

La sicurezza delle reti LAN: Le soluzioni opensource.

Il ruolo dei Brand nello sviluppo

Dott. Matteo Lobbiani

ICT Specialist

lobbiani@punto blu.it

PUNTOBLU Srl

Profili stilati dal Federal Bureau Investigation

- **Insider impiegati licenziati, insoddisfatti o infedeli** in grado di danneggiare l'azienda o di sottrarre informazioni riservate attraverso una profonda conoscenza della rete telematica da colpire.
- **Hackers o Crackers** soggetti che si dedicano ad azioni delittuose per il gusto della sfida o per accreditarsi nella comunità "Hacker". Tuttavia, è sempre più frequente il caso di Hacker dediti ad attività delittuose per scopi di lucro.
- **Virus Writers** dediti ad ideare codici in grado di infettare le risorse presenti nella Rete.
- **Criminal Organization** associazioni a delinquere finalizzate a sfruttare internet per procurarsi profitti economici.
- **Terrorists** L'FBI ha individuato organizzazioni vicine a gruppi estremisti di Hamas e Al Qaeda che utilizzano la rete per propagandare, procurarsi fondi e comunicare in maniera anonima. Vi è un ulteriore pericolo proveniente dall'estremismo politico è il cd. cyberterrorism ovvero l'uso di strumenti telematici al fine di provocare lo "shut down", letteralmente spegnimento, delle infrastrutture critiche informatizzate (energia elettrica, trasporti, servizi sociali e sanitari).

Le grandi mafie mondiali hanno capito che le nuove tecnologie possono essere sfruttate per guadagni illeciti, e si stanno lanciando sul questo nuovo affare. I criminali informatici prima danneggiano i siti poi chiedono soldi per evitare altri attacchi.

Attaccano i siti Internet, poi si offrono di garantirne la sicurezza. A pagamento, ovviamente.

La notizia è nuova, ma il metodo è vecchio: i criminali informatici hanno infatti riscoperto e aggiornato l'antica pratica del racket delle estorsioni. E si stanno attrezzando in tutto il mondo supportati anche dalla mafia internazionale per organizzare un business che potrebbe essere miliardario.

