# Pentera Use Cases

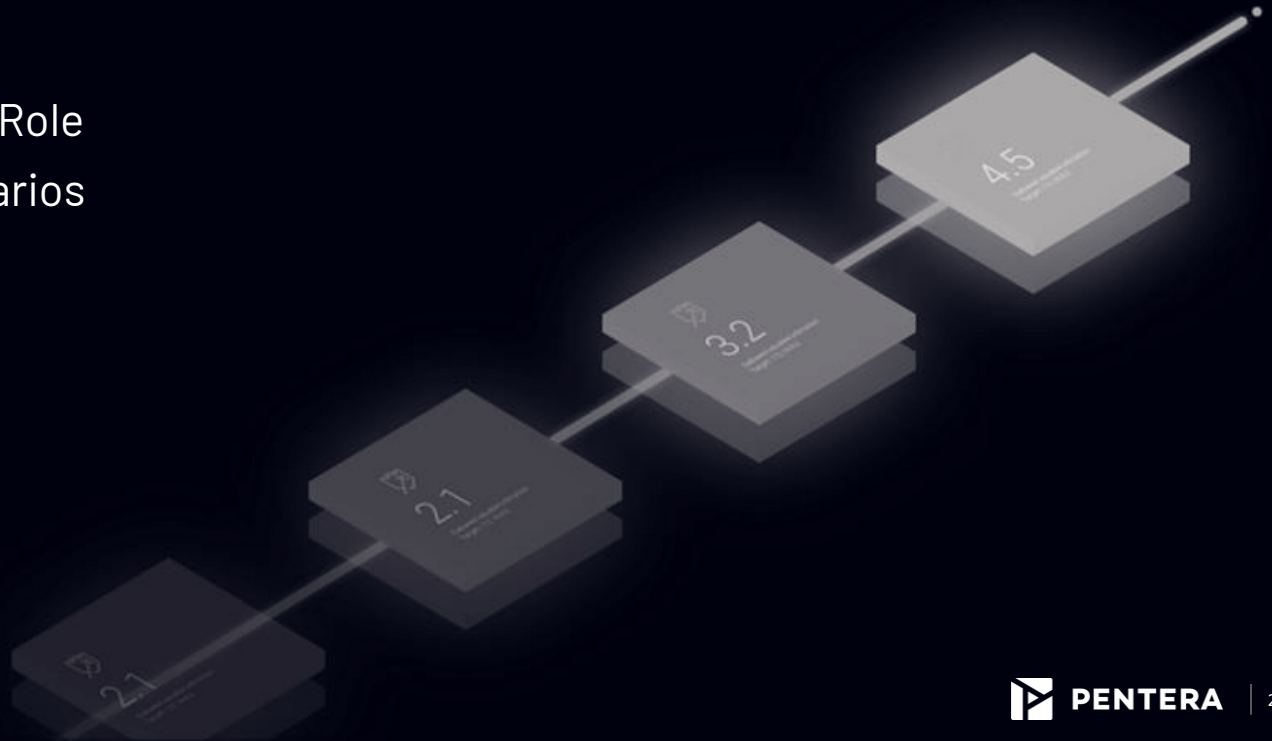
*Sion Retzkin, Penterian*

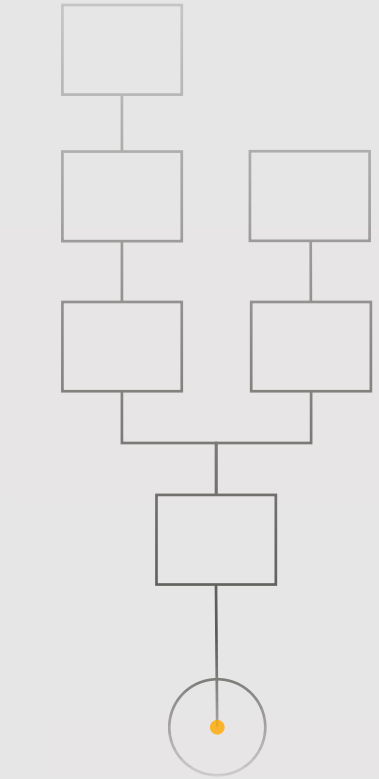
PENTERA

# Agenda

- Use Cases
- Appendix
  - Use cases per Role
  - Optional Scenarios



# Pentera Use Cases



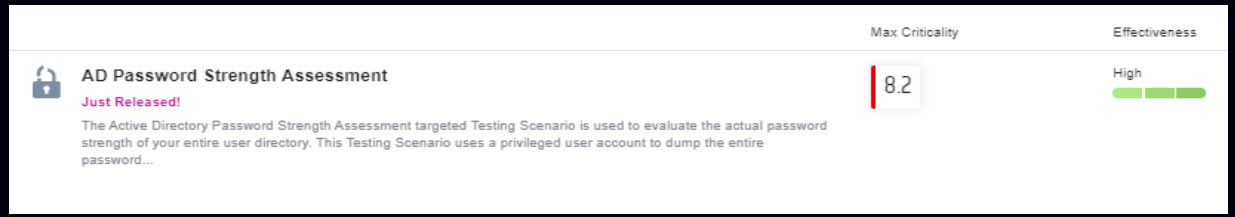
# Automated security validation

- Penetration Testing - Continuous Network Security Improvement
- Active Directory Assessments – Password Strength, A-D Limitations
- Testing Critical Assets, critical files
- Business Operations - M&A, Change Management
- Validating Existing Security Products - Validate strength of SIEM, EDR, and IDS/IPS
- Security products analysis – Test the security product you want to purchase
- Compliance
- Etc. (add as relevant)

*Create a continuous security testing program for clients that address different aspects of security infrastructure and operations delivered monthly over an annual engagement.*

# Password Policy Strength Assessment

- Active Directory Password Assessments – Pentera can download the entire password DB from the domain controller and try to crack them, providing an in-depth view of the policy and adherence to it
- This allows you to test the password policy within your environment. It often isn't the policy itself that needs improving but rather those accounts that aren't following the policy
- Pentera not only sniffs credentials on the network and tries to relay them, it also tries to crack the passwords themselves offline (on the Pentera machine, with it's GPU), to prevent locking out accounts
- Pentera can try to crack domain, local, service credentials and more, using 4 levels of password cracking (from Dictionary Attacks to permutated Brute force attacks)



