



Vincenzo De Cesare matr.56/100463
Luana Garofalo matr.56/00434
Antonia Motta matr.53/10752
Vincenzo Ragone matr.56/00307

Cos'è Retina

- ◆ Retina è uno scanner per la sicurezza della rete, realizzato nel 1998 dalla Eye Digital Security.
- ◆ Retina rompe gli schemi tipici degli scanner per la sicurezza mediante l'uso dell' AI.

Cosa fa?

- ◆ Retina conduce una ricerca delle vulnerabilità, utilizzando una metodologia di tipo hacker per sfruttare gli errori di configurazione e le debolezze insite nei protocolli e negli applicativi utilizzati.

Cosa fa?

- ◆ Attraverso un'analisi puntuale delle macchine target, Retina è in grado di:
 - identificare e segnalare le vulnerabilità della sicurezza;
 - suggerire le modifiche del caso e soprattutto
 - evidenziare possibili "buchi" che potrebbero rappresentare una debolezza futura per il sistema.

Scanning delle vulnerabilità

- ◆ Processo di controllo di tutti i potenziali metodi di attacco per la violazione di una rete, basato sull'analisi dei tipi di software e di configurazioni presenti su una certa rete.
- ◆ Fornisce ad una rete gli strumenti necessari per potersi difendere.

Cosa fornisce?

- ◆ Una serie di tool di report facili da usare per identificare ed isolare i problemi con priorità più alta, consentendo un controllo globale sulle verifiche della sicurezza della rete.

Caratteristiche

Retina è stata progettata per:

- ◆ identificare e avvisare gli utenti delle potenziali vulnerabilità della sicurezza;
- ◆ suggerire, "fissare" e fare rapporti su eventuali buchi nella sicurezza di un sistema di rete;
- ◆ fornire alla rete l'analisi di sicurezza più completa possibile.

Vulnerabilità dei sistemi/servizi

Retina comprende dei moduli per la verifica delle vulnerabilità dei seguenti sistemi e servizi:

- ◆ **NetBIOS (Network Basic Input Output System):** programma che consente ad applicazioni su diversi computer di comunicare tramite un'area locale di rete (LAN).
- ◆ **HTTP :** protocollo di trasferimento di ipertesti usato per la distribuzione delle pagine web attraverso internet.

Vulnerabilità dei sistemi/servizi

- ◆ **CGI e WinCGI:**
semplice interfaccia per eseguire programmi esterni, software o gateway, sotto un information server (quali i server HTTP), indipendentemente dalla piattaforma.
- ◆ **FTP:**
Protocollo per il trasferimento dei file dal computer al server o viceversa.
- ◆ **DNS (Domain Name System):**
Servizio che fornisce corrispondenze di nomi delle reti per gli indirizzi IP.

Vulnerabilità DoS

- ◆ **Vulnerabilità DoS (Denial of Service):**
un attacco DoS è un attacco remoto tendente a saturare la capacità dei server, tutte le connessioni disponibili per un particolare servizio o addirittura mandare in crash il sistema.

Attacchi DoS: come proteggersi?

- ◆ disabilitare tutte le porte TCP/UDP non necessarie.
- ◆ eseguire frequenti simulazioni di attacco.
- ◆ disabilitare tutti i servizi, i protocolli ed i programmi che non sono assolutamente necessari.
- ◆ prima di utilizzare un nuovo prodotto, assicurarsi della compatibilità (in termini di sicurezza) con il S.O.

Vulnerabilità dei sistemi/servizi

- ◆ **POP, SMTP e LDAP**
POP (Post Office Protocol):
protocollo progettato per consentire agli host di un singolo utente di leggere la posta da un server.
- SMTP (Simple Mail Transfer Protocol) :**
protocollo usato per trasferire posta elettronica tra computer. E' un protocollo "server to server" , quindi sono necessari altri protocolli per accedere ai messaggi.
- LDAP (Lightweight Directory Access Protocol):**
protocollo di rete utilizzato dai server di posta elettronica per gestire le liste degli utenti e degli indirizzi di posta elettronica dei server.

Vulnerabilità dei sistemi/servizi

◆ TCP/IP e UDP

TCP/IP Protocol Suite :

Protocollo per il controllo delle trasmissioni su protocollo Internet.

UDP (User Datagram Protocol):

protocollo internet a strati per il trasporto.