COME CI ATTACCANO

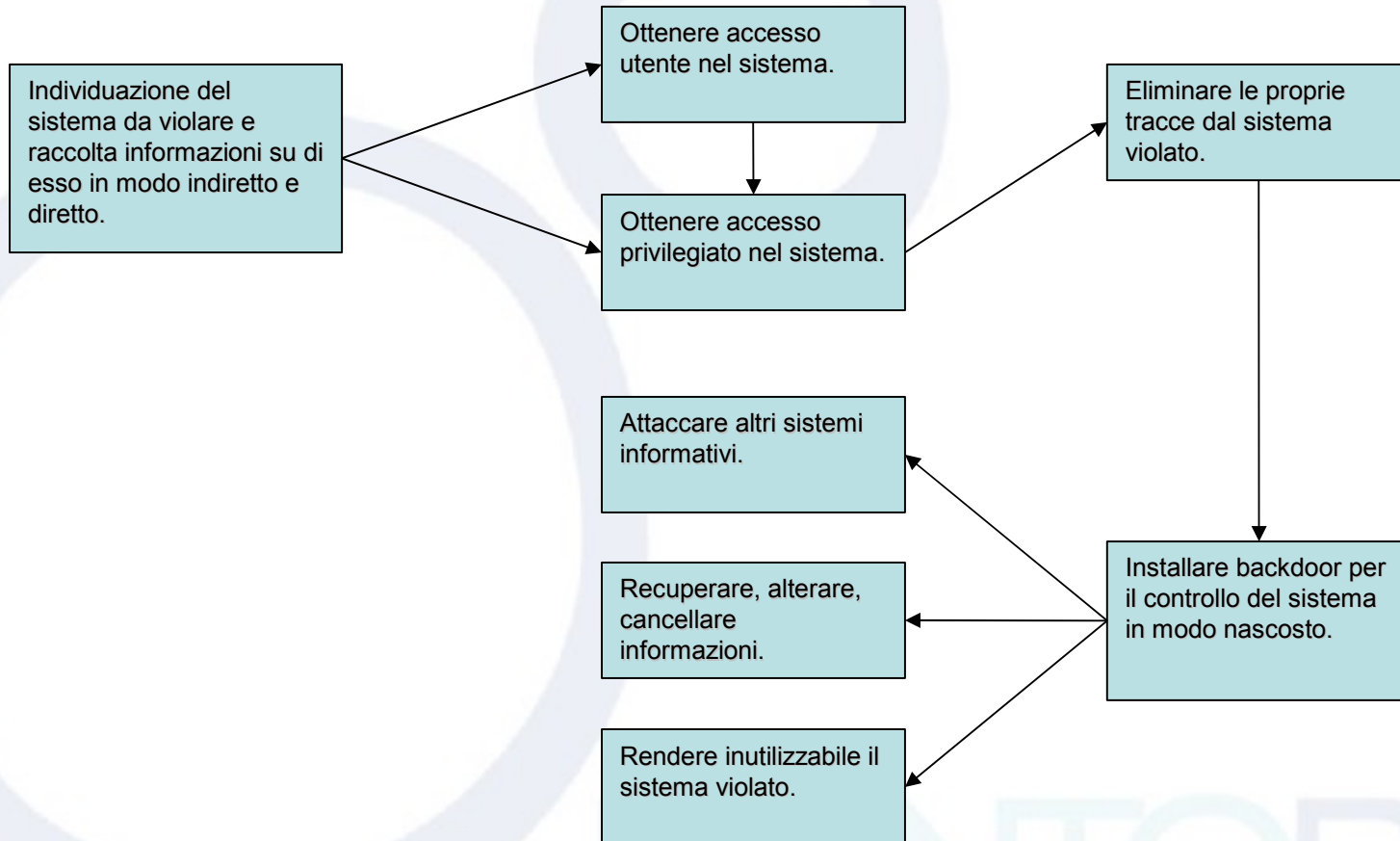
- DoS
- Esecuzione di codice arbitrario
- Virus
- Worm
- Trojan Horse
- Backdoor
- Spyware
- Dialer
- Hijacker
- Rootkit
- Adware
- Bot

ESEC. DI CODICE ARBITR.: si intende la possibilità che ha un Hacker di sfruttare una falla di un servizio offerto per eseguire poi codice sulla macchina obiettivo con i privilegi del servizio stesso

