Shorr Kan

digital security

Security Probe
Modus Operandi

Versione 2.1 – Marzo 2006

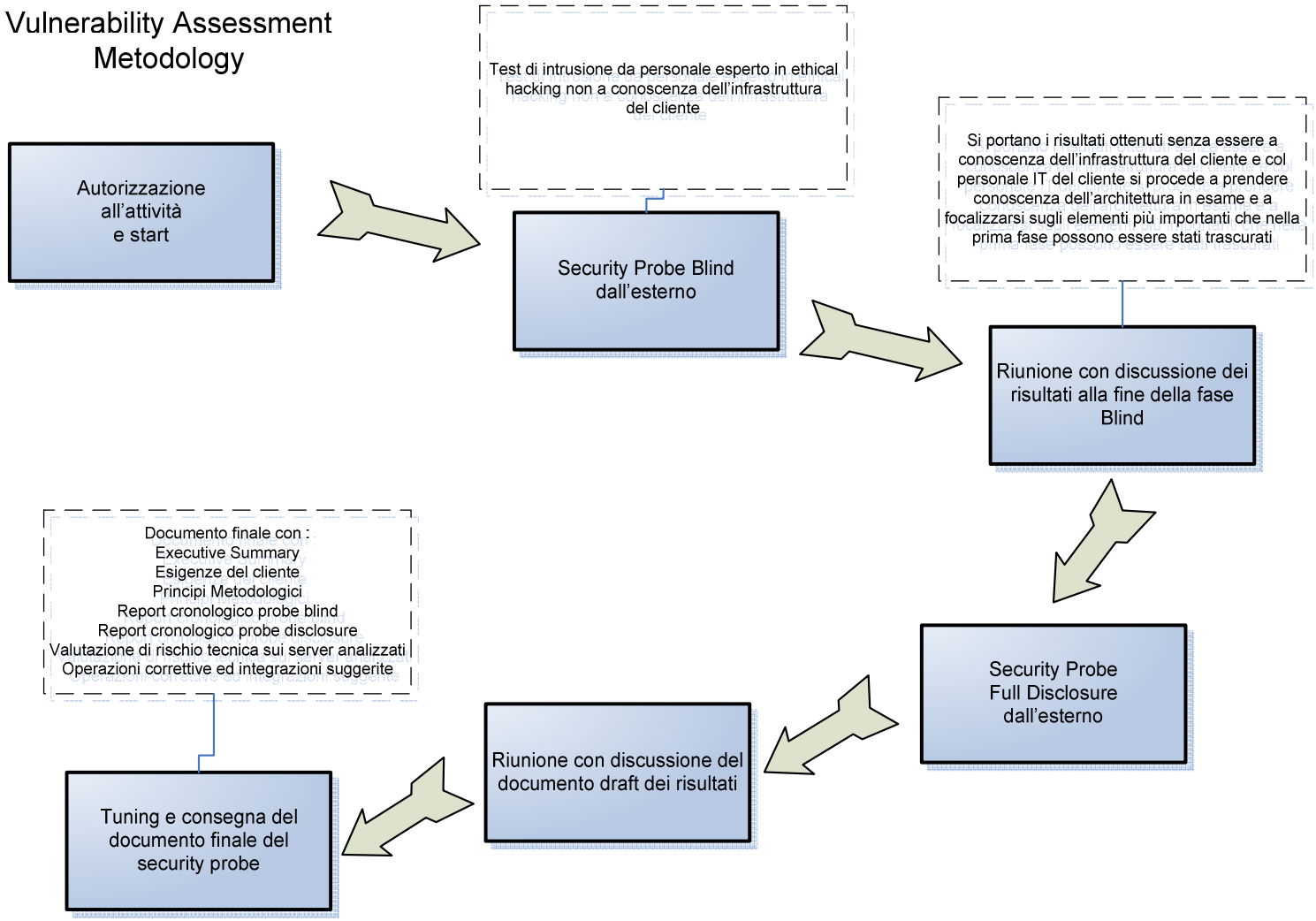
Overview

Shorr Kan Digital Security è la divisione di Shorr Kan specializzata nella fornitura di servizi di sicurezza dei sistemi informativi.