Vulnerabilità dei sistemi/servizi

◆ Firewall e Routers

FIREWALL: viene usato per limitare l'accesso ad alcune parti di una rete o addirittura all'intera rete.

ROUTER: sistema responsabile delle decisioni riguardanti quali percorsi di rete seguire.

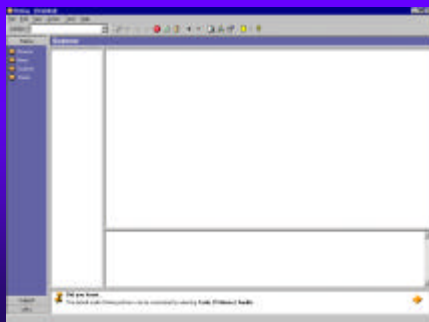
Componenti

- ◆ GUI - Interfaccia Grafica Utente
- ◆ CHAM – Metodi comuni di attacco
- ◆ Tecnologia FIX-IT
- ◆ Moduli plug.in
- ◆ Auto-update

GUI: Interfaccia Grafica Utente

- ◆ Retina contiene un'interfaccia utente molto simile a quella di un browser internet, facile da usare, che consente di controllare tutti gli aspetti dello scanning e del reporting.

Interfaccia all'avvio di Retina

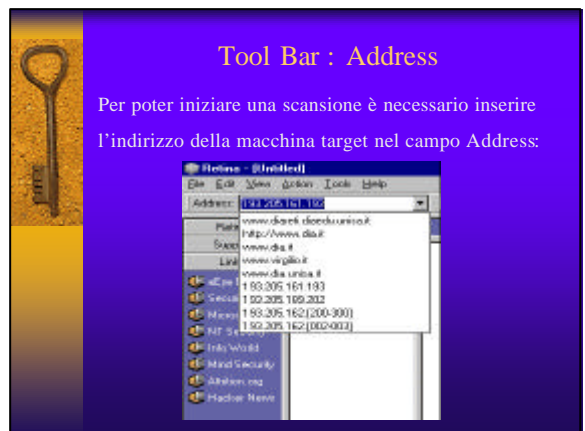
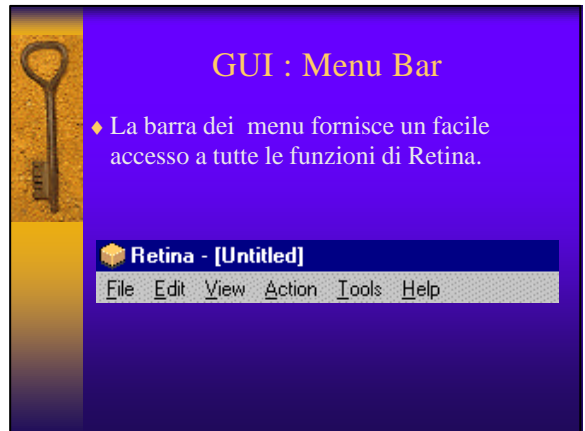
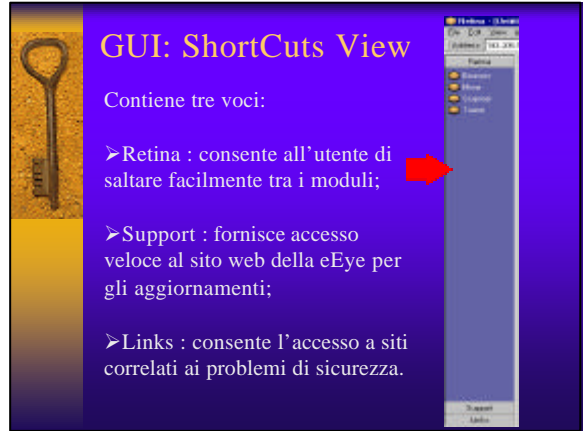
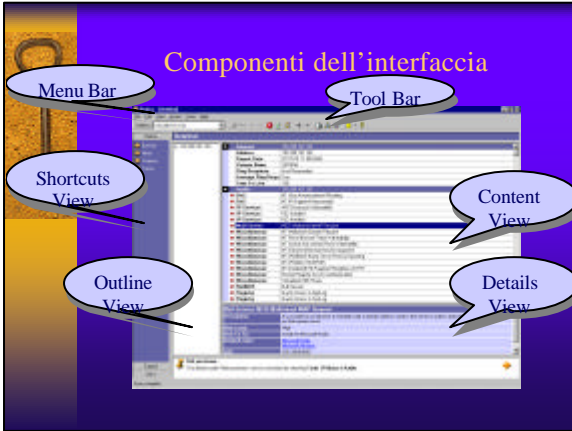


