ISGroup
Information Security

IT Security

Prodotti e soluzioni

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Istituzionale ISGroup

ISGroup è una struttura indipendente specializzata in IT *Security* in grado di offrire servizi e prodotti di sicurezza informatica di livello qualitativo elevato.

ISGroup è nata da un piccolo gruppo di ricercatori fortemente motivati a produrre i migliori risultati tramite la loro capacità, esperienza e creatività.

ISGroup oggi rappresenta una soluzione per gli operatori ICT e le agenzie di sicurezza che necessitano forniture di servizi indipendenti e personalizzati.

Amiamo quello che facciamo e non siamo spaventati dalle sfide.

Le nostre conoscenze spaziano dalla sicurezza fisica a quella delle infrastrutture, dei sistemi operativi, delle reti, delle applicazioni, del web e "lato client". Collaboriamo con agenzie di IT *Security* nazionali ed internazionali e grazie a questo operiamo ai più alti standard qualitativi. Inoltre siamo parte attiva all'interno della comunità dei ricercatori indipendenti.

La nostra struttura, essenziale, efficiente e competitiva, è composta da liberi professionisti.

Per questo ci proponiamo come ideale **Outsourcing Partner** per le aziende di ICT e IT *Security*.

Possiamo essere la Vostra risorsa per compiti specializzati o la forza lavoro addizionale di cui necessitate.

Approfondisci i servizi e prodotti:

- VA - Vulnerability Assessment
- NPT - Network Penetration Test
- WAPT - Web Application Penetration Test
- EH - Ethical Hacking
- CR - Code Review
- EDU - Formazione/Training

Contattateci per ottenere uno *Starter Kit* e per maggiori informazioni riguardo la nostra metodologia e prassi. Chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

Perchè scegliere ISGroup

ISGroup rappresenta un modello di business non convenzionale nel panorama Italiano proponendosi come "associazione" di liberi professionisti e consulenti che già operano con successo nel settore dell'IT *Security* legati da forte fiducia e considerazione reciproca.

A chi ci rivolgiamo

A società che si occupano di sicurezza informatica alla ricerca di un *Outsourcing Partner*.

A società terze che non hanno la sicurezza informatica come core business ma vogliono offrire servizi di IT *Security* ai propri clienti.

Vantaggi e benefici

Costi! La nostra struttura snella ci consente di minimizzare i costi.

Spese di spostamento ridotte al minimo: il lavoro può nella maggior parte dei casi essere svolto in remoto.

ISGroup già collabora con leader di mercato nella fornitura di servizi e prodotti di sicurezza informatica garantendo pertanto la stessa qualità sul lavoro svolto ma ad un costo concorrenziale.

Il lavoro che svolgiamo ha *standard* qualitativi definiti e viene diviso tra i componenti di ISGroup secondo moderni schemi di gestione dei progetti. Non vi è quindi un unico referente cui il cliente deve "legarsi".

ISGroup dispone di una rete di contatti composta da professionisti e ricercatori che primeggiano in ambiti specifici per garantire l'eccellenza nel servizio e la piena soddisfazione del cliente.

ISGroup è indipendente dalle piattaforme e quindi è trasversale alle eterogeneità dei bisogni della sicurezza informatica.

ISGroup opera già da anni come *pool* di ricerca nell'ambito della sicurezza informatica e per questo i propri membri compaiono come consulenti e come relatori in molti corsi di aggiornamento e conferenze fruite da professionisti del settore.

Servizi offerti

- VA - Vulnerability assessment
- NPT - Network penetration test
- WAPT - Web application penetration test
- EH - Ethical hacking
- CR - Code review
- EDU - Formazione/Training

Servizi e prodotti offerti

La nostra offerta si concentra su pochi ma ben definiti servizi di alto livello qualitativo.

NPT - Network Penetration Test

Verifica manuale dell'effettivo livello di sicurezza di un'infrastruttura IT tramite la simulazione di tecniche e modalità proprie di un attaccante. Un NPT è finalizzato ad identificare problematiche di sicurezza sconosciute e che diversamente non verrebbero rilevate da strumenti automatici. Esperienza e creatività vengono sommate all'uso delle metodologie più accreditate quali OSSTMM e OWASP.

WAPT - Web Application Penetration Test

Verifica manuale dell'effettivo livello di sicurezza di una o più applicazioni web tremite la simulazione di tecniche e modalità proprie di un attaccante. Un WAPT è finalizzato ad identificare problematiche di sicurezza sconosciute e che diversamente non verrebbero rilevate da strumenti automatici. Esperienza e creatività vengono sommate all'uso delle metodologie più accreditate quali OSSTMM e OWASP.