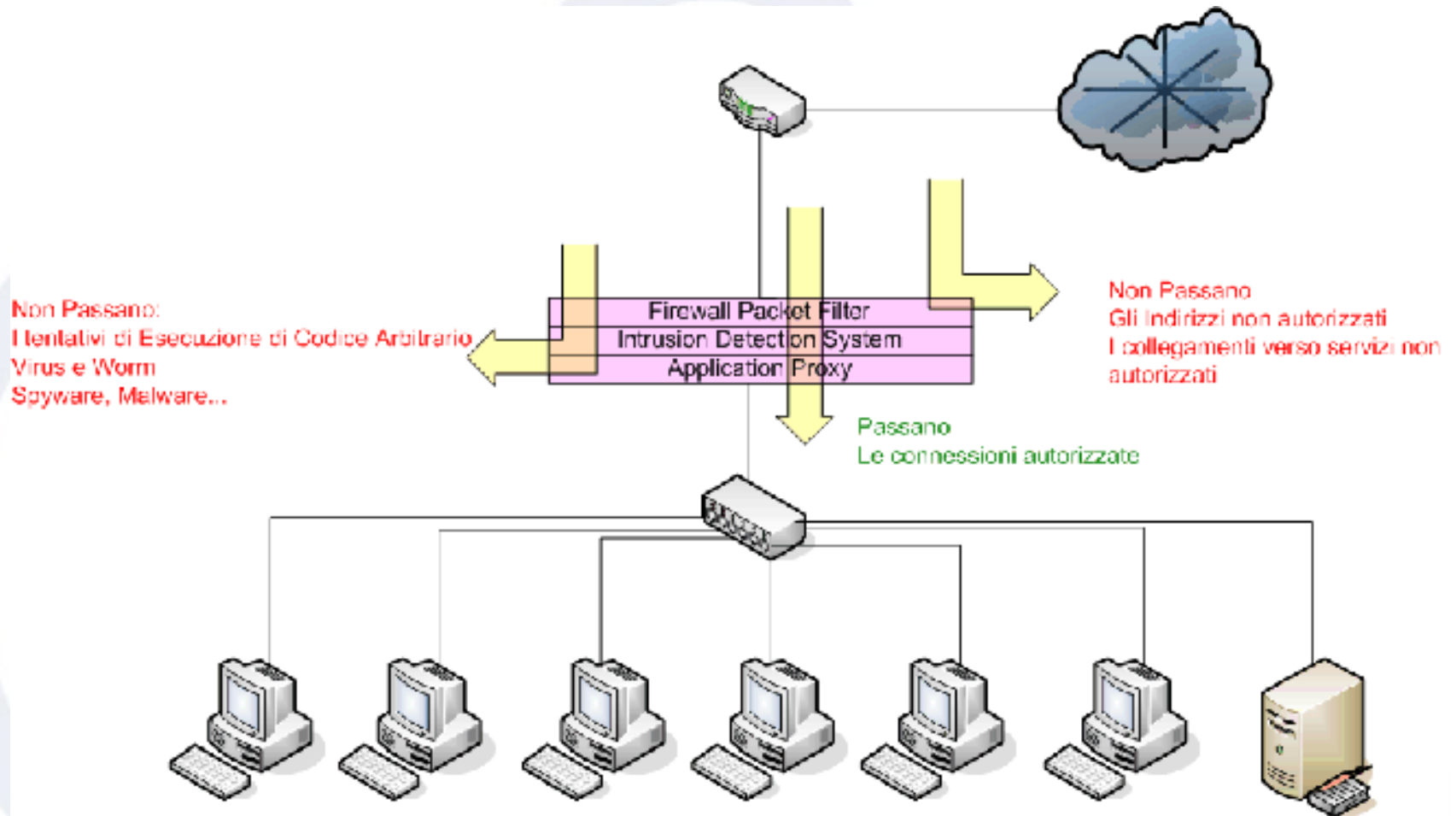
Sp...
i rootk...
un di...
modifi...
prese...
sono c...
funzio...
che a...
prese...
impostazioni del sistema. vengono quindi utilizzati per mascherare *spyware* e *trojan*