GUI: componenti

Elenchiamo di seguito le varie componenti dell'interfaccia, che conferiscono a quest'ultima un'estrema semplicità di utilizzo:

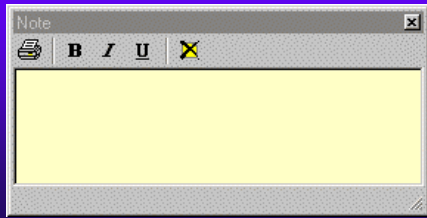
- ◆ Shortcuts View
- ◆ Menu Bar
- ◆ Tool Bar
- ◆ Content View
- ◆ Outline View
- ◆ Details View
- ◆ Options Dialog
- ◆ Policies Dialog

Visualizziamo nella figura seguente alcune delle componenti citate.



Tool Bar : editor Note

Caratteristica che funziona come un Note Pad digitale.

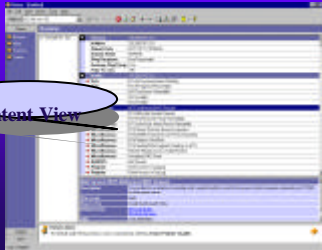


Tool Bar : Help On-line



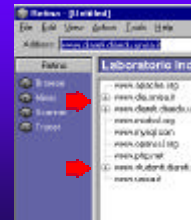
GUI : Content View

Schermata principale usata dai moduli Scanner, Miner e Tracer per visualizzare le informazioni raccolte e dal modulo Browser come finestra di browser web.



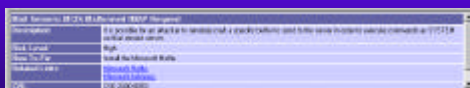
GUI: Outline View

La finestra di Outline fornisce una visione organizzata dei dati attraverso un albero, che si può espandere o collassare:



GUI: Details View

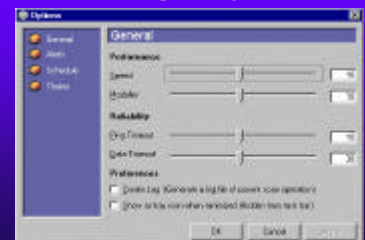
La finestra Details fornisce informazioni specifiche e dettagliate, che varieranno a seconda del modulo attualmente in uso.



GUI: Options Dialog

Consente all'utente di personalizzare varie impostazioni di Retina, quali l'esecuzione, i segnali di allarme e il tema, tramite le opzioni seguenti:

- General
- Alerts
- Schedule
- Theme



General Option|Performance

- ◆ **General Option | Performance | Speed:**
specifica il numero dei processi che i moduli possono utilizzare; più alto è il numero, più veloce sarà la scansione, anche se saranno necessarie più risorse.
- ◆ **General Option | Performance | Modules:**
permette di controllare il numero di macchine analizzate contemporaneamente specificando il numero di moduli eseguiti contemporaneamente; anche in questo caso, la specifica di più moduli richiederà più risorse.

General Options|Reliability

- ◆ **General Option | Reliability | Ping Timeout:**
permette di controllare per quanto tempo Retina aspetterà una risposta dalla macchina che sta tentando di contattare; questa variabile può essere modificata per compensare i problemi di congestione della rete.
- ◆ **General Option | Reliability | Data Timeout:**
permette di controllare per quanto tempo Retina aspetterà una risposta, se il trasferimento di alcuni dati si è bloccato.

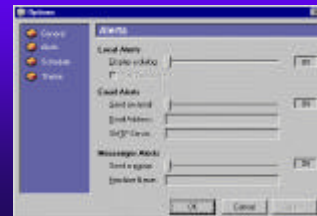
General Options|Preferences

- ◆ **General Option | Preferences | Create Log:**
Il controllo di quest'opzione permetterà a Retina di creare un file di log di tutti i casi che si verificano in una scansione. Questo file viene usato, generalmente, per il debug.
- ◆ **General Option | Preferences | Tray Icon:**
L'attivazione di quest'opzione nasconderà Retina dalla task bar di Windows, quando Retina è minimizzato. Un' icona del programma risiederà, invece, sul desktop.