Ethical Hacking

Gli attaccanti non seguono regole e possono agire nei modi più disparati per raggiungere il loro obbiettivo col minor sforzo possibile. Il nostro *Tiger Team* analizzerà l'infrastruttura IT, le procedure, le risorse umane e la sicurezza fisica del cliente per scoprirne le falle e sfruttarle al fine di svolgere una simulazione quanto più veritiera possibile di quello che potrebbe avvenire in condizioni reali.

VA - Vulnerability Assessment

Esecuzione di una serie di *audit* non invasivi sia manuali che tramite strumenti software open source e commerciali di infrastrutture IT e applicazioni web. Un VA è in grado di individuare eventuali vulnerabilità conosciute. Nessun servizio da noi erogato è solamente automatico e per questo i nostri VA sono di qualità superiore pur mantenendo costi e tempi ridotti.

CR - Code Review

Analisi del codice sorgente di un'applicazione mirata ad individuare problematiche di sicurezza e "bad pratices". I CR permettono di individuare la maggior parte delle vulnerabilità trattandosi di un'attività *White Box* (in cui il cliente fornisce tutte le informazioni utili all'*auditor*), anche quelle che normalmente non sarebbero esposte durante un WAPT o un NPT.

Molte delle vulnerabilità da noi scoperte nell'ambito della nostra attività di ricerca sono frutto dell'analisi del codice sorgente delle applicazioni.

Formazione

Proponiamo diversi percorsi formativi e di aggiornamento per amministratori di rete, sistemisti, sviluppatori e *penetration testers*. La formazione è una componente fondamentale per innalzare il livello di sicurezza e la consapevolezza di un *team* sul lungo periodo.

ISGroup
Information Security

VA

Vulnerability Assessment

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Vulnerability Assessment (VA)

Il servizio di *Vulnerability Assessment* fornito da ISGroup ha il compito di analizzare e valutare la sicurezza del sistema (o dei sistemi) al fine di rilevare eventuali vulnerabilità note.

L'attività può essere condotta esternamente o internamente. Nel caso di *Vulnerability Assessment* condotto esternamente, la scansione viene effettuata da un host remoto, il quale ha accesso al sistema solamente attraverso la rete *Internet*.

Nel secondo caso invece, la scansione viene effettuata dall'interno della rete privata (*Intranet*), in modo da avere maggiore visibilità sul sistema in esame.

Queste due configurazioni permettono di simulare diversi scenari di attacco: il primo simula l'attacco da parte di un soggetto esterno (ad esempio un concorrente aziendale sleale); il scenario invece simula l'attacco da parte di un soggetto interno (ad esempio un dipendente vendicativo).

In seguito allo svolgimento della fase di scansione tutte le vulnerabilità identificate vengono controllate per eliminare gli eventuali falsi positivi. Per ogni vulnerabilità effettiva viene fornita una descrizione dettagliata e sopratutto di come vi si può porre rimedio.

Dato l'alto numero di nuove vulnerabilità che vengono scoperte ogni giorno è fondamentale svolgere un *Vulnerability Assessment* con la giusta frequenza al fine di assicurarsi che le configurazioni dei sistemi siano corrette e le opportune patch di sicurezza applicate.

ISGroup fornisce soluzioni di *Vulnerability Assessment* adatte a qualsiasi esigenza e dimensione aziendale, garantendo un livello qualitativo elevato.

Descrizione del servizio

L'attività di *Vulnerability Assessment* inizia con l'identificazione dei sistemi e delle risorse (servizi, applicazioni web, etc) messe a disposizione. Successivamente tramite l'utilizzo di *tool* automatici e manualmente vengono identificate le problematiche di sicurezza conosciute in maniera non invasiva. I *Vulnerability Assessment* permettono di comprendere velocemente il livello si sicurezza di una rete.

L'identificazione avviene attraverso tecniche attive (ad esempio il numero di versione che il programma invia nelle risposte), passive o basate sull'inferenza (caratteristiche che un programma ha e non può nascondere). I risultati sono verificati manualmente in modo da eliminare i falsi positivi e ottenere un *Report* compatto e dettagliato, destinato sia al *Management* che allo *staff* operativo che dovrà correggere le problematiche.

Output

Il *Report* è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

Executive Summary
All'inizio del *Report* e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al *Management*.

Vulnerability Details
La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, dedicata al *Security Manager*.

Remediation Plan
Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*.

