



Wireless monitoring & protection

Pietro Nicoletti
piero[at]studioreti.it



Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



La problematica

- Rilevare e bloccare attività sospette di intrusione nelle reti aziendali attraverso apparati e reti wireless:
 - I recenti PC portatili dispongono tutti di CHIP Wireless
 - I PC possono avere l'interfaccia Wireless configurata in modalità Ad Hoc
 - Errore di configurazione da parte dell'utente
 - Trojan che ha attivato la scheda Wireless all'insaputa dell'utente
 - Ci possono essere dei Rogue Access Point non autorizzati che cercano di fra associare a se stessi dei PC utenti per svolgere attività canaglia
- Come proteggersi?



I controller Wireless

- Alcuni produttori hanno realizzato degli apparati o appliance basati su uno switch che controlla un certo numero di Access Point e può svolgere le seguenti funzioni:
 - Controllare gli AP della rete e assegnare loro dinamicamente i canali radio in base al snr (signal to noise ratio)
 - Rilevare e/o bloccare attività intrusione, rogue AP, Ad Hoc networks
- Una rete aziendale anche se non dispone di un'infrastruttura Wireless può essere vittima di tentativi di intrusione attraverso i CHIP Wireless presenti nei PC portatili
- I Firewall proteggono il perimetro della rete, ma non il cuore



Controller Wireless, Firewall, AP

- I controller Wireless hanno al loro interno delle funzioni tipiche dei Firewall evoluti e sono in grado quindi di:
 - rilevare e bloccare tentativi di attacchi
 - rilevare e bloccare tentativi di intrusione
- Gli AP devono essere in grado di dialogare con il controller per:
 - Inviare informazioni di tentativi di intrusione e/o attacco
 - Ricevere dal controller comandi per de-autenticare utenti wireless sospetti
- Morale:
 - Gli AP devono essere dello stesso produttore che produce il Controller
 - Bisogna scegliere gli AP in base al tipo di controller che si vuole utilizzare



Esempio di AP violation rilevata da un controller

Events > Policy Violations

Monitoring | Configuration | Diagnostics | Maintenance | Plan | **Events** | Reports | Logout

Custom Reports
Create Event Report
<No Custom Reports>

Events > Policy Violations

Search Results [Search](#)

Group By: None

<input type="checkbox"/>	Event ID	Type	Info	Device	MAC Address	Count	Occurred Time
<input type="checkbox"/>	56	IBSS Violation	Not Active	00:0b:86:c3:ab:20	2	16:46:46 10/9/2006	
<input type="checkbox"/>	10	IBSS Violation	AP	00:0b:86:a4:bc:30	2	16:16:19 10/6/2006	
<input type="checkbox"/>	12	IBSS Violation	AP	00:0b:86:a4:c0:10	3	16:15:56 10/6/2006	

1 | 1-3 of 3 | 10

Delete Selected Events

E-mail Support

Internet

start | RUBRICA1.DOC... | WIRELESS-1.d... | Documento1 - ... | Prompt dei com... | Events > Policy ... | 15.19



Esempio di Station violation and deauthentication

Events > Man in the Middle Attacks - Microsoft Internet Explorer

File Modifica Visualizza Preferiti Strumenti ?

Indirizzo <http://172.25.255.70:8888/screens/wmsi/events.html?mode=event-custom&mode-title=Man%20in%20the%20Middle%20Attacks&type=4&type=5&typ>

ALCATEL Events **OmniAccess 4308**

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Logout

Custom Reports
Create Event Report
<No Custom Reports>

Events > Man in the Middle Attacks

Search Results [Search](#)

Group By: None

<input type="checkbox"/>	Event ID	Type	Info	Device	MAC Address	Count	Occurred Time
<input type="checkbox"/>	33	IDS: Disconnect Station Attack	Deauth	STA	00:0c:f1:17:e0:af	2	16:19:10 10/6/2006
<input type="checkbox"/>	29	IDS: Disconnect Station Attack	Deauth	Not Active	be:01:53:01:55:01	2	16:19:10 10/6/2006
<input type="checkbox"/>	32	IDS: Sequence Number Anomaly	00:0c:f1:17:e0:af	STA	00:0c:f1:17:e0:af	1	16:18:37 10/6/2006
<input type="checkbox"/>	28	IDS: Sequence Number Anomaly	be:01:53:01:55:01	Not Active	be:01:53:01:55:01	1	16:18:14 10/6/2006

1 | 1-4 of 4 | 10

Delete Selected Events

E-mail Support

<http://172.25.255.70:8888/screens/wmsi/reports.html?mode=sta&mac=00:0c:f1:17:e0:af> Internet

start RUBRICA1.DOC... WIRELESS-1.d... Documento1 - ... Prompt dei com... Events > Man i... 15.22



Reti Wireless di monitoring

- In ambiti particolarmente sensibili con elevati requisiti di sicurezza dove per policy aziendale non ci sono reti Wireless è comunque necessario

Realizzare una rete Wireless di solo Monitoring per rilevare e bloccare attività sospette !

- La copertura radio dell'edificio o del campus deve essere totale
 - Il numero degli AP può essere contenuto se si usano antenne ad elevato guadagno
 - Gli AP non devono trasmettere dati, ma solo rilevare attività sospette e bloccarle