Una delle nostre principali attività di consulenza in tale ambito sono i Security Probe ed i Vulnerability Assessment.

Di seguito riportiamo la nostra Metodologia, gli Strumenti utilizzati e la struttura del Report con cui vengono descritti i risultati ottenuti.

Fasi dell'attività di analisi :



Metodologia

Passi della metodologia ‘classica’ di Security Probe:

- Footprinting
- Scanning
- Enumeration
- Gaining Access
- Escalating Privileges
- Pilfering (*)
- Covering traces and creating back doors (*)

(*) attività di hacking non eseguite in un security probe autorizzato

Footprinting

Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza riferirsi direttamente all'obiettivo stesso, ovvero effettuando una cosiddetta "analisi non invasiva". In particolare in questa fase è importante determinare: *domini, blocchi di rete e gli indirizzi ip dei sistemi direttamente collegati ad internet*. Gli strumenti utilizzati sono i motori di ricerca, gli archivi pubblici whois, Arin, Ripe e le interrogazioni ai server dns.

Scanning

L’obiettivo dello scanning è ottenere una mappa il più dettagliata possibile del sistema da attaccare; ciò significa acquisire informazioni su quali ip dei blocchi di rete trovati nella fase precedente siano effettivamente contattabili dall’esterno (ip discovery) e, relativamente a tali ip, scoprire che servizi abbiano attivi (Tcp/udp port scan) e che sistemi operativi posseggano. Gli strumenti utilizzati sono: interrogazioni ICMP (gping, hping, ecc.), la scansione delle porte tcp e udp (strobe, netcat, nmap, rascan) e fingerprint dello stack (nmap, queso).

Enumeration

Con questa fase si inizia “l’analisi invasiva” infatti si effettuano connessioni dirette ai server ed interrogazioni esplicite, il che potrebbe (a seconda della configurazione presente sui sistemi target) originare dei logs.

Attraverso l’enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, degli account validi (list user accounts), delle risorse condivise (list file shares) e delle applicazioni attive sulle porte in ascolto (identify application). Le tecniche utilizzate variano dai sistemi operativi delle macchine che si vogliono analizzare.

Gaining Access

Una volta ottenute le informazioni del punto precedente inizia il vero e proprio attacco che ha come obiettivo il riuscire ad entrare nel sistema remoto.

I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina target, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflows, attacchi data driven, ecc.) o del sistema operativo stesso.

Escalating Privileges

L’obiettivo di questa fase è sfruttare i risultati ottenuti nella fase precedente per ottenere il pieno controllo del sistema remoto attaccato. Questo si può ottenere reperendo i files presenti sul sistema che contengono le password e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando codice appositamente studiato per ottenere i privilegi di amministratore (exploits).

Probe Applicativo (Web Application Vulnerability Assessment – WAVA)

Questa analisi è costituita da una serie di tentativi d'attacco che coinvolgono i protocolli e le logiche di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni. Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server. Esistono diverse categorie di attacchi verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: Web Server, Application Server, Middle Tier, Database Management System.

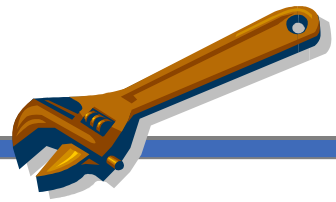
Probe Applicativo: classi di attacco (1)

- Cross-site scripting: attacchi che sfruttano una non corretta validazione dei contenuti restituiti dal server in risposta a richieste HTTP opportunamente modificate.
- Parameter tampering: attacchi che sfruttano una non corretta validazione dei parametri passati dal browser al web server.
- Backdoors, opzioni di debug e configurazioni errate di cgi: attacchi basati su errori di configurazione e/o di programmazioni molto noti e diffusi.
- Command injection: attacchi che mediante tecniche di injection mirano ad eseguire comandi sui server.