Alerts Options

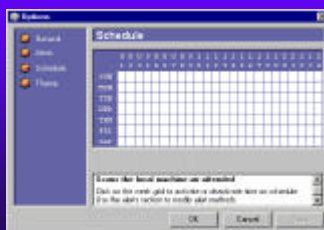
Permette la selezione di certi eventi di notifica per le scansioni schedate di Retina. Le possibili notifiche sono:

- ◆ **Local Alerts:** notifica alfa-numerica con eventuale suono aggiuntivo;
- ◆ **Email Alerts:** avvisi delle e-mail e
- ◆ **Messenger Alerts:** servizio di notifica dei messaggi.



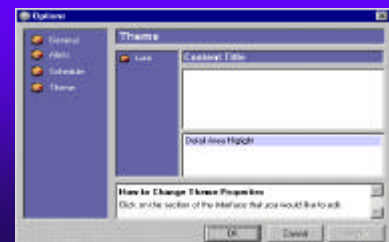
Schedule Options

Le opzioni di schedulazione permettono a un utente di selezionare date e tempi di un mese per eseguire automaticamente le scansioni dell'elaboratore locali:



Theme Options

L'opzione tema permette a un utente di modificare colore e aspetto dell'interfaccia di Retina:



GUI: Policies Dialog

Finestra di dialogo che consente all'utente di personalizzare le scansioni effettuate da Retina.

CHAM (Common Hacking Methods Attack)

Componente che impiega tecnologia AI per simulare il processo mentale di un hacker (o di un analista di rete alla ricerca di "buchi") ed evitare violazioni della sicurezza.

CHAM pensa come un hacker

Quando si selezionano le funzionalità di CHAM Retina:

- ◆ esegue una normale scansione, identificando le vulnerabilità note;
- ◆ diventa un consulente-hacker interno di fiducia.

Retina acquisisce il maggior numero di informazioni possibili sulla rete, grazie alla scansione che effettua, usando poi tali informazioni per scoprire le vulnerabilità sconosciute nella rete; questa è la parte di intelligenza artificiale del software.

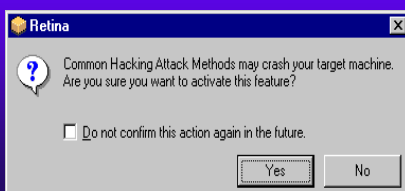
CHAM : i protocolli

Basandosi sulle informazioni raccolte CHAM esegue poi vari attacchi di tipo hacker su diversi protocolli, precedentemente selezionati dal menu Politiche (FTP, POP3, SMTP,HTTP):



Avviso CHAM

Qualora il tipo di attacco CHAM prescelto possa causare il crash del sistema, Retina chiede all'utente la conferma per l'attivazione dell'azione richiesta:



CHAM: scoperta delle vulnerabilità

Se CHAM trova delle vulnerabilità, agisce come segue:

- Visualizza in quale servizio è stata trovata la vulnerabilità.
- Rende noto il tipo di attacco effettuato.
- Fornisce tutte le informazioni alla eEye.
- Contatta il fornitore del software, nel quale è stata trovata la vulnerabilità, per avvertirlo del possibile rischio e suggerire una possibile strategia.
- Inoltra l'eventuale risposta del fornitore alla persona/organizzazione che ha rilevato la vulnerabilità.

Fix-it

- ◆ Caratteristica che consente all'amministratore di correggere automaticamente i risultati della sicurezza, quali le impostazioni dei registri e l'accesso ai file.
- ◆ Può anche lavorare in modalità remota attraverso una grande rete.

Fix-It : esempio



MODULI

I moduli sono i componenti individuali che costituiscono Retina. Attualmente Retina ha quattro moduli:

- ◆ Scanner
- ◆ Miner
- ◆ Tracer
- ◆ Browser

SCANNER

- Analizza indirizzi IP scelti per tutte le porte aperte indicate in una Politica e compila una verifica di sicurezza del computer target.
- Basandosi sui suoi risultati inicializza gli altri moduli in modo, che analizzino porte e servizi specifici.

SCANNER

Passi per avviare la scansione di un server specifico:

Passo 1 : Selezionare la voce "Scanner" dalla barra delle Shortcuts.

