

Alessandro Bassi

Via Repubblica 48 , Novate M.se - 20026, Milano, Italia

eiphuntard@gmail.com

T: (+39) 3338187302

Sommario delle qualificazioni

Ambizioso specialista di sicurezza informatica di 26 anni, dedito ad offrire la più alta qualità di lavoro ed ha dimostrato capacità nel campo del penetration testing, ricerca di vulnerabilità e configurazioni di sistema relative alla sicurezza.

Certificazioni

Offensive Security Certified Expert (OSCE).....In progresso
Offensive Security Certified Professional (OSCP).....Aprile 2013
Cisco Certified Network Associate (CCNA).....Luglio 2012

Esperienze nel campo della sicurezza informatica

- Sviluppato programmi personalizzati per assistere nei test di penetrazione, valutazione di vulnerabilità e ingegneria inversa.
- Test della sicurezza di reti wireless , cracking delle password e l'individuazione di punti di accesso non autorizzati.
- Creazione manuale di shellcode in modo da eludere programmi Anti-Virus.
- Condurre elevazione di privilegi su entrambi i sistemi operativi Windows e Linux.
- Condurre Fuzzing per trovare e sfruttare stack e heap Buffer Overflows.
- Usare SSH o altri mezzi per raggiungere altre reti e macchine con accesso limitato.
- Testare manualmente parametri di richiesta come GET / POST, intestazioni HTML e cookies per vulnerabilità comuni come SQL injection , Blind SQL injection , SQL Injection di secondo ordine , inclusione di file locali o remoti, XSS, CSRF, WAF bypass etc.
- Raccolta di prove digitali tramite la creazione di immagini del disco rigido, garantendo nel contempo l'integrità dei dati.
- Analisi di codice sorgente e file di log per determinare e mitigare vettori di attacco.
- Estesa esperienza con i sistemi operativi Windows XP/Server 2003/Vista/7/8, Linux (Ubuntu, Archlinux, Redhat, Gentoo, Fedora, Debian e le comuni distribuzioni orientate al penetration testing (e.g. Backtrack, Kali, Pentoo and Blackarch).

Software di sicurezza

- Burp suite, Metasploit, Wireshark, programmi per crackare passwords (e.g. john the ripper, pyrit etc), Ollydbg, Immunity Debugger, IDA pro, Netcat, Nessus, Nmap, Pwdump, Sqlmap, Sulley fuzzing framework, Acunetix ed altri.
- log2timeline, log2parse, volatility, sandboxed environments per analizzare malware.
- Bash, Assembler, C, C++, Python, HTML , PHP, Javascript and Lua.

Formazione Scolastica

1999-2002 Licenza di scuola media – Istituto Gianni Rodari.

2002-2006 Istituto professionale indirizzo perito informatico – Istituto Monteceneri (fino alla 4° compresa).

Esperienza Professionale

Officina Bassi, Amministratore di rete

Novate Milanese, Milano.

2006 – 2014

Provvedere alla sicurezza e risolvere problemi di rete di vari dispositivi (ad esempio computer, cellulari e tablet), pur mantenendo un elevato livello di disponibilità della rete e riservatezza dei dati.

Installare e configurare Firewalls e Intrusion Detection Systems per fornire un livello di sicurezza ragionevole.

Analizzare i protocolli di rete con Wireshark per individuare e risolvere problemi.

Inoltre ho anche fornito assistenza con le revisioni statali bi-annuali di automobili e motocicli.

Progetti

- Sviluppato web-shells in PHP personalizzate per aiutare negli attacchi di tipo SQL Injection e altri vettori di attacco.
- Sviluppato Crypters personalizzati in modo da eludere programmi Anti-Virus. (C++)
- Sviluppato programmi in Python per interagire con reti e/o analizzarle per testare la loro sicurezza (e.g. <https://github.com/eiphunter/SPSE>)

Miscellanea

- Lingue parlate: Italiano e Inglese.
- Munito di patente.
- Aperto un blog personale sulla tecnologia per condividere conoscenze e progetti con il World Wide Web
- Profonda passione per tutto ciò relativo all'Informatica con forte enfasi sulla sicurezza.
- In costante apprendimento cerco di rimanere sempre informato sulle più recenti novità tecnologiche.
- Disposto a trasferirsi, viaggiare molto e lavorare in remoto da casa.