# New Network or M&A network security validation

- After setting up a new network, run Pentera to create a baseline, remediate until the risk is acceptable, then retest periodically or after network changes.
- Pentera also be used during mergers and acquisitions.
  Pentera allows you to quickly assess the security of the company being acquired and what business risks you might be taking on while integrating their network into yours and to also continuously assess the network security until and after full assimilation/merge

# Segmentation Validation = Pivoting Prevention (Lateral Movement between networks)

- Pentera can help validate whether reaching isolated network segments is possible (pivoting).
- If Pentera is located on segment A and according to the firewall policy it should not be able to reach segment B, you can provide both network segments in a Testing Scenario and test if Pentera can not only scan and enumerate those machines but run actual exploits on them. This can be extremely beneficial in showing how an attacker could laterally move (or pivot) from a less to a more secure network, or start in your on-premise network and move into your cloud infrastructure, etc.
- In addition, Pentera identifies 'pivot machines' - any machine with multiple network interfaces - identifying key machines attackers could use to move laterally to other segments.

# Active Directory Weaknesses

- Manual penetration testers simply do not have time nor the ability to do a full analysis of your Active Directory environment and look for privilege loopholes within it.
  Luckily, this is a task perfect for Pentera.
- Pentera can test if relaying to a domain controller is possible, over LDAP/LDAPS.
- Pentera looks for and identifies vulnerabilities within your AD such as circular nested groups, shadow admins and other types of privilege abuse.

