

Sistemi di Elaborazione dell'Informazione (Sicurezza su Reti)
 Prof. A. De Santis
 A.A. 2003/2004

WEB APPLICATION SECURITY

PAROS

A cura di
Brignola Salvatore, Di Santo Valentina, Iazzetta Carla
 (056/101054) (056/101558) (056/100638)

SOMMARIO

- INTRODUZIONE
- NOZIONI DI RETI
 - Internet
 - Protocolli e Strati
 - TCP/IP
 - WWW, HTTP e HTTPS
 - Server Proxy
 - Cookie
- ATTACCHI AD UN SISTEMA IN RETE
- PAROS
 - Le Funzioni
 - Le Versioni
 - Installazione e Configurazione
 - Esempio di Scansione
 - Considerazioni
- APPENDICE
 - Funzioni Hash
 - Certification Authority
- BIBLIOGRAFIA

Sicurezza su Reti PAROS 2

INTRODUZIONE

- La sicurezza in ambienti d'inter-rete è un problema che merita particolare attenzione.
- I dati spesso passano attraverso sistemi intermedi non controllati.
- Possono essere intercettati e compromessi e i contenuti, quindi, non possono di certo essere considerati sicuri.
- Le organizzazioni stanno diventando sempre più dipendenti da applicazioni basate sul web.
- Gli attaccanti possono usare queste applicazioni come punti di ingresso per compromettere i dati.

Sicurezza su Reti PAROS 3

INTERNET

- La comunicazione "via Internet" è, oggi giorno, un aspetto fondamentale della nostra vita.
- Il **World Wide Web** contiene informazioni riguardanti una vastissima varietà di argomenti.
- **Internet** oggi significa:
 - 240.000 domini
 - 100.00 reti
 - 10.000.000 di calcolatori
- L'evoluzione di Internet è guidata dalla **Internet Society** responsabile dello sviluppo e della pubblicazione degli standard relativi a Internet.

Sicurezza su Reti PAROS 4

TCP/IP

- Un **Protocollo** è utilizzato nelle comunicazioni e costituisce l'insieme delle regole che governano lo scambio fra due entità.
- **TCP/IP** è stato sviluppato nel 1974 e raccoglie un vasto insieme di protocolli che sono stati pubblicati come standard di Internet.

APPLICAZIONE	←	Descrive la comunicazione tra processi su host differenti.
TRASPORTO (TCP)	←	Garantisce il corretto ordinamento dei pacchetti e la consegna affidabile dei dati.
INTERNETWORKING (IP)	←	Definisce il formato dei pacchetti e il meccanismo del loro instradamento.
ACCESSO ALLA RETE	←	Definisce le modalità di individuazione del destinatario e il tipo di servizio.
FISICO	←	Definisce tutti i dettagli relativi alla trasmissione.

Sicurezza su Reti PAROS 5

TCP/IP (2)

- Quando un'applicazione deve inviare dati, questi vengono passati al livello inferiore, fino a raggiungere la rete fisica sottostante.

Sicurezza su Reti PAROS 6

WWW, HTTP e HTTPS

- La più nota applicazione che utilizza TCP/IP è **WWW** (World Wide Web).
- Il protocollo usato per la comunicazione tra browser e un server Web è noto come **HTTP**.
- **SSL** è un protocollo sviluppato da *Netscape*.
- Come ovvia conseguenza alla standardizzazione di tale protocollo nasce **HTTPS**, che è il normale protocollo HTTP con il supporto sottostante di SSL.

SERVER PROXY

- Svolge un importante ruolo nell'architettura Web, perché ottimizza i tempi di latenza e il carico sui server.
- Un proxy si interpone tra i client e la rete Internet, tutelando gli stessi da eventuali attacchi esterni.
- Intercetta le richieste che arrivano dai client per procurare le pagine HTML e replicarle in locale.
- Permette di accedere ad un servizio senza mostrare il personale IP address: fornisce anonimata.



SERVER PROXY (2)

- Per un maggior grado di sicurezza si possono concatenare più server proxy.
- Concatenare più proxy vuol dire arrivare al sito di interesse passando per vari proxy: solo il primo proxy della catena conosce la vera identità del client.
- La concatenazione deve essere effettuata in questo modo:
<http://Proxy1:Porta1/http://Proxy2:Porta2/http://www.Sito.it/>

COOKIE

- Rappresentano un sistema che può essere utilizzato da connessioni lato server per memorizzare e/o recuperare informazioni sul lato client della connessione.
- Permettono al sito che li utilizza di essere più efficiente.
- Un cookie è costituito da una coppia **NAME / VALUE** che si può considerare come una variabile e da una data di scadenza, **EXPIRES**, oltre la quale si autoelimina.
- Ad ogni cookie sono associati anche un **DOMAIN** (domino) ed un **PATH** (percorso).

