



H-CYBER INTRUSION

(SERVIÇO DE PENTEST & PENTEST AS A SERVICE)

CYBER EFFECT - NÍVEL 2 - PROATIVO



DESCRIÇÃO

h.cyber INTRUSION

O serviço de Pentest & Pentest as a Service consiste na execução de um conjunto de técnicas de ethical hacking, de forma a identificar as vulnerabilidades e falhas de configuração de qualquer equipamento IP ligado na rede de dados da organização.



PROPOSTA DE VALOR

Os ciberataques são cada vez mais complexos e sofisticados. Consistem em inúmeras e diferentes ameaças virtuais que proliferam-se através das redes, sendo um motivo de preocupação crescente pois as suas consequências são devastadoras, podendo provocar a perda de informação da entidade, bloqueio no acesso aos serviços e danos causados ao nível da reputação da entidade.

Este serviço permite ao cliente ter uma melhor compreensão das suas vulnerabilidades e desta forma ter a capacidade de remediar as mesmas, antes que possam ser exploradas.



CARACTERÍSTICAS DO SERVIÇO

► **Análise e Gestão de Vulnerabilidades:** Fornecimento de recursos de análise de vulnerabilidades para realizar avaliações/auditorias contínuas e dinâmicas das infraestruturas/sistemas de forma a identificar quaisquer vulnerabilidades no software ou configurações. Inclui a realização das seguintes verificações:

- Inventário de todos os dispositivos ligados.
- Inventário de software autorizado e não autorizado.
- Inventário do estado de correção e atualização de todo o software e sistemas operativos instalados.





H-CYBER INTRUSION

(SERVIÇO DE PENTEST & PENTEST AS A SERVICE)

CYBER EFFECT - NÍVEL 2 - PROATIVO

- Análise à configuração de segurança ao nível do hardware e software em computadores, servidores, equipamentos mobile, ativos de rede (routers, firewalls, switches), equipamentos wireless.
- Identificação das configurações contra malware e mecanismos de segurança instalados nos endpoint.
- Configurações seguras para dispositivos de rede geridos localmente.
- Sistemas de Controlo Industrial e Sistemas de Gestão Building, para assegurar a conformidade com as normas, políticas, diretivas, processos, procedimentos e documentos de orientação de segurança aprovadas internamente pelos clientes.

► **Suporte na Remediação:** Os relatórios personalizados, entregues com o detalhe da informação que foi possível recolher via meios OSINT, risco geral da instituição e detalhe de cada vulnerabilidade, caracterizada da seguinte forma:

- Descrição da vulnerabilidade;
- Identificador;
- Impacto;
- Probabilidade;
- Recomendação;
- Custo da mitigação;
- Sistemas afetados;
- Nível de Risco;
- Evidência, de forma a validar tecnicamente que não é um falso positivo.

► **Teste de Intrusão:** Fornecimento de recursos para avaliar a segurança de sistemas ou redes informáticas, através da simulação de ataques de hackers, de forma a identificar reais vulnerabilidades.

► **Red Team:** Fornecimento de recursos para avaliar a segurança de sistemas ou redes informáticas através da simulação de ataques de hackers, sem qualquer notificação ao pessoal para além do Diretor de TI e do responsável de segurança.





H-CYBER INTRUSION

(SERVIÇO DE PENTEST & PENTEST AS A SERVICE)

CYBER EFFECT - NÍVEL 2 - PROATIVO

- ▶ **Aplicação Web/Auditoria de segurança a bases de dados:** Disponibilização de recursos para avaliar as aplicações Web com que a Internet se defronta em termos de má configuração de segurança, vulnerabilidades e más práticas de codificação, bem como identificar deficiências de segurança nas bases de dados.
- ▶ **Campanhas de simulação de Phishing/Engenharia Social:** Disponibilização de recursos para a configuração de campanhas de simulação de phishing e a sua execução. Os resultados e recomendações de remediação são fornecidos com os relatórios das campanhas.
- ▶ **Avaliação de Vulnerabilidade Mobile:** Fornecimento de monitorização em tempo real dos ativos móveis de uma organização, com o objetivo de apresentar contramedidas realistas e eficazes para limitar a divulgação de informações a pessoal não autorizado, identificação de erros de configuração de segurança, vulnerabilidades e más práticas de codificação. As conclusões e recomendações de remediação são fornecidas com o relatório de avaliação.
- ▶ **Network Scanning:** Disponibilização de recursos para realizar o scanner em redes com ou sem wireless, para identificar e remediar potenciais falhas de segurança. As conclusões e recomendações de remediação são fornecidas com o relatório de avaliação.
- ▶ **Teste de intrusão em redes wireless:** apoio na identificação de redes Wi-Fi, com execução de várias técnicas de hacking, tais como cracking de encriptação, sniffing e sequestro de sessões, identificando oportunidades de penetração na rede através da utilização de medidas de controlo de acesso ou evasivas e identificando identidades e credenciais de utilizadores legítimos para aceder a redes e serviços.



VALOR ACRESCENTADO

As principais diferenças na forma como um Pentest é executado por nós:

- » Desenvolvimento de exploits, criamos novos CVEs (alguns com a respetiva publicação), de acordo com o ambiente de cada cliente.
- » Testamos todos os sistemas & redes (infraestruturas, ATMs & POS, mobile, aplicações web, bases de dados, wireless, perímetro).





H-CYBER INTRUSION

(SERVIÇO DE PENTEST & PENTEST AS A SERVICE)

CYBER EFFECT - NÍVEL 2 - PROATIVO

- » Customizamos os testes, de acordo com o ambiente informático do nosso cliente, validamos (manualmente) novos exploits/CVEs, que possam afetar diretamente o cliente.
- » Mostramos tecnicamente aos nossos clientes como fazemos, para promover a troca de experiências e conhecimentos.
- » Combinamos vulnerabilidades de baixo risco, de forma a escalar privilégios dentro de uma infraestrutura.
- » Utilizamos várias fontes de informação (OSINT, MITRE, CERTs,...) que utilizamos numa framework integrada, garantindo um vasto leque de ações.
- » Utilizamos várias metodologias (black box, grey box ou white box) e frameworks (PTES, OWASP, OWF, PTF, OSSTMM, W3AF,...).
- » Integramos os nossos resultados (logs & eventos) com SIEMs, independentemente da tecnologia utilizada (temos conectores/parsers desenvolvidos para o efeito).
- » Serviço realizado desde 2014, o que nos dá uma vasta experiência na realização deste serviço.
- » O serviço pode ser realizado sob diferentes abordagens, nomeadamente:
 - One Time Shot.
 - Contínuo (entregas de relatórios semanalmente, mensalmente ou trimestralmente).
 - Execução ad hoc, de acordo com as necessidades do nosso cliente.





hardsecure
WE MAKE SECURITY

H-CYBER INTRUSION

(SERVIÇO DE PENTEST & PENTEST AS A SERVICE)

CYBER EFFECT - NÍVEL 2 - PROATIVO



PEDIDOS DE PROPOSTA / INFORMAÇÃO

Para informações adicionais ou mais esclarecimentos, por favor entre em contato através de um dos seguintes meios:



Formulário “Hardsecure – Serviço de Pentest & Pentest as a Service” (disponibilizado na página do serviço no website)



Comercial da Hardsecure:

(+351) 218 278 126

geral@hardsecure.com



Website:

www.hardsecure.com (Formulário “Solicitar Proposta”)



Rua Acácio de Paiva 16
1ºD - 1700-006 Lisboa



www.hardsecure.com



(+351) 218 278 126

@ geral@hardsecure.com