Probe Applicativo: classi di attacco (2)

- Full Spidering: attacchi che mirano ad accedere a risorse protette seguendo percorsi di navigazione non previsti.
- Cookie poisoning: attacchi basati sulla manipolazione dei coockie di sessione HTTP.
- Vulnerabilità note: attacchi che sfruttano la mancata applicazione di patch al server web o a script cgi noti.
- SQL injection: attacchi che mirano all'esecuzione di query non previste sui DBMS di backend

Strumenti



Strumenti

Le analisi saranno svolte da personale esperto umano e non da semplici tools automatici in grado di generare report rigidi e privi di intelligenza (al contrario di un vero attaccante alla vostra infrastruttura). Il nostro personale userà gli stessi tools in mano alla comunità hacker e si mantiene costantemente aggiornato sulle nuove vulnerabilità scoperte o su nuove tecniche o tools di intrusione e di protezione. Alcuni esempi di tools usati sono :

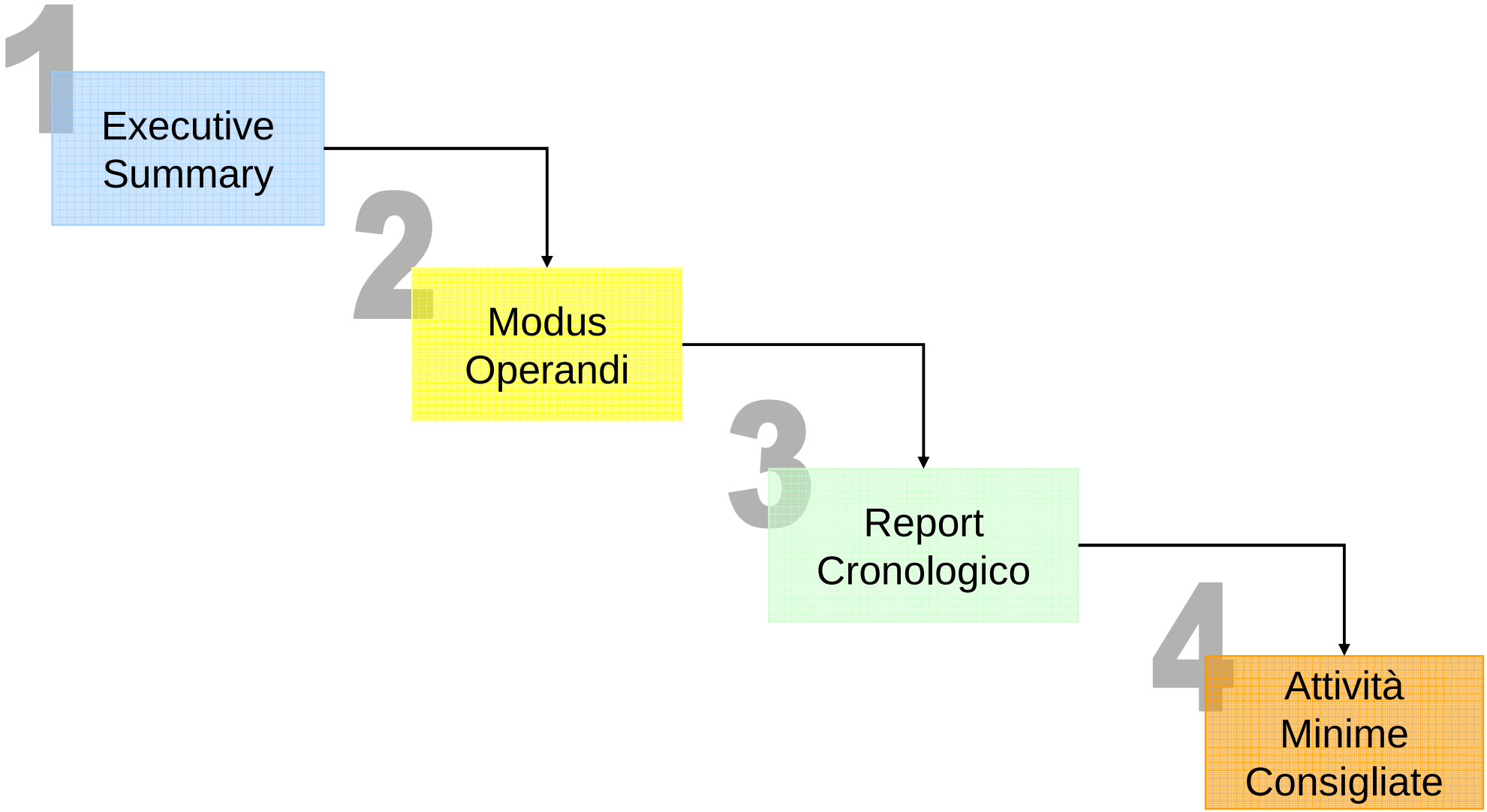
- nmap
- hping
- cain & abel
- Atstake LC5
- Exploit Always updated per specifiche vulnerabilità di servizi e applicazioni
- Keygrab
- Ethereal
- Ettercap
- Acunetix (WAVA)
- Sandcat Suite (WAVA)
- KisMet per le reti 802.11 (wi-fi)
- etc.