ATTACCHI AD UN SISTEMA IN RETE

- L'accesso ad un sistema è consentito solo:
 - se si utilizzano gli opportuni protocolli di comunicazione;
 - se si è autorizzati,
 - mediante procedure di riconoscimento(password, smartcard).
- Un sistema sicuro garantisce:
 - riservatezza e integrità dei dati;
 - funzionalità e affidabilità del servizio e delle macchine.
- Le password ed altri strumenti di riconoscimento possono essere scoperti o falsificati da malintenzionati.
- Molti software per la gestione dei servizi di rete possono presentare comportamenti anomali, utilizzabili per accedere illegalmente alle macchine.

ATTACCHI AD UN SISTEMA IN RETE (2)

Ecco alcuni dei principali attacchi a cui un sistema in rete può essere sottoposto

- **Denial of Service (DoS)**
 - Può mandare in crash il sistema rendendo così necessario un reboot delle macchine.
 - Yahoo!* è stato il primo a subirlo, avendo riportato un blackout di tre ore domenica 6 febbraio 2000.
- **Buffer Overflow**
 - Usato per "iniettare" codice estraneo nella memoria del computer vittima.
 - Sfrutta i bug noti nella gestione della memoria dati dei programmi.

ATTACCHI AD UN SISTEMA IN RETE (3)

- **Sniffing**
 - Un malintenzionato potrebbe accedere a dati riservati semplicemente mettendosi in ascolto sulla rete.
 - Si può rendere incomprensibile il risultato dello sniffing mediante la cifratura dei dati.
- **Man-In-The-Middle (MITM)**
 - Il traffico generato durante la comunicazione tra due host, viene dirottato verso un terzo host (*attaccante*).
 - L'attaccante riceve tutto il traffico prodotto dai due host.
 - Potrebbe consultare e modificare le informazioni catturate.

ATTACCHI AD UN SISTEMA IN RETE (4)

- **Cross Site Scripting (XSS)**
 - Permette ad un malintenzionato di inserire codice arbitrario come input di un'applicazione web.
- **SQL injection**
 - Attacco particolarmente legato al web.
 - Colpisce il cuore dell'applicazione web: il database.
 - **CRLF injection** (detto anche **Cookie Tampering**): tecnica di SQL injection, dove il codice arbitrario è inserito nei cookie.
- **Parameter Tampering**
 - Letteralmente: *Falsificazione dei parametri*.
 - L'attaccante può modificare i parametri che rendono sicure determinate operazioni.

PAROS

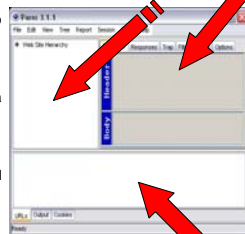
- Creato dai progettisti di **ProofSecure.com** (<http://www.parosproxy.org>)
- Open source
- Freeware
- Scritto interamente in java (portabile)
- Applicazione robusta e potente
- Lavora da proxy (man-in-the-middle) tra web server e browser del client.

PAROS (2)

- Permette di intercettare, visualizzare e modificare dati HTTP e HTTPS, al volo, scambiati tra server e client, inclusi cookie e campi form.
- Supporta:
 - *Certificati client*;
 - *Catene di proxy*;
 - *Filtraggio dei pacchetti*;
 - *Scansione intelligente delle vulnerabilità delle applicazioni web*.
- La versione che abbiamo analizzato è la **3.1.3** per Windows, che abbiamo provato su una macchina con processore *PIV 2.4 GHz* con *512 Mb* di memoria *RAM*, su cui è installato *Microsoft Windows XP Professional*.

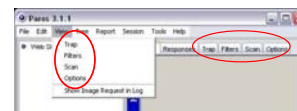
LE FUNZIONI

- **A sinistra:** gerarchia dei siti web visitati.
- **A destra:** gestione interazione tra proxy e utente.
- **In basso:** comportamento del proxy.



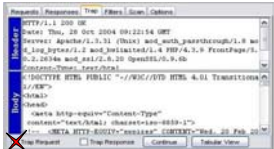
LE FUNZIONI: MENU' VIEW

- Il menu View contiene le fondamentali funzionalità di Paros.
- Sono specificate anche sulla finestra di destra.