nome deriva dal famoso cavallo di Troia

FLUSSO DI UN ATTACCO



SICUREZZA PERIMETRALE



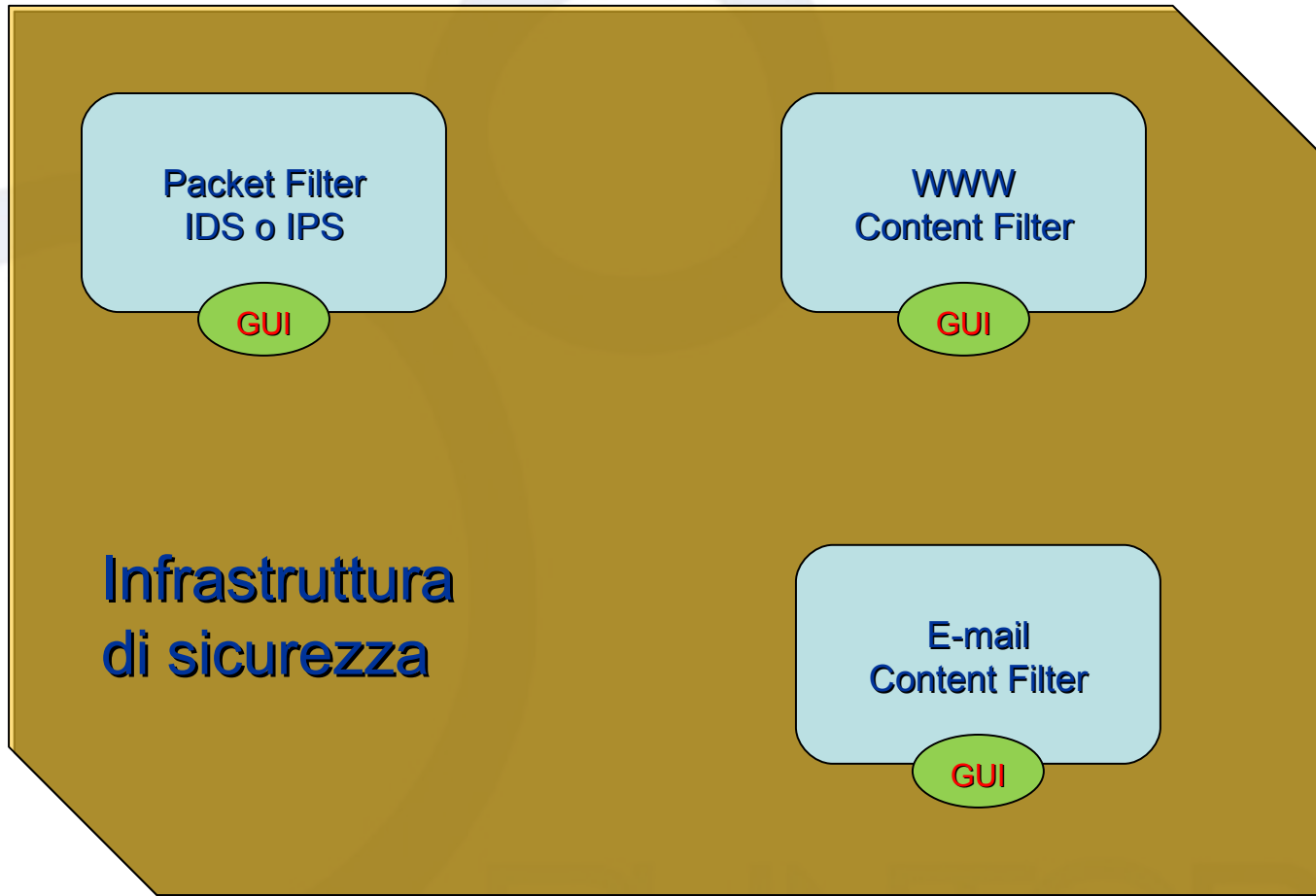
UNIFIED THREAT MANAGEMENT

Una soluzione Unified Threat Management (UTM) è un firewall di Rete che ingloba in se una serie