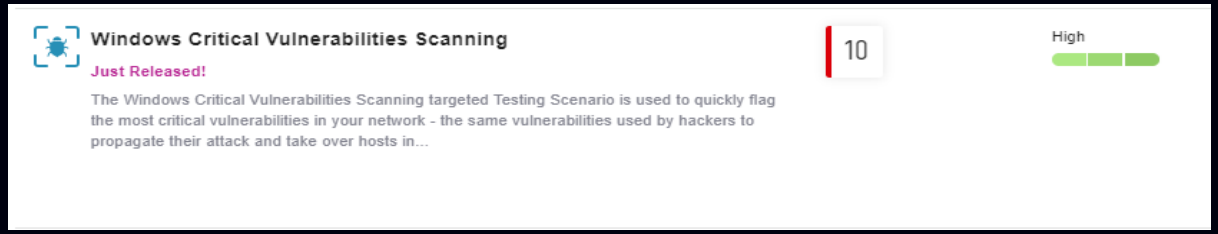
# Malware Injection = Test your EDR

- All payloads used by Pentera are safe and created by the Pentera R&D team, from scratch.
- Pentera has multiple types of payloads, ranging from ones with known malicious signatures to others which were developed by R&D and would probably not be picked up from a hash or signature perspective.
- These payloads emulate true zero day attacks and test the behavioral defenses of organizational endpoint detection and response mechanisms.
- EDRs, AVs and other types of EPP tools efficacy can thus be validated with Pentera.

# SIEM Integration = Detection Readiness

- With the ability to integrate with SIEM platforms, Pentera helps organizations validate their detection capabilities.
- EDRs & AVs connected to the SIEM should trigger alerts, preventive measures and log information in SIEMs allowing the SOC Teams to verify they are detecting everything occurring in Pentera's attacks.
- This also enables the SOC Teams to train, using Pentera to emulate attackers.

# Critical Windows Vulnerability Scanning = Find those vulnerabilities that are really putting you at risk




- Rather than a full Vulnerability Scan that takes time and floods you with countless other vulnerabilities, Pentera can run a targeted vulnerability scan on up to 20,000 machines for only the most critical ones attackers use. This would be minimally invasive and organizations can quickly check any new networks they spin up or validate existing ones.

| | |
|---|---|
| **SMBGhost (CVE-2020-0796)** | **Citrix (CVE-2019-19781)** |
| **Remove mic (CVE-2019-1040)** | **ZeroLogon (CVE-2020-1472)** |
| **Bluekeep (CVE-2019-0708)** | **Heartbleed (CVE-2014-0160)** |
| **EternalBlue (MS17-010)** | **MS08-067** |
| **SMB Signing not required** | **And more** |

# Validating the Efficacy of Incident Response Protocols

- Pentera customers run Pentera to test their Incident Response protocols and playbooks.
- Some of the actions that their ‘playbooks’ have instructed them to do in response to a breach ended up actually giving Pentera more privileges or further access to continue the attack rather than stopping it!
- Pentera can be used in this manner for tabletop exercises with its real yet benign attacks

# IPS/IDS Alert Threshold Tuning

- Pentera has multiple Stealthiness settings that it can run on in the Discovery & Enumeration phases.
- Running Pentera on varying levels of Stealthiness can help verify that the IPS/IDS tools are detecting correctly.
- Starting from full 'Noisy', SOC & Detection teams can verify their effectiveness and move stealthier, until they reach the threshold of their detection capabilities.
  This provides a true picture of what can be detected by the organization.
  (Many vendors claim to be able to detect "everything" but if the tool isn't configured correctly,
  it isn't effective)

# Critical Assets Security Validation

- Pentera provides the capability to test critical assets.
  These can be user accounts, specific machines, entire IP ranges, web services, etc.
- Exploitation of a critical asset by Pentera will trigger a 9.9 achievement demonstrating how the critical asset was exploited and providing remediation recommendations to quickly close the gap.

# Rogue Asset/Shadow IT Detection = Minimizing the unknown attack surface

- Pentera can scan entire subnets or network segments at once.
  Due to this, Pentera can often detect devices that the organization did not know were there.
  For example: IoT devices that weren't supposed to be plugged in, vulnerable computers not under the organization's control, VMs or computers installed by R&D or any other employee, unsanctioned by IT and more.
- Many devices on a network that are managed by vendors such as printers or ATMs, are actually running a Windows operating system and aren't being properly updated or managed, leaving an entry point for an attacker to enter the network and move laterally to more important assets.

# Validating Network Device security

- One of the things Pentera can do on network devices such as routers and switches is to test for the default/manufacturer's credentials being left available on these devices. This is especially important for larger enterprises that are potentially spinning up new networks constantly.