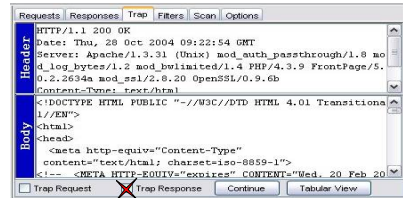
LE FUNZIONI: TRAP

- Mediante il **Trapping**, Paros intercetta richieste/risposte HTTP, consentendone la modifica.
- TRAP DELLE RICHIESTE**
 - Abilitando la casella "trap Request".
 - Tutte le richieste saranno trattenute.
 - Possono essere modificati i contenuti delle aree di testo Header/Body.



LE FUNZIONI: TRAP (2)

- TRAP DELLE RISPOSTE**
 - Abilitando la casella "Trap Response".
 - Tutte le risposte saranno trattenute.
 - Possono essere modificati i contenuti delle aree di testo Header/Body.



LE FUNZIONI: FILTERS

- I filtri vengono usati per scoprire la presenza di pattern predefiniti nei messaggi HTTP e avvertire l'utente a riguardo.
- Tenere traccia delle informazioni alle quali è interessato l'utente, ad esempio, i cookie.



LE FUNZIONI: FILTERS (2)

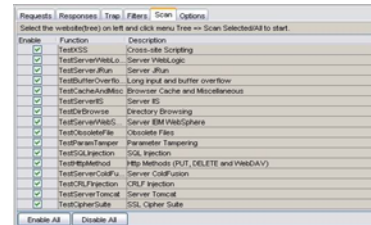


LE FUNZIONI: FILTERS (3)



LE FUNZIONI: SCANNER

- Consente di esaminare i server tramite la gerarchia dei siti web.
- Ricerca malfunzionamenti e vulnerabilità a particolari tipologie di attacchi da parte di malintenzionati.



LE FUNZIONI: SCANNER (2)

Durante una scansione, Paros è in grado di controllare:

- se l'applicazione web è vulnerabile a: Cross Site Scripting (XSS), Parameter Tampering, SQL injection, Buffer overflow, CRLF injection (o Cookie Tampering);
- vulnerabilità specifiche di vari application server come *WebLogic*, *Jrun*, *IIS*, *IBM WebSphere*, *ColdFusion*, *Tomcat*;
- la gestione della cache del browser;

LE FUNZIONI: SCANNER (3)

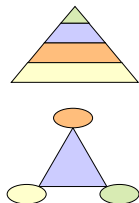
Durante una scansione, Paros è in grado di controllare:

- se le directory del server possono essere attraversate e se esistono file obsoleti;
- se i metodi *PUT* e *DELETE* sono supportati dal server in questione e, in generale, se sono supportati i metodi introdotti dallo standard WebDAV;
- quali caratteristiche della *Cipher Suite* SSL permette di stabilire l'applicazione web.

LE FUNZIONI: SCANNER (4)

■ La scansione può essere effettuata:

- su tutta la gerarchia dei siti (Tree/scan all).
- su un solo sito web nell'albero (Tree/scan selected node).



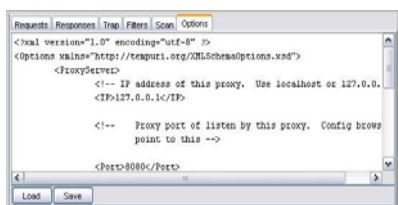
LE FUNZIONI: SCANNER (5)

■ Al termine di una scansione, lo Scanner produce un rapporto che viene memorizzato in un file HTML, consultabile in qualsiasi momento.

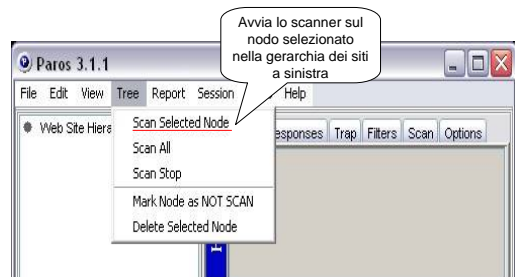
- Nel report, vengono riportati:
 - numero di "alert" riscontrati, con corrispondente livello di rischio;
 - breve descrizione di ogni problema riscontrato;
 - per qualche problema, un suggerimento per la soluzione.
- ***E' da questo file che bisogna partire per risolvere gli eventuali problemi riscontrati in una applicazione web.***

LE FUNZIONI: OPTIONS

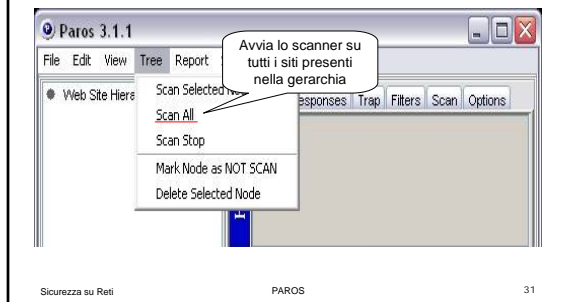
■ La finestra contiene un file XML che specifica le impostazioni di default del Proxy (che eventualmente possono essere modificate).



