Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

How a medical research facility was able to understand risk and ensure its infrastructure is fully protected with a red team exercise

The Requirement

A UK based medical research facility wanted to gain a better understanding of its current threat landscape, in the wake of an increase in cyberattacks experienced within its industry.

The organisation was looking for a cybersecurity partner to perform an internal and external infrastructure penetration test. The aim of the test was to provide visibility of current vulnerabilities and where the company's most prominent risks, which could be exploited by hackers, were located.

The organisation engaged DigitalXRAID to discuss the penetration testing project, however as part of the scoping phase DigitalXRAID's experts suggested that a red team exercise would be more effective to achieve the medical research facility's objectives.

A full red team exercise would highlight how a malicious actor might manipulate any risks or vulnerabilities that could be present in the network.

caseStudy

Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

caseStudy

The Solution

The medical research facility chose to continue the engagement as a full red team exercise provided by the DigitalXRAID team.

The scoping phase focused on key objectives that the red team exercise needed to achieve including; Obtain domain or admin level permissions, exfiltrate data including login credentials, gain access to an endpoint or server within the network, move laterally across the network.

All objectives needed to be achieved without the medical research facility's IT and Security teams becoming aware of the exercise.

The first step in DigitalXRAID's red team exercise methodology was to perform extensive reconnaissance using Open-source intelligence (OSINT) tools and resources to gather information from public platforms and the dark web, looking for top level domains and any IP addresses or infrastructure that was running out of date software.

Following the attack planning stage of the engagement, the first attack attempt utilised breached log in credentials VPN portals discovered during the reconnaissance phase.

This log in attempt failed and was quickly identified by the facility's IT and Security teams.

The next step was to test an access attempt, or exploitation, using login credentials, to ramp up the exercise. The user profile that the team had been provided with was very well contained in terms of permissions.

The aim of this attempt was to spend some time on the internal networks, looking to gain access controls. The VPN access was very well isolated, so the team were unable to access more than business printers on the internal network.

Red Team Exercise - Case Study

DigitalXRAID
CYBER SECURITY EXPERTS

Service:

Red Team Exercise

The Results

The DigitalXRAID team were unable to gain access into the medical research facility's entire network or move laterally within networks once inside.

The organisation's IT and Security teams were able to identify where the red team exercise was being conducted at every step, using proactive monitoring, and effectively stopped access very quickly. This proves a strong resilience against cyber threats.

At the completion of the red team exercise, DigitalXRAID supplied a comprehensive report that outlined all the information gathered during all phases of the engagement, showing how an attacker would view the organisation. This included any publicly available information gathered during the OSINT reconnaissance phase.

The medical research facility has had external validation that its approach to cybersecurity is thorough and at that point in time, there were no risks or vulnerabilities to exploit in its infrastructure. It also has a deeper understanding of how it can withstand a real-world attack.

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