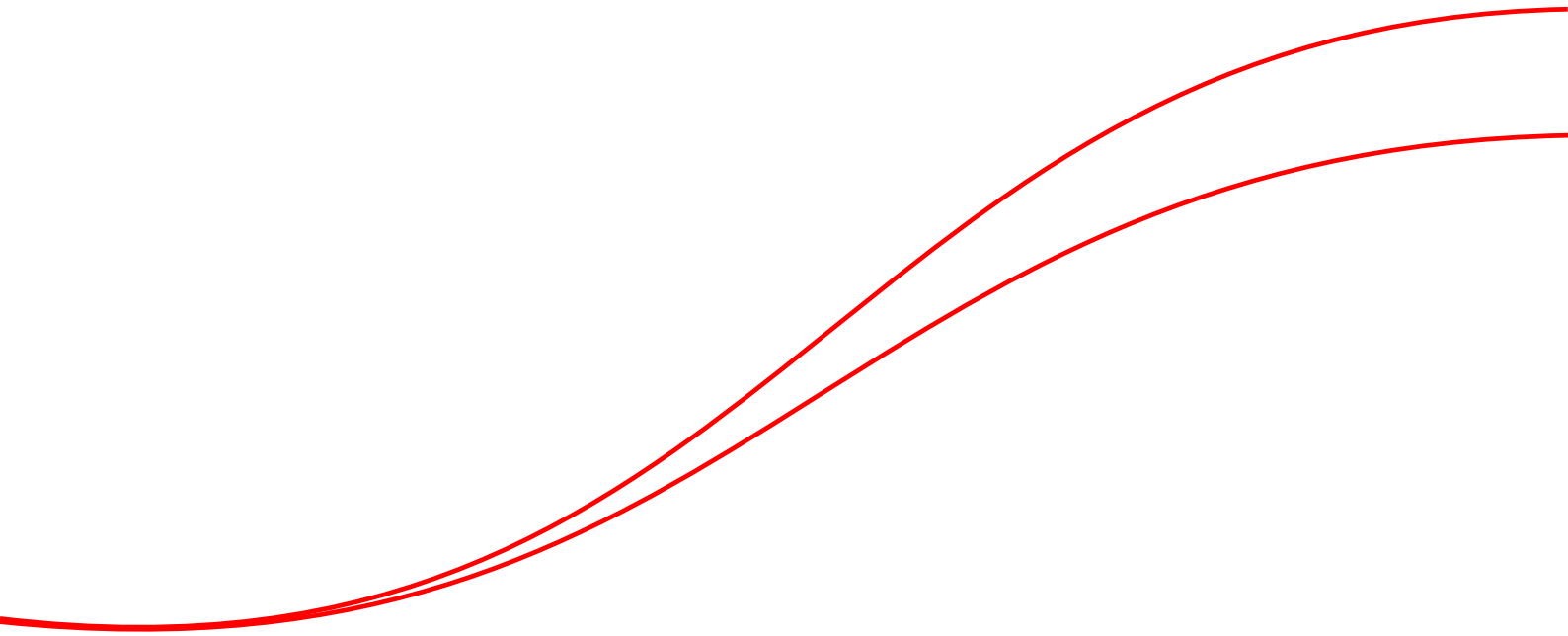
Richiedi servizi di Vulnerability Assessment

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

ISGroup
Information Security

NPT

Network Penetration Test



www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Network Penetration Test (NPT)

Trovare le vulnerabilità nei propri sistemi prima che lo faccia qualcun'altro è un processo importante per la sicurezza della propria rete. Un *Network Penetration Test* ha lo scopo di identificare le vulnerabilità, focalizzandosi sulle aree di maggior impatto per il business aziendale.

Un *Network Penetration Test* è orientato alla valutazione della sicurezza di una rete e può essere svolto dall'interno (*Internal PT*), dall'esterno (*External PT*) e con vari livelli di informazione e accesso alle infrastrutture e risorse del cliente (*Black Box*, *Gray Box* e *White Box*).

É possibile quindi simulare scenari di attacco differenti. Un *External PT* di tipo *Black Box* ad esempio mira ad identificare quale danno può essere causato da un attaccante casuale esterno all'organizzazione mentre un *Internal PT* di tipo *Gray Box* simula un dipendente malintenzionato.

ISGroup è il fornitore ideale per le Vostre necessità di Network Penetration Test e opera con serietà secondo standard internazionalmente riconosciuti ai più alti livelli di qualità grazie al costante impegno nell'ambito della ricerca. Contattateci per informazioni e richiedete un preventivo personalizzato.

Descrizione del servizio

Oggi che il commercio elettronico, le operazioni *on-line B2B (Business-to-Business)* e la connettività globale sono diventati componenti fondamentali della strategia di un business di successo, le imprese hanno adottato processi e pratiche di sicurezza.