LE FUNZIONI: MENU' TREE



LE FUNZIONI: MENU' TREE (2)

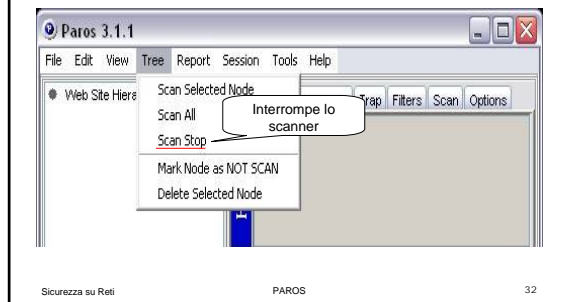


Sicurezza su Reti

PAROS

31

LE FUNZIONI: MENU' TREE (3)

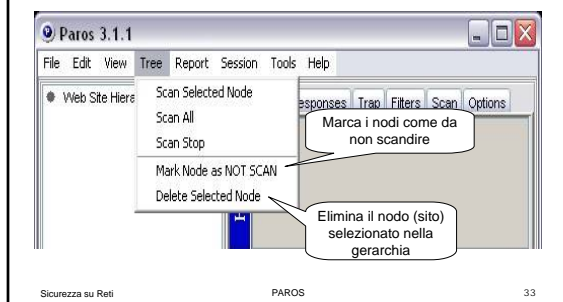


Sicurezza su Reti

PAROS

32

LE FUNZIONI: MENU' TREE (4)



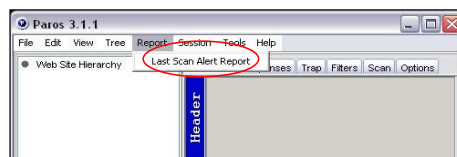
Sicurezza su Reti

PAROS

33

LE FUNZIONI: MENU' REPORT

- Per conoscere l'ultimo report generato dallo scanner: *Report/Last Scan Alert Report* (visualizza il report in una pagina web).



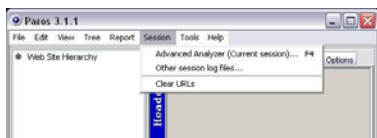
Sicurezza su Reti

PAROS

34

LE FUNZIONI: MENU' SESSION

- Advanced Analyzer**
 - Avvia l'analizzatore del file log della sessione corrente.
- Other session log files**
 - Avvia l'analizzatore del file log di una sessione a scelta dell'utente.
- Clear URLs**
 - Svuota la lista visualizzata nella finestra in basso dell'interfaccia (non cancellandola dai file log di sessione).



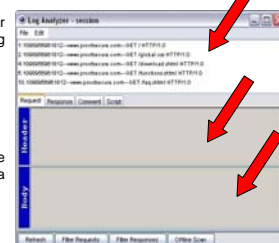
Sicurezza su Reti

PAROS

35

LE FUNZIONI: LOG ANALYZER

- La finestra in alto del Log Analyzer mostra il contenuto del file log selezionato.
- Le finestre in basso eseguono le stesse funzioni dell'interfaccia iniziale di Paros, ma offline.



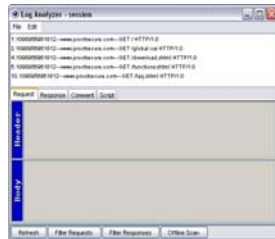
Sicurezza su Reti

PAROS

36

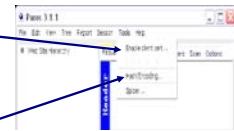
LE FUNZIONI: LOG ANALYZER (2)

- Refresh
 - Ripulisce la finestra di output da eventuali operazioni effettuate.
- Filter Requests
 - Filtra il contenuto del file log relativo alle richieste sulla base di uno specifico pattern inserito dall'utente.
- Filter Responses
 - fa lo stesso ma con le risposte.
- Offline Scan
 - avvia lo scanner sul file di log (scansione offline).