di features nello stesso box. Solitamente una soluzione UTM permette di gestire :

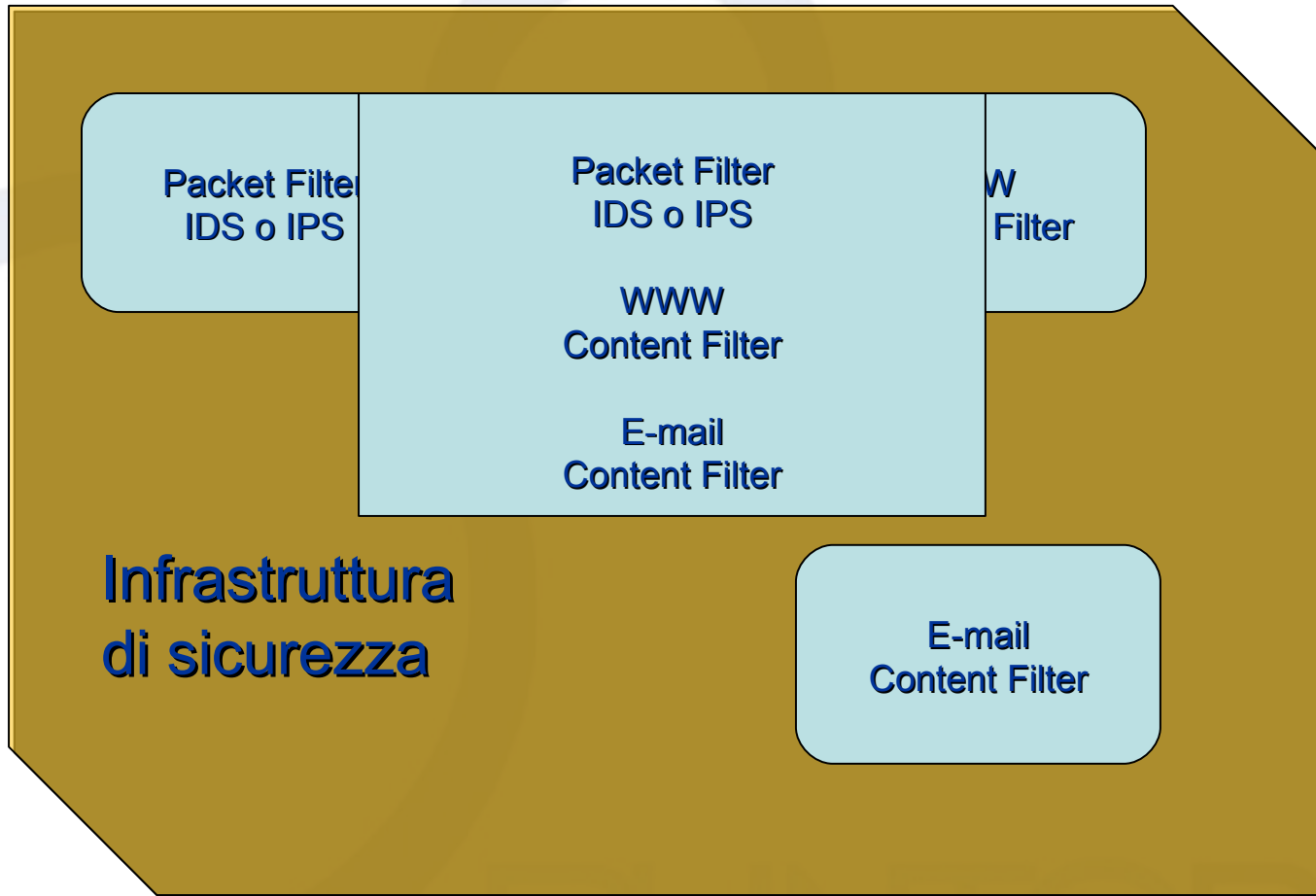
- **Packet Filtering**
- **Antivirus**
- **Antispam**
- **Intrusion Detection/Prevention System**
- **WWW Content Filtering**

