PCYSYS

Case Study

NHS Royal Bolton Hospital
Automated Penetration Testing

NHS
Bolton
NHS Foundation Trust

PenTera™

NHS Bolton
NHS Foundation Trust

PenTera, the automated penetration testing platform, provides Royal Bolton Hospital the ability to quickly and frequently pen-test their network and detect the most pressing needs in their growing and ever-changing IT environment.

Quote

" Not only does PenTera help guide the team to the vulnerabilities that need to be corrected, it also provides the ability to confirm the effectiveness of security policies and remediation patches while reducing the costs. "

Brett Walmsley
Chief Technology Officer

Customer Profile

- NHS Hospital with 30 locations expanding to 60
- 8,000 employees and 800 beds
- Homogeneous IT and cybersecurity team employing the latest cyber security technologies

Challenges

- Maintaining a strong cyber posture across all facilities in a dynamic IT network environment
- Validating changes in the network without opening up new and unexpected vulnerabilities
- Validating all cybersecurity defenses are properly configured in accordance with policy
- Enable a small team to oversee the cybersecurity risk of a large network 24/7

Results

- Ability to run daily penetration tests providing a consistent security blanket
- Continuous penetration testing insights, identified vulnerabilities and suggested security improvements
- Immediate validation of security patches

" This solution opened our eyes. We were able to quickly close the most urgent security gaps. PenTera provides a security posture snapshot on-demand. "

Background

In adherence with the UK compliance regulations, Royal Bolton ran routine penetration tests on their network once a year. Although not affected by the WannaCry attack in 2017, Royal Bolton's IT team understood the need to further invest in their cybersecurity defences.

With their ever-growing network, they realised the need to improve and challenge their resilience on a consistent basis using the adversary perspective.

" In only 30 minutes with PenTera, we achieved more than 3 manual penetration testers completed over 9 days at £1,500 per tester per day. "

Challenges

Even for a security conscious team, as your environment grows, different scripts get pushed to the back of your mind and old machines that are not in regular use can create additional attack surfaces causing you to lose control of some of the IT operation.

As the Royal Bolton Hospital expanded and added new machines, users, and software, the hospital network became more complex in tandem. This increasingly complex infrastructure required constant changes to their cybersecurity defense with the ongoing addition of new solutions and hardware.

Manual penetration testing, as a way to validate cybersecurity effectiveness, is costly and only covers a segment of the network. It can not be a solution for maintaining a completely secure network.

27

30

30 minutes of PenTera = 27 working days

The Technology Evaluation

Royal Bolton was introduced to PenTera and requested to validate the solution. and observe its value in their own environment before committing to the solution. The proof-of-concept was set for one day, and was concluded in 5 hours.

The predefined success criteria were set at:
- Successful discovery & enumeration of hosts and devices within the IP range(s) selected
- Successful static vulnerability scanning and assessment
- Generating a prioritized list of pen-testing achievements within the selected segment(s)
- Display of the full attack vector for each pen-test achievement
- Review and analysis of the results, impact and remediation options
- Generating a penetration test summary report that includes an executive summary, full action report, found vulnerabilities, and remediation suggestions (action items)

The observed value as seen by the Royal Bolton IT security team was:
- PenTera provided the opportunity to have complete visibility of the vulnerabilities on an ongoing basis
- The team could observe almost instantly the most crucial remediations that need to take place
- The team could audit password and user privilege policies in the field
- Bolton's IT team was now able to "stress test" their other cybersecurity tools and check their effectiveness

> *" We felt we got back the keys to the cybersecurity kingdom by detecting and directing the security team to the most pressing needs in their ever-growing network environment. "*

> *" You don't need a whole team of external security experts, all you need is a mouse. "*

The Hereafter

Before Pcysys, Royal Bolton met compliance requirements through their annual penetration test but didn't truly benefit from the activity. With PenTera, the hospital was able to schedule regular, automated penetration tests for the different network segments and continuously improve their cyber resilience by finding new vulnerabilities and checking remediation effectiveness. With PenTera, Royal Bolton gains real insights that help identify security issues, necessary network configuration improvements, and keep their guard up at all times.

> *" PenTera turns unknown unknowns into known unknowns and acts as a warm security blanket we run on demand to make sure our network remains resilient to threats. "*

The Age of PT-on-Demand (PToD)

Penetration testing is a project. Vetting the vendor, scheduling the project, catering for logistics, hosting and accompanying 3rd party ethical hackers. We all know the drill.

PenTera changes the game by performing the work of a penetration testing team without actually employing one. Royal Bolton was able to skip the resource-heavy, costly steps of clearance, on-boarding and travel logistics for continuous pentesting. PT has become a standard and weekly procedure of the department that can now instantly audit every change in the network and test against the equivalent of a nation-sponsored hacker. Security team members can focus on their other tasks while PenTera runs in the background and when they are ready, review the vulnerabilities uncovered before prioritising the necessary remediation.

Long Term Benefits

Prioritised Remediation: With a complex network, there is an immense number of theoretical vulnerabilities. With PenTera, you can see the most critical vulnerabilities and prioritize remediation. For Royal Bolton, this has resulted in the cybersecurity team being much more responsive and efficient in handling exploitable vulnerabilities.

Perpetual Security Resilience: PenTera allows companies to run automated penetration tests as needed. Unlike manual penetration testing on a set schedule, regular automated penetration testing assures a state of perpetual security validation. For Royal Bolton, this ensures that all network-wide patches and fixes are tested for effectiveness immediately after rollout.

Cost Reduction: In addition to penetration testing cost savings, Royal Bolton is able to save on other costs by creating efficient processes for their team. Simulated and prioritized fixes assure the team spends time on the most breach-baring vulnerabilities.

Technology Investment Justification: With frequent and ever-evolving pen-testing practices, the Bolton's IT team can now validate the investment in security tools used in the past, optimize the use of current technology in place and understand where additional investments need to take place based on the attack-vectors that led to their crown jewels.

Improved Resilience: Following PenTera's implementation, Royal Bolton was able to make significant improvements to their network security. While some of these improvements represented major investments, Royal Bolton had the penetration testing insights to justify the business case for these changes.

Conclusions

Over 70% of healthcare institutions worldwide have suffered a data breach in their history and almost 50% have suffered a breach in the last year. It is vital for Royal Bolton and other healthcare institutions to maintain a strong cybersecurity posture and protect their patients' medical records.

The call of the hour is that any process or defense measure that can be automated is becoming a priority. Royal Bolton was able to deploy PenTera to secure their network and achieve perpetual validation of their cybersecurity posture.

About Pcysys

Pcysys delivers an automated penetration-testing platform that assesses and reduces corporate cybersecurity risks. By applying the hacker's perspective, our software identifies, analyses and prioritizes remediation of cyber defense vulnerabilities. Security officers and service providers around the world use Pcysys to perform continuous, machine-based penetration tests that improve their immunity against cyber attacks across their organisational networks.

www.pcysys.com

About Royal Bolton Hospital

The Royal Bolton Hospital is an NHS Trust Organisation. The Royal Bolton Hospital provides a range of inpatient and outpatient services and is a centre of excellence for maternity, neonatal and children's services.
www.boltonft.nhs.uk

PCYSYS