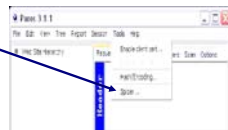
LE FUNZIONI: MENU' TOOLS

- Abilita il supporto ai certificati client che alcune applicazioni web potrebbero richiedere.
- Converti dati in differenti formati di codifica/hash, incluso Base64, MD5 e SHA1.



LE FUNZIONI: SPIDER

- Consente di esplorare siti web in modo da raccogliere e memorizzare più link URL possibili, senza navigare effettivamente questi siti.
- Supporta cookie e catene di proxy.
- Tutti i link "catturati" vengono memorizzati nell'albero gerarchico dei siti web, utilizzabile dallo Scanner.



LE VERSIONI

- Agosto 2002
 - Prima versione, 1.0.
 - Permette agli utenti di intercettare richieste/risposte sia HTTP che HTTPS (*Trapping*).
- Dicembre 2002
 - Rilasciata la versione 2.0.
 - Completamente riscritta l'interfaccia GUI e il motore di proxy.
 - Aggiunti:
 - vista ad albero per mostrare la gerarchia dei siti web;
 - Scanner, Filter.
- Aprile 2003
 - Rilasciata la versione 2.1.
 - Supporta i certificati client.
 - Perfezionato lo Scanner.
 - Aggiunti:
 - controlli sulla vulnerabilità, filtri per memorizzare richieste GET/POST;
 - funzione Hash e conversione Base64.

LE VERSIONI (2)

- Giugno 2003
 - Rilasciata la versione 2.2.
 - Supporta connessioni HTTP 1.1.
 - Scansione per la vulnerabilità al *Cross Site Scripting* (XSS) del sito web selezionato dopo la navigazione.
 - Rimozione siti web dalla vista ad albero.
 - Aggiunta la funzionalità *Spider*.
 - Rilascio versione 3.0: l'unica differenza è nella licenza (*Clarified Artistic License*).
- Settembre 2003
 - Rilasciata la versione 3.0.1.
 - Corretto e migliorato il controllo sul *Cross Site Scripting*.
 - Aggiunto il controllo per l'*SQL injection*.

LE VERSIONI (3)

- Ottobre 2003
 - Rilasciata la versione 3.0.2.
 - Migliorato il controllo sull'*SQL injection* e aggiunti ulteriori controlli e filtri.
 - Rilascio versione 3.0.2b: risolto bug nell'uso delle catene di proxy.
- Novembre 2003
 - Rilasciata la versione 3.0.2c: risolto bug in una conversione e migliorato il supporto per alcune URI non standard.
- Dicembre 2003
 - Rilasciata la versione 3.0.3.
 - Apportate ulteriori modifiche al controllo per l'*SQL injection* e aggiunti altri controlli.
 - Ridotti i thread che eseguono lo scanning a 5.
 - Corretti dei bug.

LE VERSIONI (4)

■ Gennaio 2004

- Rilasciata la versione 3.1.
- Corretta memorizzazione (ora in piccoli file) di richieste/risposte HTTP.
- Aggiunta vista avanzata:
 - facile navigazione;
 - semplice filtraggio dei log.
- Supporta la scansione off-line.
- Vengono generati rapporti di scansione in formato HTML:
 - livelli di rischio;
 - descrizioni;
 - soluzioni.
- Supporta la modifica del numero di thread da usare.
- Aggiunti considerevoli controlli allo Scanner.
- Corretti ulteriori bug.

LE VERSIONI (5)

■ Marzo 2004

- Rilasciata la versione 3.1.1.
- Aggiunta la voce *encoder/decoder* al menù.
- Aggiunti pannelli di visualizzazione commenti e script nel *Log Analyzer*.
- Aggiunti altri due filtri e corretti altri bug.

■ Aprile 2004

- Rilasciata la versione 3.1.2.
- Nuovo filtro: *DetectUnsafeContent*
 - individua e visualizza nella finestra di Output particolari contenuti non sicuri.
- E' possibile svuotare la lista dei link URL anche mediante il menù di scelta rapida.
- E' possibile svuotare anche tutte le finestre mediante una nuova funzione, *Clear Current Session*.

LE VERSIONI (6)

■ Agosto 2004

- Rilasciata la versione 3.1.3.
- Scansione anche di una singola richiesta, tra quelle mostrate nella lista dei link URL in basso.
- Possibilità di poter rispedita una particolare richiesta (mediante il comando *Re-send*).
- Nuova utility: *Send HTTP(S) Request*
 - costruire una richiesta HTTP(S) a proprio piacimento e spedirla ad una particolare URL.
- Aggiunti ulteriori controlli di vulnerabilità e corretti bug.

La nostra analisi si è concentrata su quest'ultima versione.

