ADVANCED FOOTPRINTING

KEY SERVICE COMPONENTS

- Analysis of the nominated domains and/or sub-domains plus any discovered domains and/or sub-domains where there is a very high degree of infrastructure sharing between the domains
- Analysis of the nominated IP addresses including any discovered addresses where there is a very high degree of infrastructure sharing between the domains
- Investigation of the registrar exposure of the above domain names and IP addresses
- Investigation of 3rd-party DNS Name server or Mail Exchange server dependencies
- Investigation of any exposed private IP addresses
- Discovery of any websites owned by the organisation, or claiming to be representative of the organisation
- Scanning of websites for any data that would assist a would-be attacker in gaining a foothold or offer a platform allowing a would-be attacker deeper ingress to the organisation
- Conducting multi-engine scans against discovered infrastructure for open or listening ports
- Identification of services behind the discovered ports and exploitable vulnerabilities presented
- Discovery of any web applications being exposed to the internet
- Discovery of any web applications being exposed to the internet and exploitable vulnerabilities within the applications
- Harvesting of employee and executive email addresses discovered from publicly accessible sources
- Collating discovered and harvested data and comparing the results against open source vulnerability and exploit databases
- Performance of contextual, business-orientated risk analyses on the findings

SERVICE DESCRIPTION

“Footprinting” is a method of discovering information on the Internet either owned by, related to, or strongly associated to an organisation. Typically, this is performed as a part of reconnaissance conducted before an attack where a malicious actor will collect and analyse publicly available information about the intended target in an effort to map out the attack surface of an organisation or its employees.

Understanding and monitoring your potential Internet attack surface is a critical part of defending your organization and may also reveal spoofed websites being used as phishing lures or abusing the organisation’s brand.

Using techniques and methods identical to those employed by malicious actors, either as a limited test where domain names and/or IP addresses are supplied by the client, or as an unlimited test against any domain names and/or IP addresses discovered from publicly accessible sources, SecureData follows a formal methodology to mine information about DNS domains, host names, IP addresses and email addresses from various Open Source data sources.

KEY BENEFITS & DELIVERABLES

Real-World testing: Manual supervision of assessments applying 18 years’ worth of Ethical Hacker skills and experience in manipulating scanning techniques to achieve optimised results.

Asset identification: Forward and reverse analysis on the domains as representatives of the organisation’s trading identity with third-party analysis resolving unmanaged name and/or mail dependencies.

Extended visibility: Review the IP address estate for addresses owned by the organisation and those used within a shared infrastructure.

Service discovery: Discovery of any open or listening ports exposing publicly accessible services.

Vulnerability discovery:

- o Recursive discovery and analysis of the organization’s domain name servers for DNS misconfigurations and vulnerabilities.
- o Establish the configuration and patching levels of the discovered services and whether these present any exploitable vulnerabilities.
- o Analysis of any nominated and/or discovered web applications susceptible to attack, for example MYSQL, SMB or remote desktop attacks

Threat management: Comparing harvested data against online vulnerability and exploit databases defines risk levels.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com