Per alcune di queste funzionalità vengono utilizzati dei moduli applicativi a livello di proxy che permettono l'analisi del traffico in transito attraverso il firewall.

SOLUZIONI PROPRIETARIA



SOLUZIONE OPENSOURCE



**Infrastruttura
di sicurezza**

Packet Filter
IDS o IPS

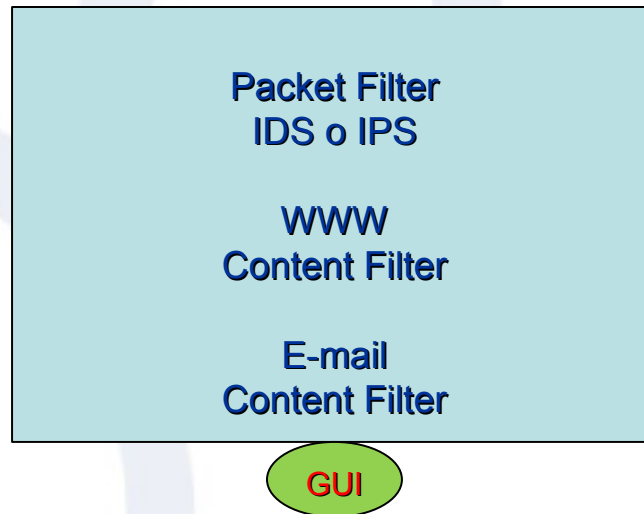
Packet Filter
IDS o IPS

WWW
Content Filter

E-mail
Content Filter

WWW
Filter

E-mail
Content Filter



Un' unica soluzione con GUI centralizzata

1. **Il software OpenSource è troppo rischioso per la IT Security.**
 - a) I Software OSS sono aggiornati più velocemente di quelli proprietari.
 - b) Molti software proprietari includono codice OSS.
 - c) Poco meno della metà delle più grandi imprese Europee utilizzano OSS.
2. **I progetti OSS sono gratis. Perché devo pagare per usarli ?**
 - a) I Progetti OSS sono scritti da sviluppatori per gli sviluppatori.
 - b) Spesso non sono corredati di manualistica appropriata per l'end-user.
 - c) Occorre un IT Manager skillato per gestire una realtà complessa.
3. **I Vendors non danno valore aggiunti ai Progetti OSS.**
 - a) Nei propri prodotti interfacciano gli OSS con GUI intuitive.
 - b) I prodotti sono corredati di manuali approfonditi
 - c) Gestiscono gli aggiornamenti dei prodotti in modo più user-friendly
 - d) Partecipano alla revisione del codice con i sviluppatori.
 - e) Finanziano economicamente i progetti OSS.

