Infrastructure Penetration Testing Primer

Penetration testing is regularly used by organisations as part of their ongoing security strategy/programme.

Infrastructure Penetration Testing is a security exercise that involves an ethical hacking team launching up to date real world attacks against your infrastructure, this can be performed from either an internal and/or an external threat perspective. We report back on the findings and how to remediate any identified vulnerabilities, this will allow you to better understand your security gaps, current security risk profile and practical steps for improvement.

Objective

Internal infrastructure penetration testing actively seeks out any vulnerabilities in your endpoints, servers, and networking systems.

External infrastructure penetration testing actively seeks out any vulnerabilities in your internet facing systems.

Both test methods essentially simulate a real attack under carefully controlled condition which can help you in determining exactly how effective your existing system defence mechanisms are, and evaluating whether or not your organisation is following security best practise.

Types of Testing

Penetration testing is generally categorized into 3 primary testing approaches. In order to deliver the outcome you wish for we recommend discussing the key objectives of the testing, your budget and time frame in order to identify the most suitable testing approach.

- **White Box Penetration Testing:** Testing is carried out from a position of full knowledge of the system to be tested. This is very helpful in carrying out extensive penetration testing.
- **Grey Box Penetration Testing:** Testing is carried out from a position of limited knowledge of the system to be tested. This allows us to focus on systems we think may be of more risk to you and value to a hacker.
- **Black Box Penetration Testing:** Testing is carried out from a position of no knowledge of the application to be tested. By being unaware of the application a tester is dependent on their own reconnaissance, using OSINT and assessment or investigative techniques. While this approach is generally perceived to be a more truthful simulation of a real life hacking campaign, it is carried out under pre-defined time and budget constraints (unlike a real-life malicious attacker) and therefore testing is likely to be less conclusive. This approach is typical suited to static and informational websites with no user login or file upload functionality.

When to Test?

Networks are a dynamic environment, penetration testing exercises should be conducted regularly, while the frequency will depend on the type of test being done and the reason for the testing, we recommend testing should be carried out when:

- Existing infrastructure is moved or expanded (including to cloud infrastructure).
- Existing infrastructure is moved or handed over to a 3rd party provider.
- New network infrastructure, internal/external facing systems or applications are introduced.
- Any significant upgrades or modifications are implemented.
- New locations or networks are established.
- After security patches are applied, or after every major OS version rollout.
- After modifications have been made to end user policies.
- After a security breach or incident response is completed.
- In the event of sale or acquisition of the organisation.

Prerequisites

Prior to testing it is recommended one takes care of the following approvals, information, and confirmations.

Sign

- The authority to perform the Infrastructure Penetration Test (This should be signed by the business owner or delegated authority).
- Non-Disclosure Agreement (NDA).

Share

- Target details in accordance to the type of testing.
- Where appropriate - testing authority provided by 3rd party hosting or service provider(s).
- Contact details for a primary and secondary technical point of contact for the activity.
- Contact details for a primary and secondary business point of contact for the activity.
- The escalation or reporting process.
- Test or dummy credentials and datasets to use during the activity.

Confirm

- Ability to perform a full back up the night before the activity.
- Ability to schedule an hourly incremental backup during the activity.
- The Incident Response or Disaster Recovery plan that is in place for any unforeseen events.
- The get-out-of-jail-free confirmation to not hold the testing provider or their employees liable for:
    - Any service disruption resulting from this activity.
    - Any attacks, intrusions, breach, or malware outbreaks during this activity, where the testing providers test machine or IP addresses are not the identified source(s).

Approach

A testing provider should have wide ranging experience with complex architecture designs, the latest attack techniques, exploits, security flaws, and digital forensics. This will allow them to combine complex penetration testing attacks with exclusive forensic techniques to achieve better outcomes.

The testing provider should follow a methodology based on industry standards such as Penetration Testing Execution Standards (PTES) and Open Source Security Testing Methodology Manual (OSSTMM).

Depending on whether the testing provider is conducting internal or external testing, their methodology should cover:

- Internal - Device and service enumeration, potential compromises through weak passwords and Windows enumeration.
- Internal - Vulnerability Assessment – using a variety of scanning techniques, and a combination of leading open source and commercial tools, to accurately identify your accessible systems and services.
- Internal - Network protocol manipulation, network traffic sniffing and network device compromising.
- Internal - Database compromise, sensitive information pilfering and privilege escalation.
- External - Open Source INTelligence (OSINT) collection – using some of the best OSINT tools and social media investigation techniques, allows a tester to perform real life reconnaissance mimicking hacking campaigns.
- External - Vulnerability Assessment – using a variety of scanning techniques, and a combination of leading open source and commercial tools a tester should accurately identify your systems and services that are open to the internet.
- External - Firewall Misconfigurations – the results of these scans, and specialised tests performed by firewall assessment tools identifies holes within your firewall configuration that can be used by remote attackers.
- Internal & External - Version Enumeration – Version information is gathered about your software and operating systems.
- Internal & External - Information Exposure – Information leaked from your systems are used to tune attacks so they have a higher success rate.
- Internal & External - Brute Force Attacks – Administration ports and web interfaces are identified. Customised login attempts are automated to compromise accounts with weak or common passwords. This can provide access to user/admin web accounts or even provide full control over your network traffic.
- Internal & External - Misconfiguration Attacks – Misconfigured services are identified and exploited to show how real world attacks are run by your systems against your systems.
- Internal & External - Exploitation Planning – Using all the information gathered, vulnerabilities are identified to determine the possible attack vectors to remotely compromise your systems.
- Internal & External - Exploitation – These vulnerabilities are exploited in a controlled fashion using a combination of leading exploitation frameworks (including open source and custom made commercial exploit packages) to compromise your systems.

Exploits

The table below is an example of commercially developed and industry sourced exploits that can be combined for use during each penetration testing exercise. Commercially developed exploits are specially designed to provide a real life Proof of Concept. The best exploits used for ICS / SCADA / Utility targets are often custom developed and not always available to all penetration test providers.

Platform	Exploits (Commercial/Other)	Unique Targets
Windows Server 2016		
Windows 10		
Windows Server 2012 R2		
Windows 8.1		
Windows Server 2012 R2		
Windows 8		
Windows Server 2008 R2		
Windows 7		
Windows Server 2008		
Windows Vista		
Widows Server 2003		
Windows XP		
Widows 2000		
Windows NT 4		
Linux		
Mac OS X		
OpenBSD		
FreeBSD		
Utility/SCADA/ICS		
Metaspolit modules		
Exploit DB-exploits		
Total	**Over 42,000**	**Over 16,000**

The success of any penetration testing exercise depends on a few factors:

1. Experience and skills
2. Type of tools used
3. Level of exploitation capability
4. Level of automated exploitation

Benefits

The benefits of Infrastructure Penetration Testing:

- Identify your information and vulnerability exposure, these are the details that can be used against you, and by malicious actors to fine tune their attack techniques for greater impact.
- Better understanding of how the identified issues can be exploited and the practical steps you can take to remediate.
- Assist in saving on remediation costs and reduce network downtime.
- Provides an evidence-based demonstration of how an internal or external attacker could compromise your systems and the associated business risks.
- Comprehensive reporting outlines for decision makers the security exposures of your border network, including high impact recommendations and root causes.
- Allows you to create a tactical action plan detailing how to resolve issues.
- Improve the protection of your business intelligence, data, IT systems, brand and reputation by implementing the remediations and recommendations.
- Build towards compliance with security regulations.

Risks

Infrastructure Penetration Testing is a simulation of a real life hacking campaign. Therefore, this activity comes with its own set of unique risks and opportunities. Some of the key risks involved are:

- Disruption or destruction of a target or service due to technical aspects outside of the testing providers reasonable ability to control.
- Disruption or destruction of a target or service due to various test activities conducted by the testing provider. Although this is unlikely to happen, it is still a possibility.

Despite the risks, performing penetration testing in a production environment using live systems is recommended and provides the following opportunities:

- Test the target in its actual live environment. This presents an opportunity for you to monitor any service disruption and the effectiveness of perimeter security controls.
- Test your Incident Response plan and Disaster Recovery procedures. This activity is performed in a controlled simulation pattern which provides the unique opportunity for you to test your IR/DR effectiveness and the ability to stop the attack.

Precautions: It is essential that you perform a full back up of the target(s) prior to the test activity, additionally it is strongly recommended that you schedule an incremental hourly back up during the activity. In the unfortunate event of target destruction or disruption, this would allow you to recover from any unintentional outage or system loss with minimal downtime or data loss.

Why Kaon Security?

Kaon Security is a highly specialised information technology security consultancy. Kaon Security team members have a wealth of in-depth technical knowledge and skill sets. Kaon Security employs leading security consultants, and invests in them, through ongoing global training and certification.

During penetration testing exercises Kaon Security provides a unique real life simulated hacking campaign experience, combining automation; multidisciplinary security skills; OSINT and forensics expertise; and most importantly our unique database of 9000+ open source, commercial, and custom built exploits.

The highly experienced Kaon Security penetration test team go beyond the point of initial access or security gap discovery, allowing us to locate additional hidden risks or threats to your environment.