PRODUCT SHEET

Hackers Reconnaissance

What is Hackers Reconnaissance?

Reconnaissance is the first step in attempting to hack into an organisation. This discovery phase assists an attacker with the methodology they will choose when attempting to breach your defences.

Attackers utilise your information to craft social engineering campaigns and target your employees through phishing emails. They can also attempt to acquire personal information to add legitimacy to communications with the potential victim.

The GCI security team has compiled a list of reconnaissance tasks using the latest security technologies, giving you an insight into your security posture on the Internet and Dark Web from the eyes of an attacker.

The Reconnaissance Report will identify hidden or publicly available company or employee information available on the Internet or Dark Web. This information ultimately provides you with the visibility to change or adapt your security posture accordingly, reducing the likelihood of this information being successfully utilised in an attack.

Key features

Using the latest hacker's tool kits, a GCI security specialist will run a comprehensive set of tests against your organisation to identify and recommend improvements to your security posture.

By acting upon this information, you can reduce the ease of an attack and the threat actor may move on to a different target altogether. Both passive and active reconnaissance are combined to detail the risks.

Passive Reconnaissance is collects information about a company or a member of staff using information available without making direct contact.

Active Reconnaissance is collects information by engaging with your network or employees through various techniques such as Vulnerability Scanning, Social engineering and network probing.

High-level summary of reconnaissance tasks:

- **Advanced Website** information is validated to highlight how attackers would select an attack vector such as a website certificate, DNS admin, hosting provider and encryption standard
- **Public DNS records** are reviewed for information useful to an attacker, ensuring DNS zone transfer is refused and any other email security layers within your external DNS are secured
- **Company Information** is obtained through passive reconnaissance techniques to ascertain if sensitive content is collectable from the public Internet
- **VIP information** leakage, analyses historic data breaches to ascertain if any or your executive team may be an easy target
- **Social media** reconnaissance via Facebook, Instagram, Twitter and LinkedIn identifies if your social media presence is giving away any information beneficial to a hacker
- **Social engineering** reconnaissance on your website identifies any potential targets and information on the company or employees
- **Dark Web** reconnaissance utilising GCI's dedicated TOR sandbox environment to inspect 'dark web chatter' relating to your organisation
- **Malicious sharing** site analysis for references to your organisation
- **Credential exposure** is ascertained by checking for your employees credentials on historic breaches

The GCI security engineer will analyse all the information gathered on completion and provide a detailed report which outlines any recommended remedial actions. A Risk and impact summary will clearly convey the priorities for resolution to ensure your security posture is improved.

ServiceNow = collaborative working
By using the ServiceNow platform - an industry-leading SaaS-based, highly configurable Service Management System, your IT teams can easily work alongside GCI's experts to quickly and easily resolve problems.

A solution before there's even a problem
Our 24/7 SIEM Monitoring and Alerting service for IT infrastructure and network traffic flags up security incidents for resolution before they have a chance to further impact your business.

Our eyes on your IT when yours are closed
Did you know that more than 30% of incidents happen at night? We offer 24/7 support and monitoring as standard for all customers.

Managed Services are the future!
59% of IT services have already transitioned from the traditional break-fix model to a Managed Service contract, and it's thought that by 2019 Managed Services will account for 20% of all IT services spending worldwide.

Customer Case Study: Thrive Homes

"Thrive has engaged the advanced capabilities of GCI's Cyber-Immune System, with the GCI Security Team. This solution encompasses an end-to-end multi-layered approach that strengthens Thrive's overall security posture to provide everything from Office 365 hardening, and Managed Firewalls, to consultancy services from GCI's dedicated Security Officers and the services of the SOC.

This provides me with the comfort that Thrive's security (that integrates people, processes, and technology) is best of breed, whilst constantly evolving to the changing threat landscape. As trusted advisors, I know that if an incident were to occur, GCI's Security Incident Response Team would be there 24/7/365 to help resolve the issue. They are more than just an extension of my IT team; they ARE Thrive's security team, and they are backed by processes that deliver an end-to-end approach from alarm response to remediation. In terms of technology, GCI's SIEM provides Thrive with enhanced threat intelligence and automation for greater visibility of activity within our environments and at the security perimeter. Security is paramount for Thrive as we handle large amounts of sensitive information, including personal details of our tenants. Having this technology in place reassures me that we are safe."

Why Managed Services from GCI?

With a team of 180-strong technical professionals to assist your users on a truly 24/7 basis and partnerships with some of the most well-renowned names in IT, GCI have the skills and expertise to deliver comprehensive, cost-effective IT support. Indeed, we've reduced budgets by 25% on average for our Managed Services customers!

REQUEST A FREE CYBER SECURITY CONSULTATION

If you would like to book a complimentary consultation or find out more about our solutions, please contact enquiries@gcicom.net, or call 0844 443 433.