Nel caso di analisi di reti WI-FI vengono utilizzate delle antenne appositamente costruite da noi per aumentare l'efficacia del wardriving.

Report

Il risultato finale di un security probe è un documento tecnico dove sono evidenziate le problematiche riscontrate sia attraverso l'analisi 'a tavolino' con la parte tecnica del cliente e sia attraverso una fase di scansioni e attacchi simulati. Il documento dovrebbe sempre concludersi con i suggerimenti per l'assessment della situazione con un elenco di contromisure minime da applicare per sanare le problematiche evidenziate.

Macroblocchi del Report Tecnico finale



Le sezioni presenti in tale documento saranno essenzialmente :

Esempio punti di un Executive Summary - Probe Esterno

- **Vulnerabilità rilevata: Sql injection (High Risk)**

Alcune pagine di autenticazione del sito WWW.CLIENTE.IT sono suscettibili ad una SQL injection. Difatti mediante una query contenente determinati parametri, si riescono a generare errori sql nel database di backend, il quale a sua volta ritornerà una pagina contenente tali errori insieme ai nomi dei campi delle tabelle del database. Dagli errori visualizzati si ottiene che inserendo nel campo login la seguente stringa (e come password qualsiasi stringa) si ottiene accesso ai servizi erogati dal portale Internet :

***’ or 1=1 --**

Esempio punti di un Executive Summary - Probe Esterno

- **Vulnerabilità rilevata: Assenza di lockdown dell'account (Medium Risk)**

  La pagina WWW.CLIENTE.IT/ADMIN presenta una mascherina di autenticazione, la quale consente di inserire credenziali fittizie numerose volte senza però bloccare l'account. Ciò risulta particolarmente utile ad un hacker nel caso voglia utilizzare un metodo di brute forcing.

Esempio punti di un Executive Summary - Probe Esterno

- **Vulnerabilità rilevata: Phishing (Low Risk)**

  Tramite opportuni parametri passati nell'url del browser alla pagina del forum di WWW.CLIENTE.IT è possibile eseguire codice java script sulla macchina dell'utente ignaro. Tale operazione risulta particolarmente semplice nel caso in cui tali parametri vengano scritti in esadecimale. Ciò permette di offuscare il codice e renderlo particolarmente difficile da leggere.

Attività Minime Consigliate - Probe Esterno

- Correggere gli errori di Sql injection e Phishing nel codice del portale Internet

- Prevedere un sistema di autenticazione che imponga un timeout in seguito ad un numero predefinito di tentativi non validi, in modo da rendere più complicato l'utilizzo di metodi di password guessing automatici. Oppure prevedere il blocco dell'account dopo un certo numero di password errate.