INSTALLAZIONE E CONFIGURAZIONE

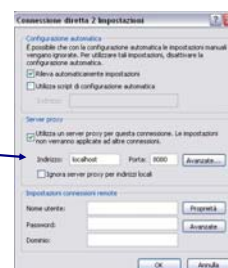
- Assicurarsi che *JRE 1.4* (o superiore) sia installato.
- Sul sito della ProofSecure.com (<http://www.parosproxy.org>) è reperibile sia la versione per Windows che quella per i sistemi Unix-like di Paros.
- **Windows**
 - Seguire le istruzioni nel programma d'installazione;
 - cliccare sul collegamento sul desktop o dal menù (*Start*) di Windows, per lanciare il programma.
- **Unix-like**
 - Scompattare tutti i file in una nuova directory manualmente;
 - cliccare sul file *.jar* per lanciare il programma.

INSTALLAZIONE E CONFIGURAZIONE (2)

- Bisogna fare in modo che il PC su cui viene installato acceda a Internet attraverso il proxy Paros:
 - impostare il browser web in modo che stabilisca una connessione con l'IP del proxy (e la porta che quest'ultimo utilizza).
- Paros utilizza due porte
 - **8080 per la connessione proxy** (in chiaro)
 - **8443 per gestire connessioni SSL** (usata automaticamente).
- Assicurarsi che le due porte non siano usate da altre applicazioni.

INSTALLAZIONE E CONFIGURAZIONE (3)

- Aprire un browser web e specificare di voler utilizzare un server proxy, nelle opzioni del browser.
- Inserire come nome proxy "localhost" e come porta proxy "8080".
- La porta 8443 è usata automaticamente da Paros: non dobbiamo preoccuparcene noi.



INSTALLAZIONE E CONFIGURAZIONE (4)

- Lanciare il programma e controllare se vengono visualizzati messaggi di errore durante l'inizializzazione.
- Aprire la finestra "Options".
- Viene mostrato il contenuto del file "options.xml" che contiene le impostazioni di default del proxy.
- In questa finestra, si possono modificare i vari parametri mostrati, a proprio piacimento:
 - IP del proxy;
 - porte del proxy;
 - numero di thread assegnati allo scanner;
 - abilitare le catene di proxy.

Sicurezza su Reti

PAROS

49

INSTALLAZIONE E CONFIGURAZIONE (5)

```
<?xml version="1.0" encoding="utf-8" ?>
<Options xmlns="https://paros.i.org/MSSchemaOptions.xsd">

  <ProxyServer>
    <IP>127.0.0.1</IP> <!-- IP address of this proxy. Use localhost if 127.0.0.1 -->
    <Port>8080</Port> <!-- Proxy port of listen by this proxy. Config browser to point to this -->
    <SSL>443</SSL> <!-- Internal SSL proxy port used by this proxy -->
  </ProxyServer>

  <ProxyChain>
    <Chain></Chain> <!-- Use blank "Chain" if no proxy chain to use -->
    <Start></Start>
    <Stop></Stop>
  </ProxyChain>

  <Scanner>
    <ThreadSc/Thread>
    </ThreadSc/Thread>
  </Scanner>
</Options>
```

Sicurezza su Reti

PAROS

50

ESEMPIO DI SCANSIONE

- Impostiamo il browser in modo da stabilire una connessione con l'IP del proxy Paros (che lanceremo sulla nostra macchina, quindi il suo IP è 127.0.0.1).
- Lanciamo il software e connettiamo la nostra macchina ad Internet.
- Avviamo lo **Spider** sull'indirizzo:
<http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/>

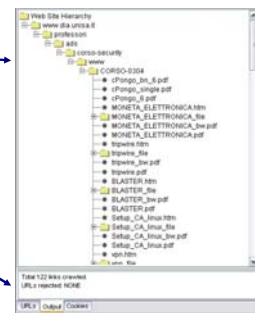
Sicurezza su Reti

PAROS

51

ESEMPIO DI SCANSIONE (2)

- Gerarchia costruita dallo Spider



- Risultato dello Spider: numero dei link raccolti ed eventuali link che non è riuscito ad attraversare.