La maggior parte delle imprese opera con diligenza per mantenere un efficiente ed efficace politica di sicurezza che implementi i più recenti prodotti e servizi per prevenire le frodi, gli atti di vandalismo, sabotaggio e attacchi *DoS (Denial of Service)*.

Nonostante questo molte imprese non danno il giusto risalto ad un ingrediente chiave del successo di una politica di sicurezza: la verifica che la rete e i sistemi di sicurezza funzionino come previsto.

L'attività di *Network Penetration Test*, utilizzando strumenti e processi per scansionare l'infrastruttura di rete alla ricerca di vulnerabilità, aiuta a rifinire una politica di sicurezza aziendale, identificando le vulnerabilità, e di garantire che l'implementazione di sicurezza effettivamente fornisca la protezione che l'azienda richiede e necessita.

Eseguire regolarmente *Penetration Test* aiuta le imprese a scoprire i punti deboli della sicurezza della rete, che possono portare a dati o apparecchiature compromesse o distrutte da *Exploit*, *Virus*, *Trojan*, attacchi *Denial of Service* e altre intrusioni. La verifica può esporre anche altre vulnerabilità che possono essere introdotte da *patch* e aggiornamenti o da errori sui *Server*, *Router* e *Firewall*.

Network Penetration Test in breve:

- Vengono ricercate dall'esterno o dall'interno vulnerabilità nei sistemi maggiormente esposti.
- Le vulnerabilità identificate vengono sfruttate al fine di violare il perimetro della rete.
- I sistemi interni vengono ispezionati alla ricerca di altre vulnerabilità che permettano di ottenere ulteriore accesso ai dati e alle infrastrutture.
- Il processo viene ripetuto fintanto possibile.

Specifiche del servizio di Network Penetration Test

Il servizio di *Network Penetration Test* viene effettuato da qualificati professionisti secondo metodologie riconosciute internazionalmente, quali l'OSSTMM (*Open Source Security Testing Methodology Manual*), un manuale *Open Source* per l'esecuzione dei *test* di sicurezza verso infrastrutture ed asset informatici), adattate rispetto le specifiche esigenze del cliente e dello scenario di attacco.

Tutte le parti più delicate e tecniche vengono svolte da ricercatori *senior* per garantire la massima professionalità e far si che non vi siano danneggiamenti né all'infrastruttura né ai dati.

Dall'esterno (*External PT*) o dall'interno (*Internal PT*) e col livello di informazioni scelto dal cliente (*Black Box*, *Gray Box* e *White Box*) per simulare diversi scenari di attacco.

Ogni nostro servizio è personalizzabile secondo le esigenze del cliente e integrabile con gli altri servizi e prodotti offerti. Un *NPT* può tenere conto dell'aspetto prettamente informatico o anche delle persone e dei processi (*Social Engineering*) e della sicurezza fisica. É il cliente a decidere quali sono gli aspetti più importanti dell'attività e dove gli sforzi del *team* di attacco debbano essere concentrati.

I risultati dell'attività di *testing* vengono riassunti ed esposti nel *Report*, un documento semplice e dettagliato composto da tre sezioni principali.

Una parte iniziale di alto livello, chiamata *Executive Summary*, dedicata al *Management*. Una parte tecnica che descrive nel dettaglio le vulnerabilità rilevate e il loro impatto, dedicata al *Security Manager*. Una parte tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*, chiamata *Remediation Plan*.

Scenari di Network Penetration Test

ISGroup esegue i propri *test* con varie modalità operative:

Internal PT
I *test* vengono effettuati posizionandosi all'interno della rete aziendale.

External PT
I *test* vengono effettuati posizionandosi all'esterno della rete aziendale.

Inoltre è possibile differenziare tra *testing Black Box*, *Gray Box* e *White Box*, a seconda delle informazioni fornite sui sistemi da attaccare. Ecco alcuni esempi e scenari:

External PT Black Box
Simula un attaccante casuale o esterno (ad esempio un concorrente) ma comunque senza accesso ad informazioni e credenziali di accesso dell'azienda.

Internal PT Black Box
Simula un attaccante che abbia accesso fisico (ad esempio un consulente esterno o un visitatore in una sala riunioni) o remoto (ad esempio un *computer* di una segretaria compromesso) alla rete aziendale.

External PT White Box
Simula la compromissione di una componente esposta all'esterno per capire che livello di accesso un attaccante possa ottenere alle altre parti dell'infrastruttura aziendale.

