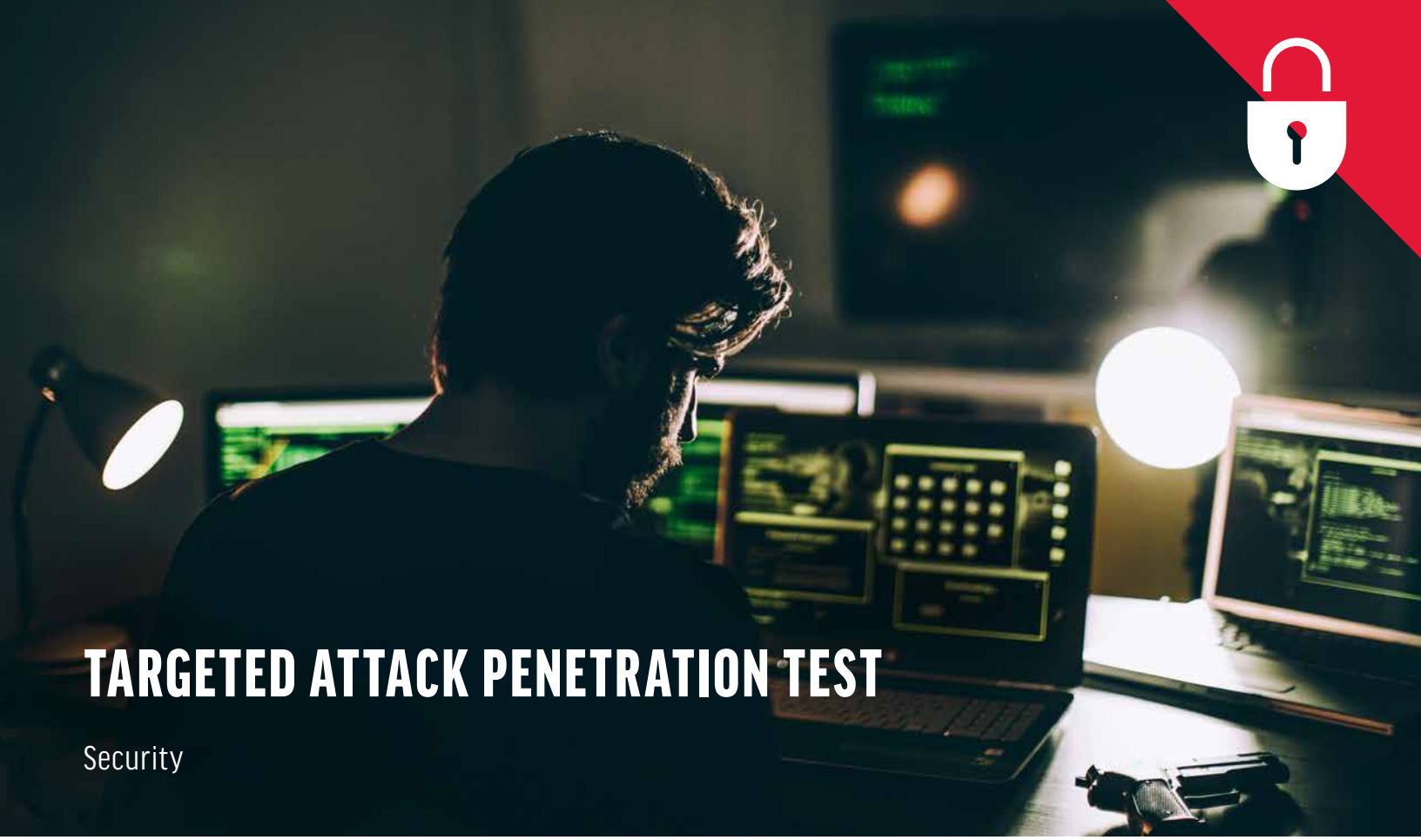


TARGETED ATTACK PENETRATION TEST

Security

ARE COMMON ATTACK PATHS PRESENT IN YOUR ENVIRONMENT?

The skill level required to execute many dangerous attack techniques continues to drop due to the increased availability of automated attack tools. Malicious actors are targeting exposed remote and cloud-based services, leveraging social engineering with open-source intelligence (OSINT) gathering to launch password-based attacks against login portals and open ports to bypass the security perimeter controls.

Using automated attack platforms, these actors are increasingly able to conduct attacks to probe for insecure services and opportunities for identity-based attacks on a grand scale, without the need to specify their targets.

