

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via San Pietro all'orto, 26 – 20121 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

## Verbale di Riunione

Informazioni generali	
CLIENTE	RAS
DATA	29 Marzo 2005
LUOGO	Via Oglio - Milano
OGGETTO	Stato avanzamento lavori dello studio di sicurezza sulle agenzie
VERBALE REDATTO DA	Gianluca Vadrucchio

Partecipanti		
Cognome e Nome	Società	Riferimenti
Dario Bonavitacola	GESI	dario.bonavitacola@rasnet.it
Alfredo Capponi	GESI	alfredo.capponi@rasnet.it
Fabio De Ferrari	GESI	fabio.deferrari@rasnet.it
Giuseppe Giannicolo	GESI	giuseppe.giannicolo@rasnet.it
Salvatore Stefanelli	GESI	salvatore.stefanelli@rasnet.it
Roberto Ticini	GESI	roberto.ticini@rasnet.it
David Vincenzetti	Hacking Team	david.vincenzetti@hackingteam.it
Gianluca Vadrucchio	Hacking Team	gianluca.vadrucchio@hackingteam.it

Argomenti trattati			
Nr.	Argomento	Descrizione	Tempistiche
1	Stato dello studio	E' stata presentata da Hacking Team la situazione in termini di fasi del progetto ed in termini di risultati ottenuti. E' emersa la necessità di rendere lo studio completo mediante l'attuazione dei due step successivi	//
2	Definizione di attacco	RAS ha manifestato la necessità di adeguarsi al gergo da loro individuato: ➤ attacco semplice: minaccia insistente sui sistemi di agenzia e relativa a vulnerabilità semplici e tradizionali ➤ attacco complesso: minaccia molto più strutturata (simile più ad uno scenario) che sfrutta vulnerabilità complesse, spesso composte da più attacchi semplici.	//

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via San Pietro all'orto, 26 – 20121 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

3	Fasi di progetto	<p>Si sono definite le tre fasi di progetto (diverse da quelle originarie) proprio per perseguire meglio l'obiettivo del cliente e per essere più aderenti ai requisiti ed all'ambiente reale:</p> <ul style="list-style-type: none"> <li>➤ AS (Attacco Semplice): studio della sicurezza della agenzia esclusivamente in termini e confini "locali". In questo caso la minaccia consiste nel reperire o danneggiare informazioni riferite strettamente al sistema locale.</li> <li>➤ AC (Attacco Complesso): studio della sicurezza relativa ai servizi erogati dall'host. In questo caso si tratta di avere informazioni o servizi o portare a compimento azioni fraudolente impersonificando sia un utente valido e riconosciuto di agenzia sia un applicativo.</li> <li>➤ AH (Attacco Host): studio della sicurezza completo del centro stella in riferimento alle connessioni di agenzia. In questo caso si tratta di sfruttare la pura connessione dell'agenzia con il centro stella per portare a compimento azioni maliziose sia senza credenziali, sia oltrepassando quelle che sono reputate essere le limitazioni di autorizzazione previste.</li> </ul> <p>L'analisi deve in tutti i casi essere condotta tenendo presente la possibilità di avere o meno la presenza di una connessione internet da parte delle agenzie.</p>	//
4	Risultati dello studio	<p>Le vulnerabilità e le minacce presentate a conclusione dello studio finale dovranno essere pesate dalla probabilità P (facilità di esecuzione, possibilità di accadimento...) e dall'impatto I (importanza degli asset colpiti, obiettivi...):  <b>RISCHIO = P x I</b></p> <p>Ad ogni minaccia dovrà anche corrispondere una proposta di soluzione, secondo lo schema definito e illustrato in fondo al presente verbale di riunione (TABELLA DI PRESENTAZIONE DEI RISULTATI).</p> <p>Inoltre, ad integrazione del documento di analisi, a fine lavoro dovrà essere fornita una tabella riepilogativa e già definita nel corso della presente riunione e descritta in fondo al presente verbale (TABELLA DEGLI SCENARI). Questa tabella ricalca la situazione reale delle agenzie e le fasi di</p>	//