Internal PT White Box
Simula un attaccante interno all'organizzazione con informazioni ed accesso ad alcune parti dell'infrastruttura per capire che livello di accesso alle componenti critiche sia possibile ottenere.

Wireless Penetration Test
Cerca di compromettere l'infrastruttura *wireless*, simula un attaccante che sia fisicamente prossimo ad uno degli edifici dell'azienda in cui sia installata una rete *wireless*.

Social Engineering
Invece di attaccare la componente informatica viene attaccata quella "umana", con tecniche di manipolazione si cerca di indurre le persone a compiere azioni o a rivelare informazioni.

Output

Il *Report* è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

Executive Summary
All'inizio del *Report* e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al *Management*.

Vulnerability Details
La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, dedicata al *Security Manager*.

Remediation Plan
Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*.

Nel caso in cui l'attività sia per una terza parte lavoriamo con disinvoltura su modelli di *Report* preventivamente forniti con la grafica e secondo le modalità che ci vengono indicate.

Precisione e dettaglio, semplicità e chiarezza sono i fondamentali di un buon *Report*. Vista la complessità delle problematiche di sicurezza cerchiamo sempre di facilitare il lavoro di chi si appoggia a noi tramite documenti redatti con la massima cura e che siano veramente utili e "pragmatici".

Poniamo grande attenzione al *Remediation Plan*. Questa componente, spesso considerata di secondo piano, è fondamentale per far si che le problematiche identificate vengano realmente risolte nella maniera corretta.

I nostri *Report* sono uniformi e facilmente compatabili tra di loro.

Per richiedere un esempio di *Report* anonimizzato, oltre che discutere delle vostre specifiche esigenze, contattateci senza impegno.

Richiedi servizi di Network Penetration Test

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

ISGroup
Information Security

WAPT

Web Application Penetration Test

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Web Application Penetration Testing (WAPT)

Il servizio di *Web Application Penetration Testing* è uno dei servizi di sicurezza applicativa (*Application Security Assessment*) proposti da ISGroup.

Le applicazioni web sono ormai prevalenti e sempre più sofisticate oltre ad essere critiche per tutti i *business* basati sul web.

Verranno analizzati i componenti critici di un portale web, un'applicazione *E-Commerce* o una piattaforma web.

Utilizzando tecniche manuali e centinaia di strumenti appropriati il *tester* è in grado di identificare problematiche evidenti e nascoste.

Come per le applicazioni *client/server* le applicazioni web generalmente soffrono di gestione impropria delle richieste del *client* e mancata o impropria validazione e controllo da parte dello sviluppatore.

Data la natura delle applicazioni web, esse sono completamente esposte ed accessibili, questo rende la "sicurezza tramite segretezza" (*security through obscurity*) impossibile e necessario codice applicativo resistente.

In secondo luogo le applicazioni web processano dati da richieste *HTTP*, un protocollo che permette una miriade di encoding e incapsulazioni diverse.

Descrizione del servizio

Un *Web Application Penetration Test* è la simulazione di un attaccante nei confronti di un sito, portale o applicazione web. Il *testing* inizialmente consiste nello scoprire e identificare tutte le risorse esposte sul *target*.

A questo punto prima di testare le applicazioni web vere e proprie viene controllata l'infrastruttura alla ricerca di vulnerabilità note e non.

Successivamente con l'ausilio di *tool* e manualmente ogni parametro viene testato con valori predefiniti e vengono provate le tecniche di attacco generiche per la data piattaforma.

In parallelo il *tester* effettua un'analisi della business logic per verificare che non vi siano problematiche concettuali.

Una volta individuati dei punti di attacco (*entry point*) validi si procede al tentativo di attacco che ha come obbiettivo la compromissione più profonda ed estesa possibile.

Dato il livello di accesso ottenuto si tenderà di compiere azioni non ammesse, prelevare dati dal *database* di *backend*, prelevare file o sorgenti dal disco, modificare informazioni e laddove possibile ottenere il pieno controllo della macchina e di quelle limitrofe.

Output

Il *Report* è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

Executive Summary

All'inizio del *Report* e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al *Management*.

Vulnerability Details

La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, dedicata al *Security Manager*.

Remediation Plan

Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*.

Richiedi servizi di Web Application Penetration Testing

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

ISGroup
Information Security

EH

Ethical Hacking

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Ethical Hacking (EH)

Il servizio di *Ethical Hacking* offerto da ISGroup simula l'attacco da parte di un utente malintenzionato (esterno o interno). Gli attacchi che verranno portati a termine non riguardano solamente l'aspetto tecnologico, ma spaziano anche in quella branca dell'hacking che si concentra non sulla tecnologia ma su quello che spesso è il vero anello debole del sistema: il fattore umano.

