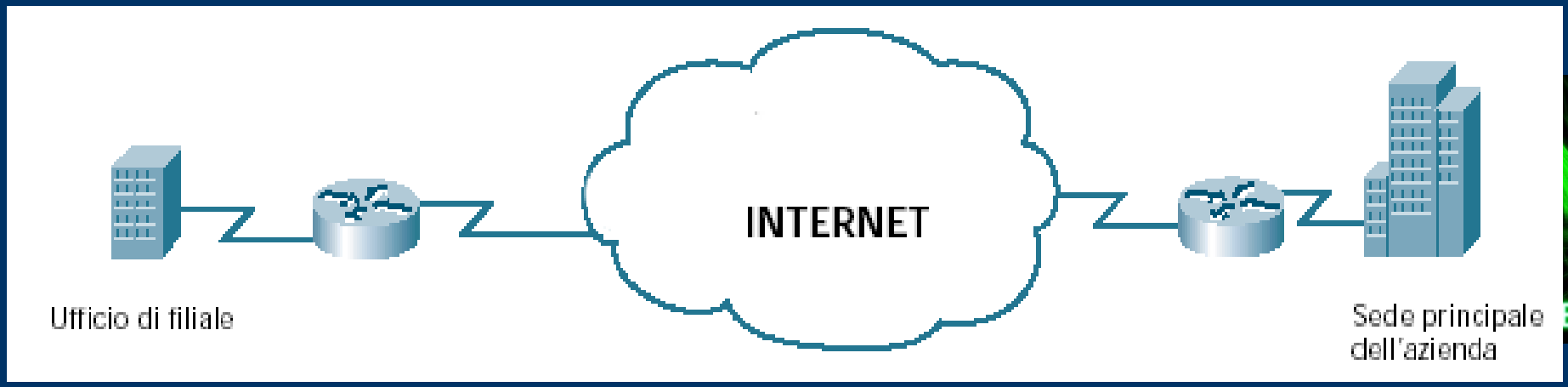
- Falsi positivi: si parla di falso positivo quando un IDS segnala erroneamente un attacco
- Falsi negativi: si parla di falso negativo quando un IDS non riesce a segnalare un'intrusione reale
- Indicatori di prestazioni degli IDS:
  - L'accuratezza di un IDS è compromessa quando tende a segnalare erroneamente un'intrusione (“falsi positivi”)
  - La completezza di un IDS è compromessa quando tende a non rilevare attacchi esistenti (“falsi negativi”)

VPN

VPN è l'acronimo di *Virtual Private Network* (ovvero Rete Privata Virtuale).

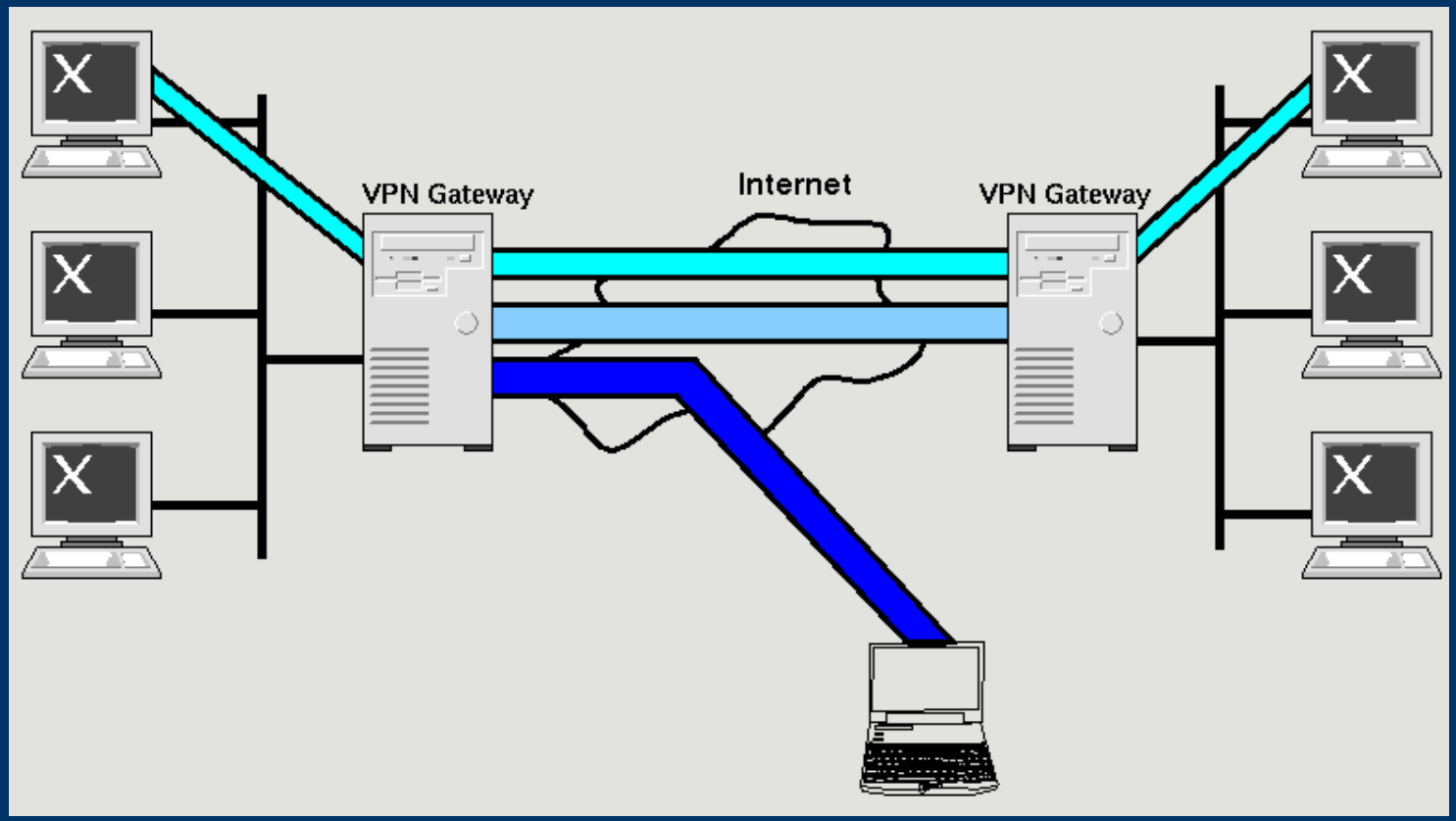
Alla base vi sono due necessità:

1. **implementazione di una *Intranet geografica***
2. **comunicazione sicura all'interno della *Intranet***



VPN: Implementazione

Si sfruttano Internet e la crittografia per far comunicare reti locali remote in modo riservato e completamente trasparente per l'utente.



Honeypot

Con il termine *honeypot* (letteralmente “vaso di miele”) si definisce un sistema studiato e configurato in modo da raccogliere informazioni su come i black hat analizzano ed attaccano un sistema informatico.

Lo scopo principale è assorbire il maggior numero di informazioni su un attaccante.

L’obiettivo è che il sistema sia analizzato, attaccato ed eventualmente violato dall’attacker.

Honeypot - Implementazione

- Sistema appositamente predisposto per essere compromesso
- Qualsiasi attività è monitorata e controllata
- Può essere hw o sw
- Non rimpiazza i sistemi di sicurezza esistenti, ma li integra