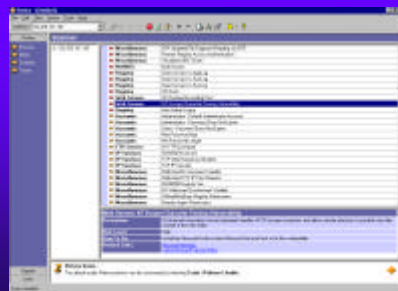
Passo 2 : Inserire l'indirizzo IP o il nome del server che si vuole analizzare nel campo indirizzo IP

Passo 3 : Premere avvio sulla Tool Bar per iniziare la scansione.

NOTE:

- > Selezionando RANDOMIZE Retina effettua una scansione random, scegliendo un indirizzo IP a caso;
- > Il campo edit deve essere disattivato durante l'esecuzione di una scansione.

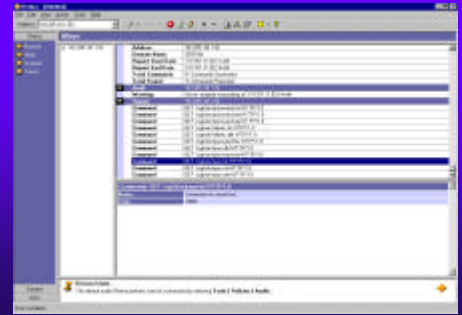
Esecuzione di SCANNER



MINER

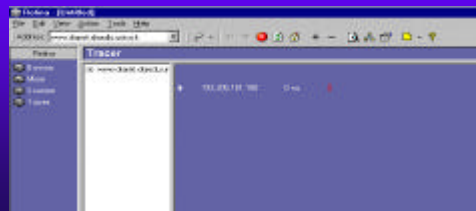
- ◆ E' il primo dei molti moduli che usano il motore AI di Retina, tramite il Brain File contenente varie parole comuni e variabili, che saranno usate come "congettura" delle passwords o per localizzare le pagine nascoste del Web.

Esecuzione di MINER



TRACER

Tale modulo crea un percorso tra il computer che correntemente esegue il Tracer e il computer obiettivo, misurando, per ogni computer, il tempo di risposta fra il computer che esegue Retina e il computer obiettivo.



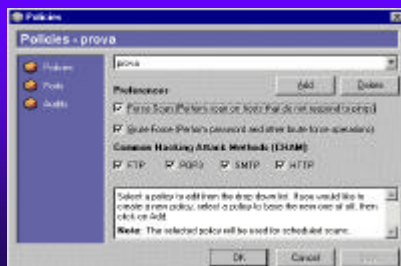
BROWSER

Il modulo browser permette di connettersi ad Internet dall'interfaccia di Retina



POLITICHE

Una politica contiene le impostazioni delle scansioni, delle porte e delle verifiche da usare ogni volta che Retina effettua una scansione.



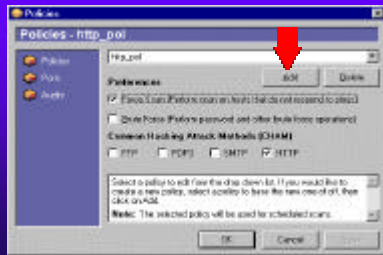
Opzioni delle politiche

Permettono a un utente di specializzare e personalizzare le impostazioni di scansione, scegliendo il tipo di attacco CHAM da simulare, le verifiche da effettuare, le porte da controllare e le modalità di scansione tra le due possibili:

- ◆ **Force Scan:** con tale modalità attivata Retina non attenderà il segnale dalla macchina target, ma la analizzerà senza verificare se essa reagisce agli impulsi o meno.
- ◆ **Brute Force:** impostazione che permette a Retina di usare i mezzi necessari per irrompere nel computer bersaglio; ciò include la scoperta delle password, così come la promozione di attacchi di tipo Denial of Service.

Aggiunta di politiche

Per aggiungere una politica, basta cliccare sul pulsante "Policies" sulla barra degli strumenti e poi su "Add" scegliendo un titolo per la nuova politica.



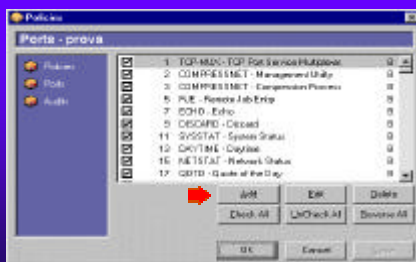
SESSIONE

Una Sessione include un file contenente tutti i dati raccolti durante una scansione, usando una politica specifica.