Questo si traduce nell'utilizzo di tecniche di attacco non convenzionali (in aggiunta a quelle normalmente utilizzate in una sessione di *Penetration Test*, sia *NTP* che *WAPT*), come ad esempio il *Social Engineering* e l'intercettazione (*sniffing*) del traffico di rete.

Descrizione del servizio

ISGroup simula in modo del tutto fedele una vera sessione di attacco, come quella portata a termine da un vero attaccante, permettendo quindi di valutare con estrema accuratezza l'effettivo rischio a cui si è esposti. Tra i servizi di *testing* offerti da ISGroup l'*Ethical Hacking* rappresenta la soluzione migliore per l'effettiva valutazione della propria sicurezza. I test effettuati comprendono tutti quelli inclusi nell'offerta di *NTP* e *WAPT*, con l'aggiunta di ulteriori tipologie di attacco.

Tra le metodologie non convenzionali vi è ad esempio il *Social Engineering*. Un'altra caratteristica del servizio di *Ethical Hacking* è quella di non utilizzare strumenti automatizzati che producano una forte evidenza della presenza di un attacco. In questo modo si simula in modo più veritiero un'organizzazione criminale che svolga, ad esempio, spionaggio industriale (nella più completa anonimità).

Output

L'*output* prodotto dal servizio di *Ethical Hacking* si concretizza in un *Report* che descrive in modo dettagliato tutte le vulnerabilità che sono state identificate e in che modo è stato possibile sfruttarle. Inoltre sarà anche fornito un piano di rientro che descriverà dettagliatamente come porre rimedio alle vulnerabilità identificate.

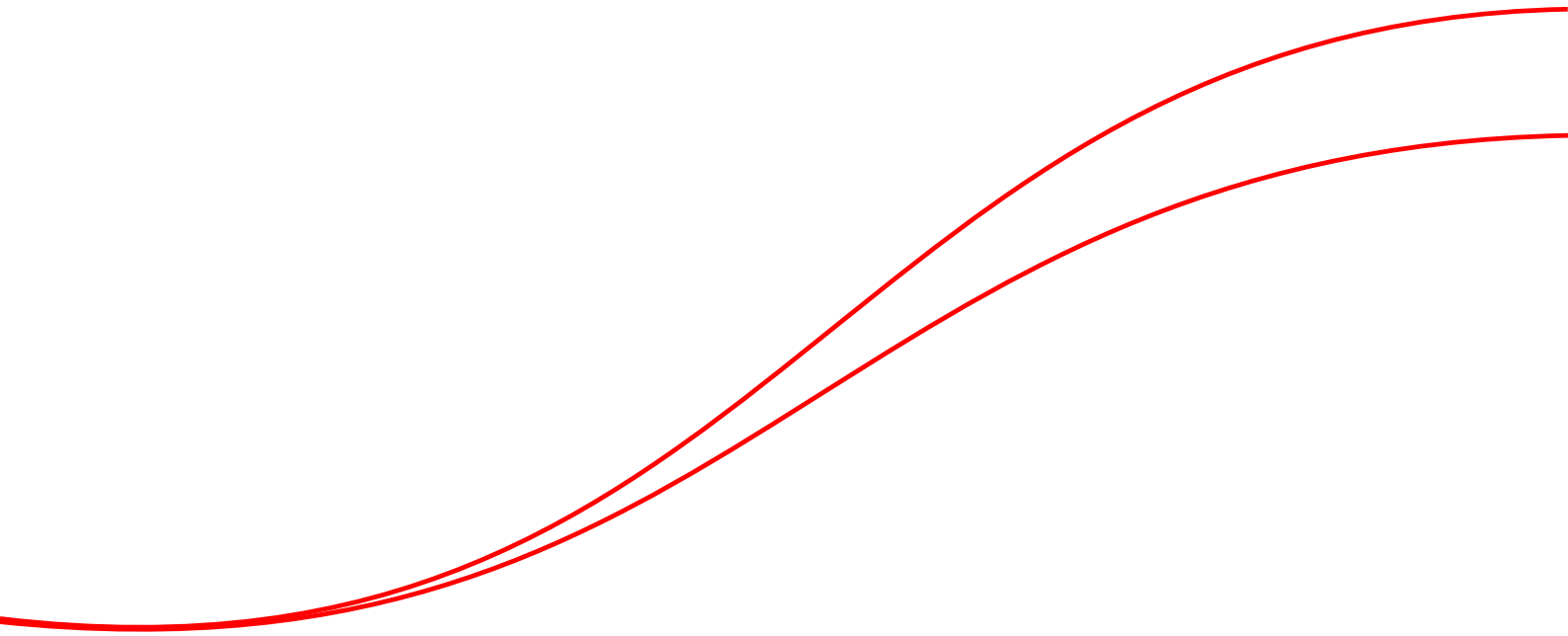
Richiedi servizi di Ethical Hacking

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

ISGroup
Information Security

CR

Code Review



www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Code Review (CR)