Sicurezza su Reti

PAROS

52

ESEMPIO DI SCANSIONE (3)

- Se clicchiamo sulla finestra **URLs**, in basso, vengono mostrare le richieste effettuate dallo Spider, le risposte ricevute dal server e i relativi tempi di risposta.

```
1: GET http://www.dia.unisa.it/ HTTP/1.1 200 OK [0.11 s]
11: GET http://www.dia.unisa.it/professori/professori.php HTTP/1.1 200 OK [0.22 s]
17: GET http://www.dia.unisa.it/professori/ads HTTP/1.1 301 Moved Permanently [0.05 s]
18: GET http://www.dia.unisa.it/professori/ads HTTP/1.1 200 OK [0.16 s]
22: GET http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/ HTTP/1.1 200 OK [0.28 s]
```

Sicurezza su Reti

PAROS

53

ESEMPIO DI SCANSIONE (4)

- Proviamo ad avviare lo **Scanner** su un nodo nella gerarchia, ad esempio su **CORSO-0304**.
- L'output dello Scanner viene visualizzato nella finestra **Output**, in basso.

```
Scanning using 4 thread(s).
Running scanner...
Testing Cross-site Scripting...
Testing Server Headers...
Testing Server IP/URL...
Testing Long read and buffer overflow...
Testing Browser Cache and Miscellaneous...
Informational: (Name) - Server header info
URL: http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/
Parameter:
-----
Testing Server EE...
Testing Directory Browsing...
Testing Server EMailOptions...
Testing Occulte Files...
Testing Parameter Tampering...
Testing CGI Function...
Testing Http Methods (PUT, DELETE and TRACE)...
Method not (Supported) - HTTP methods
URL: http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/
Parameter:
-----
URLs | Output | Cookies
```

Sicurezza su Reti

PAROS

54

ESEMPIO DI SCANSIONE (5)

- Il report generato verrà organizzato in un file HTML.
- In una prima parte di questa pagina, viene riportato un sommario: numero di alert riscontrati per ogni livello di rischio (*high, medium, low, informational*).
- Successivamente, vengono riportati tutti gli alert, raggruppati per livello di rischio. Per ognuno di essi viene riportato:
 - una descrizione;
 - l'URL che lo ha generato;
 - eventuali parametri, informazioni e riferimenti;
 - una possibile soluzione al problema.

ESEMPIO DI SCANSIONE (6)

Power Formatting Report
This report was generated at 11/02/2015 4:00:33M

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	89
Low	0
Informational	1

Alert Detail

Method (High/Low): HTTP methods

Description: HTTP method such as PUT, DELETE, HEAD/GET etc. appeared to exist as indicated by the OPTIONS method. However, this may be a false positive as they can be hidden by other means.

URL: http://www.dla.unica.it/professionista/risorse-security/news/CORSO-03&introduzione_halfpage.htm

Parameter:

Other information: PUT, DELETE

Solution: Disable PUT/DELETE/HEAD/GET support. For ID, disable HEAD/GET if not required as in reference. Unnecessary method can also be filtered using IDS/IPS.

Reference: http://support.microsoft.com/default.aspx?ks=754924538

Method (High/Low): HTTP methods

Description: HTTP method such as PUT, DELETE, HEAD/GET etc. appeared to exist as indicated by the OPTIONS method. However, this may be a false positive as they can be hidden by other means.

URL: http://www.dla.unica.it/professionista/risorse-security/news/CORSO-03&introduzione_halfpage.htm

Parameter:

Other information: PUT, DELETE

Solution: Disable PUT/DELETE/HEAD/GET support. For ID, disable HEAD/GET if not required as in reference. Unnecessary method can also be filtered using IDS/IPS.

CONSIDERAZIONI

- Tool utile ad identificare e attenuare i livelli di rischio, riscontrabili durante l'attività on-line.
- Open-source e portatile: chiunque può utilizzarlo senza alcun dispendio economico e da qualsiasi piattaforma.
- L'applicazione è robusta, potente, corredata di una buona interfaccia GUI e di un potente motore di proxy.

CONSIDERAZIONI (2)

DUE UTILIZZI:

- Lecito**
 - Tutela privacy.
 - Filtraggio pacchetti.
 - Scansione vulnerabilità.
 - Controlla la presenza di contenuti non sicuri.
- Illecito**
 - Sniffing pacchetti con cattura password.
 - Inserimento di codice maligno.
 - Modifica chiavi pubbliche scambiate all'inizio di una connessione.

CONSIDERAZIONI (3)

- Paros è destinato a collocarsi tra i più potenti tool di scansione.
- I progettisti continuano a lavorarci assiduamente: rilasciano nuove versioni con sempre maggiori funzionalità, a brevi lassi di tempo.
- Per poterlo usare è richiesta un'approfondita conoscenza:
 - su come lavorano le applicazioni web.
 - su come i vari livelli di vulnerabilità delle applicazioni si manifestano e su come questi possono essere utilizzati.