Esempio punti di un Executive Summary - Probe Interno

- **Vulnerabilità rilevata: Macchine di dominio con accessi locali non protetti: Administrator senza password o password banali di utenti amministrativi (High Risk)**

  Questo tipo di problemi ha a che fare con il principio generale della globalità. Una configurazione sbagliata di una macchina dalla quale posso accedere facilmente al dominio una volta eseguita un escalation di privilegi locali, può minare la sicurezza dell'intero dominio. Nella fattispecie, poiché la password di amministratore locale della macchina dell'utente XXXXXX era vuota, si è riusciti ad entrare sulla sua macchine ed intercettare a questo punto sia la password utilizzata per connettersi al pc con il software di accesso remoto Real-VNC e sia gli utenti di dominio e relativa password cifrata che avevano avuto accesso al computer in questione. Una volta crackate con test e confronto da vocabolario o a forza bruta le password abbiamo scoperto che l'utente antivirus, con password semplice, era anche amministratore di dominio.

Esempio punti di un Executive Summary - Probe Interno

- **Vulnerabilità rilevata: Dati sensibili contenuti su share di rete (High Risk)**

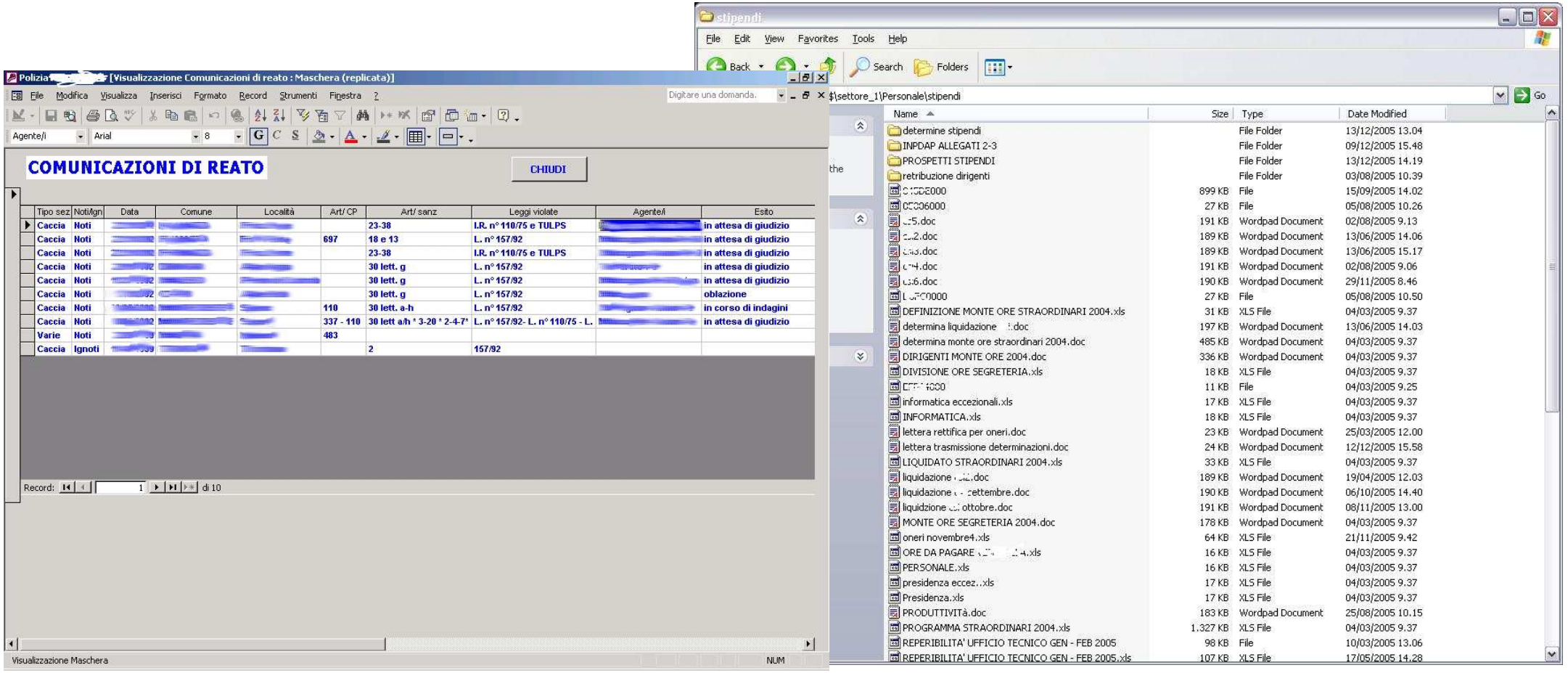
Abbiamo trovato una grande quantità di informazioni riservate e sensibili non cifrate su condivisioni di rete (share) accessibili da utenti dotati di credenziali amministrative di dominio.