Se la politica cambia, all'inizio di una nuova Sessione le informazioni vecchie verranno sovrascritte.

Per mantenere i dati per un uso futuro bisogna salvare la sessione.

Aggiunta delle porte da analizzare



Smart Audits

- ◆ Valutazioni sulla rete, che identificano e dettagliano i problemi che possono compromettere la sicurezza della rete.
- ◆ Retina offre una varietà di esempi di potenziali difetti della sicurezza da poter analizzare.

Smart Audits

Il motore AI è una delle caratteristiche più potenti di Retina.

Retina crea da sé il proprio bagaglio di conoscenze da utilizzare per gli scenari "Cosa fare se" e "Nel caso in cui" raccogliendo, confrontando e catalogando le informazioni dall'avvio.

Smart Audits

- ◆ Retina crea audit abituali in un qualsiasi linguaggio di scripting, risparmiando una considerevole quantità di tempo e risorse.

Gruppi di Audit

I gruppi di audit della sicurezza indicano in dettaglio quali tipi di scerpolature Retina deve cercare.

Visualizzazione dei gruppi di audit

1. Selezionare "Policies" dalla Tool Bar.
2. Selezionare quindi "Audits" sul lato sinistro.
3. I gruppi di audit saranno elencati alla sinistra, così che possano essere trovati nel gruppo attualmente selezionato:



TIPI DI AUDIT

- ◆ **Account Audits:** sezione che include tutte le verifiche relative agli account e alle password degli utenti e le politiche relative ai controlli di accesso dell'utente sul sistema specificato.
- ◆ **CGIScripts Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate ai CGI e agli script.
- ◆ **COM Vulnerabilities Audits:** sezione che include tutte le verifiche delle vulnerabilità associate Component Object Model (COM) and DCOM (Distributed Component Object Model).

TIPI DI AUDIT

- ◆ **Commerce Vulnerabilities Audits:** sezione che include tutte le verifiche delle vulnerabilità associate ai server commerciali.
- ◆ **Databases Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate ai database.
- ◆ **FrontPage Vulnerabilities Audits:** sezione che include tutte le verifiche delle vulnerabilità associate con le estensioni di Microsoft Frontpage.

TIPI DI AUDIT

- ◆ **FTP Servers Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate ai server FTP e ai protocolli di trasferimento dei file.
- ◆ **LDAP Servers Audits:** sezione che include tutte le verifiche legate a LDAP (Lightweight Directory Access Protocol).
- ◆ **Mail Servers Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate ai server di posta, POP3, IMAP e protocolli SMTP.

TIPI DI AUDIT

- ◆ **NetBIOS Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate al protocollo NetBIOS.
- ◆ **Registry Vulnerabilities Audit:** sezione che include tutte le verifiche delle vulnerabilità associate ai registri di Windows.
- ◆ **Remote Access Vulnerabilities:** sezione che include tutte le verifiche delle vulnerabilità associate a software dell'accesso remoto, quali PC Anywhere, MS RAS, Carbon Copy etc.

TIPI DI AUDIT

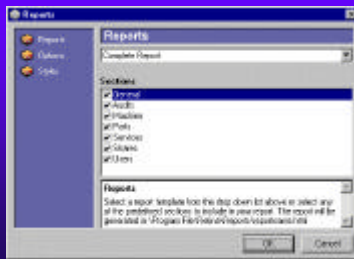
- ◆ **Server Control Audits:**
E' uso comune per molti package software consentire il controllo ed il monitoraggio remoto dei loro servizi. Questi servizi per il controllo del server potrebbero essere un'ulteriore possibile punto di attacco per un hacker remoto.
- ◆ **Web Servers Vulnerabilities Audit:**
Questa sezione include tutte le verifiche delle vulnerabilità associate ai web servers,CGIs e al protocollo HTTP.

SMART REPORTING

Retina può produrre dei rapporti di verifica della rete completamente documentati, che descrivono in dettaglio tutti i "buchi" e i difetti della sicurezza scoperti durante una scansione.

SMART REPORTING

Il rapporto di Retina è costituito dalle informazioni raccolte da Scanner e organizzate in *sezioni*: General, Audits, Machine, Ports, Services, Shares e Users.