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via San Pietro all'orto, 26 – 20121 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

		<p>studio previste al punto 3.</p> <p>L'intero studio dovrà contenere specifiche parti descrittive dei risultati e degli scenari che tengano in considerazione la possibilità di essere letti dal management. In tal senso, tali parti dovranno essere scritte con terminologie e riferimenti adatti alla comprensione della lettura di personale dirigente e non tecnico.</p>	
5	Vincoli	<p>La soluzione proposta a fine studio dovrà sin da ora tenere presente dei seguenti vincoli imposti dal cliente:</p> <ol style="list-style-type: none"> <li>1. tenere sempre presente il trade-off costo/gestione</li> <li>2. nessun genere di attività sui client di agenzia può essere proposta</li> <li>3. lo studio non dovrà comprendere proposte relative alla sicurezza fisica</li> <li>4. il cambio o la gestione delle password di administrator potrebbe diventare un vincolo qualora impatti sulla funzionalità degli applicativi</li> <li>5. il protocollo netbios dovrà essere mantenuto attivo per garantire il file sharing all'interno dell'agenzia</li> <li>6. l'host è funzionante dalle 08:00 alle 23:00, dopodiché viene spento. Di notte è garantito l'utilizzo locale per manutenzione</li> <li>7. la soluzione proposta dovrà essere facilmente gestibile in termini di upgrade, di patch di sicurezza e di configurazioni</li> <li>8. non potrà essere proposto un cambio di piattaforma locale delle agenzie (che rimarrà quindi NT4)</li> <li>9. nel caso sia presente nella proposta una soluzione custom, dovrà essere indicato anche il relativo SLA</li> <li>10. l'agenzia deve avere la piena libertà di scelta della propria linea fisica di connessione ad internet ed il proprio provider</li> </ol>	

Azioni da intraprendere		
Azione	Responsabile	Tempistiche
Fornire un verbale di riunione	Hacking Team	Appena possibile
Proseguire i lavori e completare lo studio secondo quanto concordato	GESI e Hacking Team	//

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via San Pietro all'orto, 26 – 20121 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

## Eventuali dettagli tecnici

Argomento	Descrizione
//	Nessun argomento tecnico è stato trattato durante la riunione.

## Commenti vari

Durante la riunione si è manifestata la volontà di tutti i partecipanti di continuare e portare a compimento il lavoro secondo le fasi definite ed evidenziate nel punto 3.

# ]HackingTeam[

Hacking Team S.r.l.

Sede operativa: Via della Moscova, 13 – 20121 Milano – Tel: +39.02.29060603

Sede legale e amministrativa: Via San Pietro all'orto, 26 – 20121 Milano

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

P.IVA: 03924730967 – Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 – N° R.E.A. 1712545

## **TABELLA DI PRESENTAZIONE DEI RISULTATI**

Criticità riscontrata	Descrizione	Livello di Rischio		Soluzioni proposte
		Probabilità (P)	Impatto (I)	

## **TABELLA DEGLI SCENARI**

FASI	Situazione attuale				Situazione futura	
	Senza internet		Tramite subagenzia		Con internet	
	Appl.	Tech.	Appl.	Tech.	Appl.	Tech.
Attacco Semplice (AS)						
Attacco Complesso (AC)						
Attacco Host (AH)						

Ognuno degli scenari presentati dovrà essere “mappato” con le criticità elencate nella tabella precedente (TABELLA DI PRESENTAZIONE DEI RISULTATI) e dovrà essere descritto in maniera sintetica, utilizzando terminologie non tecniche.

Anche in questa tabella sarà presente una colonna “SOLUZIONE PROPOSTA”, ovviamente legata alla medesima colonna della tabella precedente (TABELLA DI PRESENTAZIONE DEI RISULTATI), con la descrizione dell’approccio proposto più in termini “macro” e meno di dettaglio.