Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

caseStudy

How an online retail group was able to understand its open attack vectors and how to withstand a real-world attack with a red team exercise

The Requirement

An online retail group, comprising of four separate branded ecommerce sites, was looking to gain a better understanding of its current threat landscape and vulnerabilities.

The retail and ecommerce industries had been the target of increasingly frequent and public cyberattacks over the previous year. The retail group wanted to protect brand reputation across all sites and ensure that it wouldn't be the next to fall victim.

The retailer had already implemented a number of security measures, however it wanted to understand how it was seen by cyber criminals, how well the organisation could withstand an attack, and the effectiveness of its defensive cybersecurity measures in detecting assessing and reacting to a cyber incident.

The Solution

Having a long-standing relationship with DigitalXRAID and previous successful security testing engagements, the online retail group contacted the team to discuss its red team exercise requirements.

Once the online retailer's objectives and requirements had been fully understood and scoped, the red team exercise began.

Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

caseStudy

The first stage of the red team exercise was to perform extensive reconnaissance of the agreed targets.

Using Open-source intelligence (OSINT) tools and resources to gather information from public platforms and the dark web, the DigitalXRAID team were able to identify top level domains and IP addresses or infrastructure that was running out of date software. The team were also able to perform 'fingerprinting' which allowed them to determine infrastructure device types and services including open ports, or potential access points.

The team were able to identify a large number of breached credentials across the group.

As part of the attack planning stage, the DigitalXRAID team compiled a full list of most likely successes.

The team also discovered multiple VPN servers, one of which hadn't yet been upgraded to utilise two-factor authentication (2FA).

Following the attack planning stage of the engagement, the first attack attempt, or exploitation, utilised the breached credentials on a 1-1 basis to stay under the radar - rather than a brute force attack method.

The team were able to successfully access the retailer's network and download its VPN configuration. Within two hours of starting the attack phase of the red team exercise, the team had access to the full internal network.

Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

The Results

The red team exercise, coupled with previous internal and external infrastructure penetration testing, has provided the retailer with a full review of its systems and networks and a better understanding of where any open attack vectors exist within the group's ecommerce sites and entire business infrastructure.

Using all the information gathered from the reconnaissance phase and advice shared by DigitalXRAID in the comprehensive report following the red team exercise completion, the retail group is now able to understand its risk and remediate any vulnerabilities to better protect against cyberattack.

caseStudy

To see how DigitalXRAID could help you protect your systems, applications and data, get in touch with us today!

DigitalXRAID are an award-winning managed security services provider dedicated to providing our clients with state-of-the-art cyber security solutions. We specialise in Vulnerability Management, Threat Intelligence, Information Security, PCI-DSS, Penetration Testing, Managed Security Services, Security Consultancy, and offer a fully managed Security Operations Centre (SOC) for your complete cyber security protection.

Visit www.digitalxraid.com
Contact us:
0800 090 3734
info@digitalxraid.com