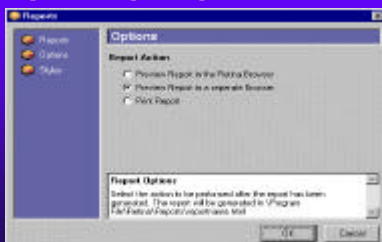


SMART REPORTING : sezioni

- ◆ **General** :comprende dati quali l'IP del computer bersaglio , la data della scansione con Retina, ed il nome del dominio del computer bersaglio.
- ◆ **Audits** :comprende una lista delle vulnerabilità della sicurezza che è stata scoperta durante la scansione
- ◆ **Machine**: dà informazioni sul computer analizzato.
- ◆ **Ports** : elenca tutte le porte attive
- ◆ **Services** :elenca i servizi Installati/attivati sulla macchina remota.
- ◆ **Shares** :elenca tutte le parti disponibili della rete
- ◆ **Users** : informazioni specifiche su tutti gli account scoperti sulla macchina remota.

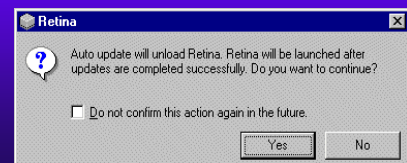
SMART REPORTING: Options

Le opzioni servono per selezionare l'azione da eseguire dopo la generazione del report : anteprima o stampa del report.



AUTO-UPDATE

Usando una connessione a internet, la caratteristica di AUTO UPDATE consente di scaricare in modo automatico gli ultimi aggiornamenti di Retina disponibili dal sito della Eye Digital Security.

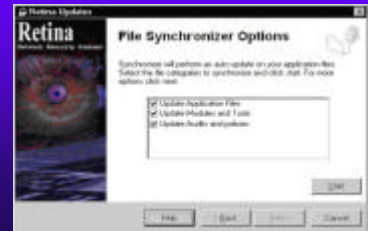


AUTO-UPDATE



Opzioni di AUTO-UPDATE

Consentono l'aggiornamento delle applicazioni, dei moduli e degli audit-files, con una semplice selezione:



VALUTAZIONI SU RETINA

- ◆ Retina ha un'architettura aperta che fornisce all'amministratore l'opportunità di sviluppare i test di vulnerabilità e i moduli di verifica specifici per le richieste di un'organizzazione.
- ◆ A differenza degli altri scanner sul mercato, Retina non forza l'amministratore ad usare un certo linguaggio di programmazione per creare questi moduli, consentendogli di scegliere quello più adatto ai suoi scopi, ad esempio PERL, C, C++, VISUAL BASIC e DELPHI.

SMART-SCANNING

- Gli scanner di sicurezza, attualmente sul mercato, inizializzano una porta scan di un sistema remoto, assumendo che tale porta usi un certo protocollo.
- Retina analizza i dati input/output specifici su una porta per determinare protocollo e servizi in uso, inizializzando dei controlli in accordo a tale protocollo.

PORT SCANNING

- ◆ Tecnica utilizzata per determinare quale porta di comunicazione del sistema obiettivo è configurata, per essere in "ascolto" verso le connessioni provenienti dall'esterno.

SMART SCANNING vs PORT SCANNING

La differenza sostanziale tra i due consiste nello "scanning" delle macchine:

- ◆ nel port scanning viene realizzato con tecniche che mandano un gran numero di pacchetti di vari protocolli in modo da dedurre quali servizi sono in ascolto verso l'esterno, dalla risposta che questi danno ai pacchetti inviati;
- ◆ in Retina, al contrario, viene effettuato scegliendo le porte da analizzare e una delle possibili strategie di attacco.



VALUTAZIONI SU CHAM

- ◆ CHAM testa i servizi sulla propria rete alla ricerca di “buchi” sconosciuti ed implementa una scansione usando gli standard IETF (Internet Engineering Task Force) per testare i responsi attesi contro quelli correnti.



VALUTAZIONI SU CHAM

- ◆ Spedisce comandi e argomenti nel tentativo di causare problemi. Al verificarsi di overflow nel buffer remoto, è importante riuscire a scoprire questi tipi di problemi prima che vengano sfruttati.



Approvato da eEye

- ◆ L'approvazione eEye è il supporto fondamentale di Retina.
- ◆ Il team della eEye Digital Security si sforza continuamente di mantenere la sicurezza della rete dell'organizzazione, tenendo informati gli amministratori di rete sulle più recenti vulnerabilità della sicurezza, tecniche di hacking e metodi di analisi.