TARGETED ATTACK PENETRATION TEST

CDW's targeted attack penetration test focuses on evaluating and exploiting common attack paths found in your environment. Using open-source intelligence (OSINT) techniques, our testers will gather and leverage pertinent information about the organization such as passwords found in public data breaches, to assist in the forthcoming attack phase. Next, our testers will conduct an external network focused penetration test to discover public facing services, identify attack paths for those services, and attempt to exploit vulnerabilities in order to breach your network.

We will also conduct a social engineering phishing campaign to gauge your employees' cybersecurity awareness and their ability to spot and react appropriately to suspicious emails.

Our security team will work to explore your potential risk exposure and provide recommendations on how to remediate the findings identified during the test. Evaluating your organization's defenses against common tactics will enable you to meaningfully improve your organization's security posture, and help you prepare for future security events.

FEATURES

- Our penentration testing team is based in Canada
- You will receive risk-based reporting with prioritized recommendations
- Assessments are conducted remotely

BENEFITS

- Find commonly exploited vulnerabilities in your environment and receive our recommendations on how to remediate them
- Address top cybersecurity risks
- Work toward compliance with industry standards and regulations
- Gauge your employees' security awareness level and receive our recommendations on how to improve it

DELIVERABLES

A final report consisting of:

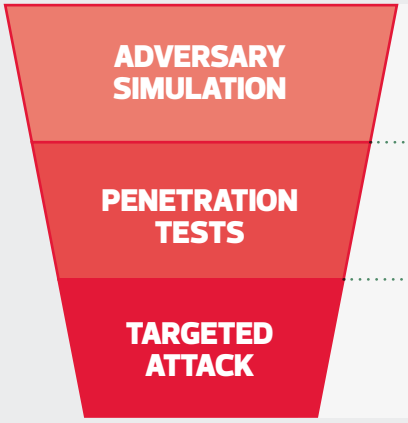
- An executive summary of work carried out and the results of the test
- A detailed review of the test findings
- A review of remediation recommendations
- A final presentation highlighting significant findings and recommendations

CDW leverages industry standards and methodologies for vulnerability assessments and penetration tests such as:

- Open Web Application Security Project (OWASP) Testing Guide, which is the standard used for web application vulnerability assessments and penetration tests
- Penetration Testing Execution Standard (PTES), which is the standard used for general vulnerability scan, vulnerability assessment and penetration methodology execution. This standard is also used for intelligence gathering, social engineering, wireless and network penetration tests
- NIST Technical Guide to Information Security Testing & Assessment (SP800-115), which is used as a general approach for conducting security testing and assessments

WHAT WE DO

Our services come in three tiers, dependent upon your requirements:



Advanced service performed to assess your organization's detection and response capabilities to real-world cyberattacks.

Comprehensive test of targeted systems for known vulnerabilities, misconfigurations and mismanagement of devices using advanced exploitation attacks.

Focused penetration test used to evaluate and exploit commonly used attack paths.

OUR TEAM CAN:

- Provide guidance on how to implement controls against common attack paths
- Help identify and address the top risks to your organization
- Assess your people, processes and technologies
- Formulate recommendations on how to remediate security gaps in your environment

WHY CDW?

Depth of expertise – CDW consultants have training and strong specializations in core areas such as adversarial simulation, web application penetration testing, network penetration testing and social engineering, with years of previous experience as system or network administrators, developers and incident handlers to help provide practical and defence-in-depth solutions to your business needs.

Continuous Improvement – We invest in our people. Training is integral to ensuring our consultants are up-to-date on the latest security trends, technologies and remediation options. Our consultants regularly attend industry-leading conferences and training sessions to maintain their level of expertise.

Track record – CDW has helped many organizations across varied industries with adversarial emulation, vulnerability and penetration testing services to help customers better understand their attack surface. CDW has performed penetration tests across many industries, including government, financial and critical infrastructure.

Full-service consultancy – CDW has the capability to assess threats, architect and implement complex IT solutions, as well as leverage specialized expertise, (e.g., engineering, cloud solutions) from different organizational areas, as required.

Verified – Leverage adversarial emulation (CDW's Red Team), vulnerability and penetration testing services with consultants who have best of industry offensive security certifications such as OSCE, OSCP, OSWE, OSWP, CEH and CRTP, in addition to networking and general security certifications such as CISSP, CISM, GSEC, Network+ and Security+.

For more information, contact your CDW account team at 800.972.3922 or visit CDW.ca/training

CDW® PEOPLE WHO GET IT™