CONSIDERAZIONI (4)

- Il sito ufficiale, non fornisce particolari informazioni a riguardo delle problematiche affrontate da Paros e delle sue funzionalità.
- L'uso improprio potrebbe mandare in crash il sistema o causare piccoli danni alle reti.

APPENDICE

- Funzioni Hash
- Certification Authority

FUNZIONI HASH

- Il valore hash $h(M)$ è una rappresentazione **non ambigua e non falsificabile** di un messaggio M , facile da calcolare e tale da **comprimere** il messaggio stesso.
- **Proprietà**
 - Sicurezza forte
 - Sicurezza debole
 - One-way
- **Utilizzi:**
 - Firme digitali
 - Timestamping
 - MAC (Message Authentication Code)

CERTIFICATION AUTHORITY

- Chi assicura che una chiave pubblica è effettivamente quella di una determinata entità?
- E' necessario un documento che leghi inequivocabilmente il proprietario della chiave pubblica con la stessa: il **certificato digitale**.
- Non è possibile pensare che un singolo possa distribuire il proprio certificato: si ricorre ad una **Autorità di Certificazione (CA, Certification Authority)**.

CERTIFICATION AUTHORITY (2)

- Una **CA** è una terza parte credibile (**TTP, Trusted Third Part**), incaricata di:
 - rilascio dei certificati e verifica dell'identità richiedente;
 - mantenimento della "lista di revoca dei certificati" (**CRL, Certificate Revocation List**), dove sono conservati i certificati non validi.
- Può emettere un certificato anche per un'altra CA, in modo da creare catene gerarchiche di certificati.
 - In cima alla gerarchia c'è una **RootCA**.

CERTIFICATION AUTHORITY (3)

- **Uno degli standard più utilizzati per la struttura dei certificati è X.509**
 - nome del richiedente
 - periodo di validità del certificato
 - nome dell'autorità che lo ha rilasciato
 - numero di serie
 - chiave pubblica del richiedente
 - firma digitale (ottenuta tramite cifratura di quanto sopra con la chiave privata della CA).
- Tra i certificati più usati: Certificato Client, Certificato Server, Certificati di email, Certificati di applicazioni, Certificato della Autorità di Certificazione.

BIBLIOGRAFIA

- Struttura di Internet, suite TCP/IP, HTTP e HTTPS, Server Proxy e Cookie:
 - Douglas E. Comer, "Internetworking con TCP/IP, Principi, protocolli e architetture", Addison Wesley, 2002;
 - W. Richard Stevens, "TCP/IP Illustrated Volume 1", Addison Wesley, 2001;
 - W. Stallings, "Trasmissione Dati e Reti di Computer", Jackson Libri, 2000.
- Ulteriore materiale riguardante HTTP, HTTPS e Internet in generale:
 - www.ietf.org (Internet Engineering Task Force)
 - www.w3.org (World Wide Web Consortium)
 - <http://openskills.info/index-it.php>
- Significativa può essere la consultazione della [RFC2616](https://www.rfc-editor.org/rfc/rfc2616) che definisce lo standard HTTP/1.1.

BIBLIOGRAFIA (2)

- Struttura e gestione dei Server Proxy:
 - <http://www.gnomixland.com> (tratta anche la Sicurezza in generale)
 - Lista frequentemente aggiornata dei Server Proxy disponibili on line:
<http://www.atomintersoft.com/products/alive-proxy/proxy-list/>
- Informazioni sulla Sicurezza Informatica (tecniche di Crittografia, Firme Digitali, Certificati Digitali, attacchi informatici, etc...):
 - <http://www.rsasecurity.com/> (*RSA Security*)
 - <http://www.cert.org/> (*CERT Coordination Center*)
 - <http://www.bsa.org/italias/> (*Business Software Alliance*)
 - <http://www.issa.org/> (*Information Security Systems Association*)
 - <http://www.ftc.gov/> (*Federal Trade Commission*)
 - <http://security.itworld.com>
 - <http://www.puntosicuro.it> (*articoli e dati statistic*)
 - <http://sicurezza.html.it/index.asp>
 - <http://www.sicurezzainrete.com>
 - <http://www.tonycrypt.com/>
 - <http://www.gxware.org/>

BIBLIOGRAFIA (3)

- Articoli, recensioni e varie informazioni su Paros:
 - <http://www.securityfocus.com/>
 - http://security.itworld.com/hl/security_strat/03022004/
 - <http://www.blacksheepnetworks.com/>
 - <http://lists.jammed.com/>
- Riferimenti ufficiali di Paros: <http://www.parosproxy.org> e contact@parosproxy.org