Il processo *Code Review* ha come scopo l'identificazione di vulnerabilità all'interno del codice sorgente. Esso rappresenta una delle fasi più importanti per lo sviluppo di applicazioni sicure, permettendo di identificare eventuali problematiche di sicurezza prima che il *software* vada in produzione riducendo sensibilmente i costi.

L'attività di *Code Review* ha un alto grado di complessità, ragion per cui è fondamentale che l'*auditor* abbia solide basi sui concetti di programmazione sicura, sulle maggiori tipologie di attacco e che abbia una buona confidenza con la lettura e analisi del codice.

Il servizio di *Code Review* offerto da ISGroup viene effettuato da un *team* di persone con anni di esperienza sia nella programmazione che nell'analisi dei sorgenti di grandi applicazioni.

ISGroup è il fornitore ideale per le Vostre necessità di *Code Review* e opera con serietà secondo *standard* internazionalmente riconosciuti ai più alti livelli di qualità grazie al costante impegno nell'ambito della ricerca. Contattateci per informazioni e richiedete un preventivo personalizzato.

Descrizione del servizio

Il processo si compone fondamentalmente di due fasi, in quella iniziale l'intera applicazione viene esaminata da uno o più *tool* di analisi statica. Tali *tool* hanno lo scopo di simulare l'esecuzione del codice e di identificarne le eventuali vulnerabilità. Questo approccio ha dei grossi vantaggi rispetto al solo *testing* dell'applicazione, perchè si ha piena consapevolezza del comportamento dell'applicazione.

Nella fase successiva si analizza manualmente il codice concentrandosi sulle parti più delicate dell'applicazione. L'analisi viene effettuata da un *team* eterogeneo di persone altamente specializzate, con il fine di identificare tutte le varie vulnerabilità che non sono immediatamente identificabili.

Questa seconda fase è necessaria poichè i *tool* automatici non sono in grado di identificare correttamente tutte le vulnerabilità a causa dell'intrinseca complessità di tale compito.

Output

Alla fine dell'attività viene presentato al cliente un *Report* composto di due sezioni:

Executive Summary

Riassume le problematiche riscontrate nel codice sorgente dell'applicazione ed eventuali errori di implementazione. Inoltre fornisce una valutazione del livello generale di sicurezza.

Technical details

Indica per ogni problematica individuata la sezione dei sorgenti in oggetto, una spiegazione dettagliata del problema individuato e la sua soluzione (*Remediation*).

Richiedi servizi di Code Review

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

ISGroup
Information Security

Training

Training/Formazione

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Formazione e Training (EDU)

ISGroup eroga servizi di formazione e *training* sulle maggiori tematiche di sicurezza esistenti.

Il percorso di formazione ha il compito di formare tecnici che siano capaci sia di esaminare approfonditamente la sicurezza di un sistema che di proteggerlo contro minacce esterne.

Formare il proprio *staff* di sistemisti o sviluppatori è fondamentale per ridurre i costi legati alle problematiche di sicurezza.

Descrizione del servizio

I corsi offerti comprendono sia una parte teorica che una parte pratica. Durante le sessioni di teoria verranno illustrate le metodologie e il funzionamento dei vari aspetti tecnologici che coinvolgono l'argomento. Nelle sessioni di pratica verranno dati ai partecipanti delle prove (dette anche *challenge*) che dovranno essere portate a termine.

Questi *challenge* consistono in applicazioni/sistemi che dovranno essere esaminati o messi in sicurezza (a seconda del tipo di corso). Ogni prova avrà un tempo limite, e saranno date in ordine crescente di difficoltà. Al termine viene rilasciato un attestato di partecipazione al corso e recante le abilità acquisite.

Gli argomenti su cui vertono i corsi forniti da ISGroup sono:

- Secure Coding, Web Application Code Review
- Web Application Penetration Testing
- Network Hardening
- Hardening Linux, Windows, Solaris

Offesa

I corsi relativi ad aspetti di offesa si concentrano su metodologie utili nel sovvertire o violare sistemi o applicazioni, con il fine di prendere il totale controllo della macchina (anche detto "effettuare il *take over*"). In particolare verrà trattato, in modo pratico, quanto già esposto nella parte teorica, mostrando esempi significativi di vulnerabilità in applicazioni reali.