4. Maggiore affidabilità con prodotti proprietari.

- I prodotti proprietari basati su OSS prevedono manuali, aggiornamenti, customers support e training.
- b) Se un prodotto OSS non funziona, la comunità è la prima a segnalarlo e a fornire l'aggiornamento per risolvere il problema.

5. I progetti OpenSource per la sicurezza sono troppo complessi per le piccole aziende.

- I prodotti proprietari sono spesso a se stanti e occorre installare più di un prodotto per gestire una problematica di sicurezza.
- b) Una serie di prodotti OSS possono essere inglobati in un unico progetto migliorando la gestibilità della suite di sicurezza.

PROGETTI OPENSOURCE PER LA SICUREZZA

- **Netfilter/Iptables**
- **Snort**
- **Spamassassins**
- **Clamav**
- **Nessus**
- **Squid (non specifico per la Security)**
- **Exim (non specifico per la Security)**

PUNTOBLU

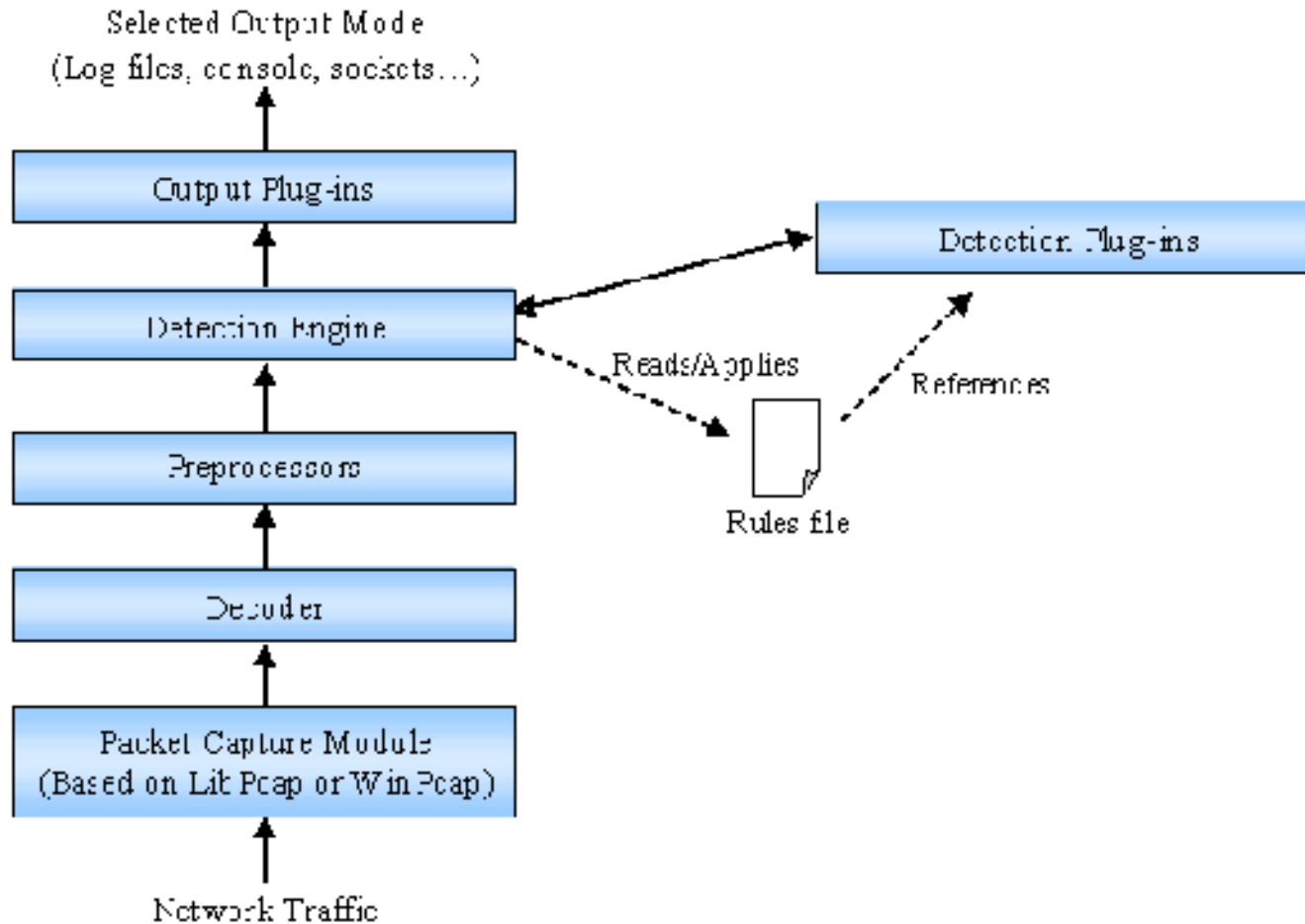


L'Intrusion Detection System o IDS è un dispositivo software e hardware (a volte la combinazione di tutti e due, sotto forma di sistemi stand-alone pre-installati e pre-configurati) utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici.

Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Questi attacchi includono gli attacchi alle reti informatiche tramite lo sfruttamento di un servizio vulnerabile, attacchi attraverso l'invio di dati malformati e applicazioni malevole, tentativi di accesso agli host tramite innalzamento illecito dei privilegi degli utenti, accessi non autorizzati a computer e file, e i classici programmi malevoli come virus, trojan e worm.

Un **IDS** è composto da quattro componenti. Uno o più **sensori** utilizzati per ricevere le informazioni dalla rete o dai computer. Una **console** utilizzata per monitorare lo stato della rete e dei computer e un **motore** che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica. Il motore di analisi si appoggia ad un **database** ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza. Esistono diverse tipologie di IDS che si differenziano a seconda del loro compito specifico e delle metodologie utilizzate per individuare violazioni della sicurezza. Il più semplice IDS è un dispositivo che integra tutte le componenti in un solo apparato.

DIAGRAMMA A BLOCCHI DI SNORT



PACKET CAPTURE MODULE

Questo modulo si occupa della cattura dei pacchetti in transito sulla rete.

Il Packet Capture Module sfrutta un altro progetto OSS, il libpcap project che si occupa del monitoraggio a basso livello del traffico di rete. Esso include anche una serie di tool per il debugging e le statistiche della rete

DECODER

Inserisce i pacchetti carritati in strutture dati e identifica i protocolli utilizzati. Questo modulo lavora a livello 3 della pila ISO/OSI e acquisisce informazioni circa porte e indirizzi del livello TCP. A questo livello Snort individua i pacchetti malformati.

Il preprocessor funge da filtro per Snort, esso verifica i pacchetti in arrivo e individua tutte quelle cose che poi il modulo successivo dovrà verificare in modo più approfondito come connessioni sospette TCP/UDP o portscan (troppi pacchetti UDP in un breve intervallo di tempo). Tutto quello che viene rilevato dal preprocessor viene indirizzato al Detection Engine. Il resto viene indirizzato verso l' Output Plugins.

Il preprocessor è un modulo fondamentale per snort perché permette al detection engine di lavorare in modo migliore occupandosi solo dei pacchetti sospetti e non di tutto quello che passa sulla rete.

PUNTOBLU



Il Detection Engine è il componente che riceve i pacchetti dai preprocessori e si occupa di confrontarli con le regole di intrusion detection. Nel caso in cui dovesse esserci una corrispondenza tra un pacchetto e più regole diverse, la prima regola che trova una corrispondenza con il contenuto di un pacchetto genera un allarme o, in alternativa, Snort offre anche la possibilità di generare un allarme per ciascun evento.

Il modulo Rules Files comprende una serie di file di testo divisi per categorie di attacchi ove sono contenute le regole del IDS. Queste regole vengono confrontate tramite il Detection Plugin con i pacchetti per verificare se trattasi di attacchi conosciuti. Queste regole vengono aggiornate come i database di un antivirus.