Il dlgs 196/03 prevede che eventuali informazioni sensibili siano matenute cifrate sui supporti di memorizzazione elettronica ed è comunque buona norma mantenere le informazioni riservate su condivisioni di rete separate da dati non riservati. Questo vale in particolare per informazioni che permettano ad un utente non privilegiato di accedere a credenziali di utenti amministrativi o di accesso remoto.

A titolo di esempio, ipotizzando di possedere le credenziali di Amministratore di Dominio e supponendo di recuperare dai file di sistema una coppia UserName/Password non scaduta associata ad un utente VPN, è possibile fare accesso alla VPN stessa con le credenziali di terze parti appena recuperate. Lo scenario di cui sopra va interpretato come violazione dell'ambito amministrativo.

Esempio punti di un Executive Summary - Probe Interno

- **Vulnerabilità rilevata: Dati sensibili contenuti su share di rete (High Risk)**



Esempio punti di un Executive Summary - Probe Interno

- **Vulnerabilità rilevata: Enumerazione utenti locali della Sun 2.7 tramite vulnerabilità del servizio finger (Medium Risk)**

La macchina Server-XXX presenta la vulnerabilità nel servizio di finger. Infatti mediante un comando finger particolarmente formattato si riesce ad ottenere la lista di tutti gli utenti locali presenti sulla macchina Sun.

Esempio punti di un Executive Summary - Probe Interno

- **Vulnerabilità rilevata: Server Web Stampanti (Low Risk)**

Le stampanti di rete che offrono un'interfaccia web sulla porta tcp 80 mancano della password di amministratore. Questo potrebbe consentire ad un malintenzionato di collegarsi, tramite un browser, alla stampante e, dopo aver modificato a piacimento alcuni parametri, impostare la password di amministratore. A questo punto potrebbe impedire all'utenza di utilizzare tale stampante. Tale password potrebbe, in questo caso, venire resettata solo agendo su un pulsante di reset presente fisicamente sulla stampante.

Attività Minime Consigliate - Probe Interno

- Eliminare gli account di amministratori locali se possibile, in alternativa utilizzare una politica di login e password più forti (basate su acronimi, ad esempio). Discorso analogo vale per per gli account non interattivi come antivirus e di amministratore di dominio o per gli account dei servizi di web administration delle stampanti; in alternativa bloccare, se non usati, i servizi web delle stampanti

- Limitare il più possibile le condivisioni di rete tra client (impedendole anche tramite policy di dominio microsoft se lo si ritiene opportuno)

Attività Minime Consigliate - Probe Interno

- Installare le patch opportune sulla macchina Solaris 2.7 per il servizio finger

- Si consiglia di cifrare documenti contenenti dati sensibili salvati sui NAS Server di rete (come richiesto anche dall'allegato B del Dlgs 196/03) o almeno di proteggerli con password (non banali) direttamente dal sistema Office.

Contatti

Per ulteriori informazioni vi preghiamo di contattare un nostro responsabile commerciale.

Shorr Kan IT Engineering srl

http://www.shorr-kan.com/security

Sede operativa:

Via Sestriere 28/a
10141 Torino
Tel. 011 382 8358
Fax. 011 384 2028

Sede di rappresentanza commerciale:

Piazza della Repubblica 11/a
20124 Milano
Tel. 800 904 147
Fax. 02 700 483 39