Il corso di Offesa offerto da ISGroup garantisce la formazione di tecnici altamente qualificati che siano effettivamente in grado di esaminare la sicurezza di un sistema, ed eventualmente trarre vantaggio dalle vulnerabilità esistenti per poterne prendere possesso.

Difesa

I corsi relativi ad aspetti di difesa si concentrano su metodologie utili nel mettere in sicurezza sistemi o applicazioni. Nella parte teorica verranno trattati concetti come l'*hardening* dei sistemi o la scrittura di codice sicuro (a seconda del tipo di corso trattato).

Nella parte pratica verranno presentati dei sistemi o delle applicazioni vulnerabili e il partecipante dovrà essere in grado di metterli in sicurezza oppure, in caso di applicazioni, di capire dove è stato commesso l'errore di programmazione. Gli esempi mostrati saranno presi direttamente da applicazioni realmente vulnerabili.

Richiedi servizi di Formazione e Training

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a sales@isgroup.it potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.

Starter Kit

ISGroup
Information Security

Offerta promozionale per i nuovi clienti

Lo Starter Kit è una promozione commerciale di ISGroup che permette a chi non ha ancora beneficiato dei nostri servizi professionali di testare il proprio sito web esposto ad internet ad un prezzo estremamente vantaggioso di *420 Euro + IVA*.

L'offerta non sostituisce un'analisi completa quale un Web Application Penetration Test (WAPT) ma è sicuramente indicativa del reale livello di sicurezza di un sito o un'applicazione Web.

L'attività viene svolta da un tecnico *Senior* per la durata di un giorno lavorativo ed evidenzia le problematiche di sicurezza più evidenti. Le tecniche utilizzate non sono invasive al fine di evitare danni all'infrastruttura del cliente.

La promozione Starter Kit *permette di conoscerci e verificare la cura e dedizione con cui svolgiamo il nostro lavoro* al fine di instaurare una proficua collaborazione.

Distinti saluti
Francesco Ongaro, ISGroup

Verifica la sicurezza del tuo *sito web* ad un prezzo estremamente vantaggioso!

Prodotti e soluzioni di IT Security

www.isgroup.it
isgroup@isgroup.it

PIVA 03526940238
Via Badile 37, Verona 37131

ISGroup
Information Security

Tel. 045 4853232
Fax. 045 4853123

Coupon Promozionale Starter Kit

Desidero usufruire dell'offerta promozionale Starter Kit per il controllo della sicurezza del Sito, Portale o Applicazione WEB della mia organizzazione in quanto nuovo cliente ISGroup.

Azienda _____
Nome _____
Cognome _____
PIVA/CF _____
Telefono _____
E-Mail _____
Indirizzo _____

Firma

Attivabile anche online: www.isgroup.it/starter

Codice

Da inviare compilato e firmato per posta o fax (045 4853123)

ISGroup
Via Antonio Badile 37
37131, Verona (VR), Italy

* Riutilizzare la busta e piegare in modo che sia visibile dalla finestra trasparente

ISGroup
di Francesco Ongaro

Information Security Group

ISGroup
Information Security

Lettera di presentazione

- VA - Vulnerability Assessment
  Identifica le vulnerabilità in una rete
- NPT - Network Penetration Test
  Simula un attacco ad una rete
- WAPT - Web Application Penetration Test
  Simula un attacco ad un sito o applicazione web
- EH - Ethical Hacking
  Servizio completo
- CR - Code Review
  Analisi del codice sorgente
- Formazione e Training
  Formazione per sistemisti e sviluppatori

Cordiali saluti
Francesco Ongaro, ISGroup

ISGroup è una struttura indipendente specializzata in *IT Security* in grado di offrire servizi e prodotti di sicurezza informatica di livello qualitativo elevato.

La nostra struttura, essenziale, efficiente e competitiva, è composta da professionisti freelance.

Per questo ci proponiamo come ideale *Outsourcing Partner* per le aziende di ITC e IT Security.

Sulla sinistra i nostri servizi e prodotti.

Alla cortese attenzione di

PIVA 03526940238
Via Badile 37, 37131, Verona
Tel. 045 4853232
Fax. 045 4853123
www.isgroup.it
isgroup@isgroup.it

ISGroup
Information Security

Promozione Starter Kit

Tutte le informazioni e il coupon sul retro.

Verifica la sicurezza del tuo sito web ad un prezzo estremamente vantaggioso in tre semplici passi!

1 *Voi ordinate*

2 *Noi testiamo*

3 *Voi risolvete*