Quando viene trovata una corrispondenza tra un pacchetto e una regola, entrano in gioco i componenti di alerting e logging, il primo usato per generare gli allarmi, il secondo per archiviare i pacchetti che hanno causato la generazione dell'allarme. È possibile archiviare i log in un database MySQL, PostgreSQL, Oracle o ODBC, oppure inviarli ad un server Syslog, o salvarli in formato compatibile con Tcpcap.

IL RUOLO DEI BRAND: UN CASO REALE - ASTARO

Name Astaro Corporation

Anno di fondazione 2000

Sede Sede centrale EMEA: Karlsruhe (Germania)
Sedi US/APAC: Burlington, MA (U.S.A.)



L'approccio unico di Astaro include l'integrazione di dieci diverse applicazioni per la sicurezza in una singola appliance. Sulla base della qualità collaudata della piattaforma Linux, Astaro integra le soluzioni migliori grazie alla combinazione dei maggiori prodotti commerciali e open source per la sicurezza. Questo concetto ha creato la miglior appliance "tutto in uno" per la protezione della rete sul mercato. Astaro Security Gateway integra la protezione della rete, i filtri Web e la protezione della posta elettronica in un'interfaccia utente basata sul Web, intuitiva e di facile uso.

IL RUOLO DEI BRAND: UN CASO REALE - ASTARO

Da Wikipedia:

Astaro is working closely with the open source community to develop its products, although its business model is to sell software licenses and subscriptions.

Open source projects that are sponsored or supported by Astaro include: Netfilter, ClamAV, Openswan, strongSwan, and OpenVPN.

PUNTOBLU



ASTARO: LA FORZA DELLA GUI IN UN PROGETTO OSS

The screenshot displays the Astaro Security Gateway V7 web administration interface. The browser window shows the URL `https://10.9.16.242:4444/`. The interface features a sidebar on the left with a navigation menu including 'Management', 'Network', 'Users', 'Definitions', 'Network Security', 'Web Security', 'Email Security', 'VoIP Security', 'IM/POP Security', 'Site-to-site VPN', 'Remote Access', and 'Logging'. The 'Network Security' section is expanded to show 'Packet Filter'. The main content area is titled 'Network Security > Packet Filter' and contains a 'Rules' section with tabs for 'ICMP' and 'Advanced'. A 'Create new rule' dialog box is open, showing fields for 'Group' (No group), 'Position' (Bottom), 'Source' (Any), 'Service' (Any), 'Destination' (Any), 'Action' (Allow), and 'Time Event' (All days). The rule list on the right shows several rules with columns for 'Edit', 'Delete', 'ID', 'Name', 'Source', 'Destination', and 'Service'. The rules are numbered 1 through 8 and include various network and user network entries.

ASTARO: LA FORZA DELLA GUI IN UN PROGETTO OSS

The screenshot displays the WebAdmin interface for the Astaro Security Gateway V7. The browser window shows the URL 'https://10.0.16.242:4444/'. The interface includes a navigation menu on the left with categories like Dashboard, Management, Network, Users, Definitions, Network Security, Web Security (selected), Email Security, VoIP Security, IM/P2P Security, Site-to-Site VPN, Remote Access, Logging, Reporting, and Support. The main content area is titled 'Web Security - HTTP Profiles' and contains an 'Overview' tab. A text block explains that proxy profiles can be used to create firewall policies. Below this is a diagram illustrating the flow from a 'Request' through a 'Proxy Profile' to 'Filter Assignments' and finally to 'Filter Actions'. The diagram shows a specific profile named 'Office LAN' with source IP '10.0.0/24' and type 'eDirectory auth'. This profile is assigned to three user groups: 'Sales Lunch' (Time: Lunch) leading to a 'Moderate' action, 'Sales' (Time: Always) leading to a 'Strict' action, and 'R&D' (Time: Always) leading to an 'Allow All' action. A 'Fallback Action' is also shown, leading to 'Allow Microsoft Update'.

La sicurezza delle reti LAN: Le soluzioni opensource.

Il ruolo dei Brand nello sviluppo

Dott. Matteo Lobbiani

ICT Specialist

lobbiani@punto blu.it

PUNTOBLU Srl

PUNTOBLU Srl

Via 1° Maggio, 4

Miralduolo di Torgiano

PERUGIA