# Basic IoT Device Security = Minor Use case

- Pentera does not support IoT VA, operating system vulnerabilities, etc., but it can and will find almost all IoT devices and detect weaknesses based on common protocols such as FTP, SSH, RDP, etc. Additionally, Pentera can look for any sort of network misconfigurations that might allow an attacker to attack, such as an ATM, printer, VoIP, or any other device connected to the network and then move laterally or gather credentials/information to use elsewhere.

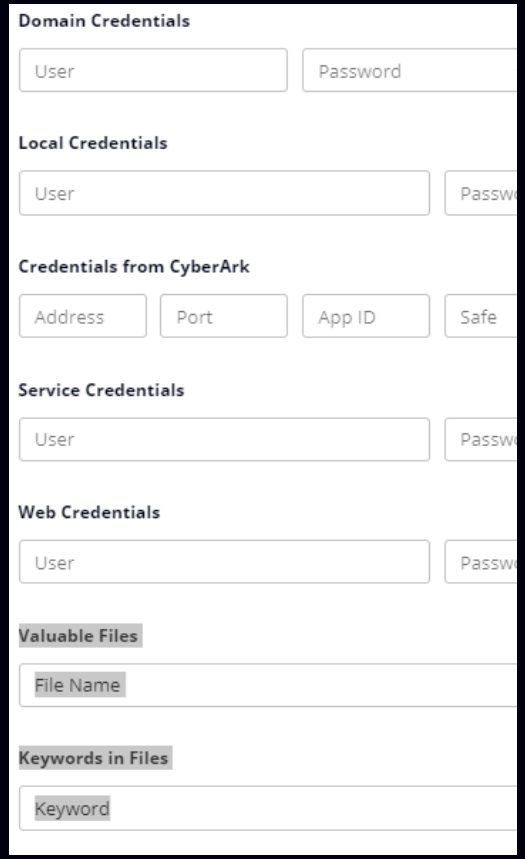
# Improve Testing Efficiency & Cadence

- Pentera allows organizations to benefit from continuous security validation - enabling improvement in the visibility of their exploitable vulnerabilities far faster than traditional penetration testing – allowing penetration testing and red teams to focus on more specific tasks
- Grey box and Targeted tests allow testing teams to validate faster - focusing on specific tasks (such as end game scenarios, default password scanning and a myriad of other testing capabilities).

  By applying machine speed and machine scale testing the organizations benefit from results in a fraction of the time traditionally seen.
- Furthermore, Pentera provides the ability to immediately validate remediations performed

# Enable Continuous Security Improvement Programs

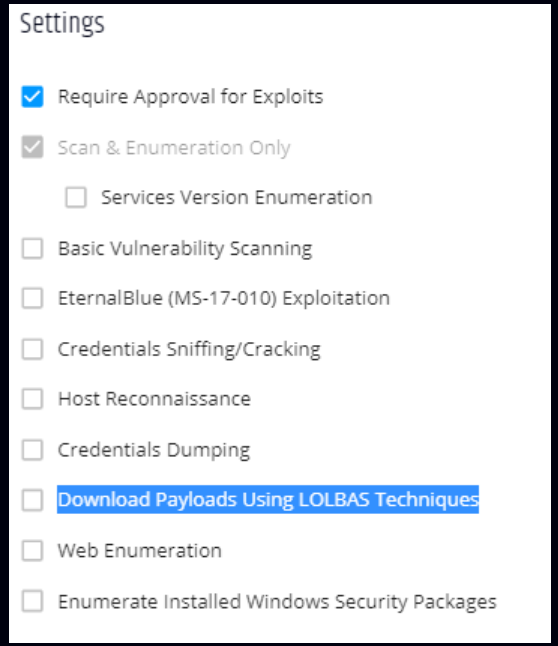
- Pentera is utilized to consistently benchmark the cyber resilience of an organization's internal and cloud network. By applying the Pentera platform to these programs, organizations benefit from consistency of measurement. As Pentera exploits are mapped to the Mitre ATT&CK Framework organizations gain consistent visibility of their resilience to ATPs. By increasing both the cadence and ability to specifically test at will, organizations are able to validate the changes in their cyber resilience over time.




# Validate Data Hygiene

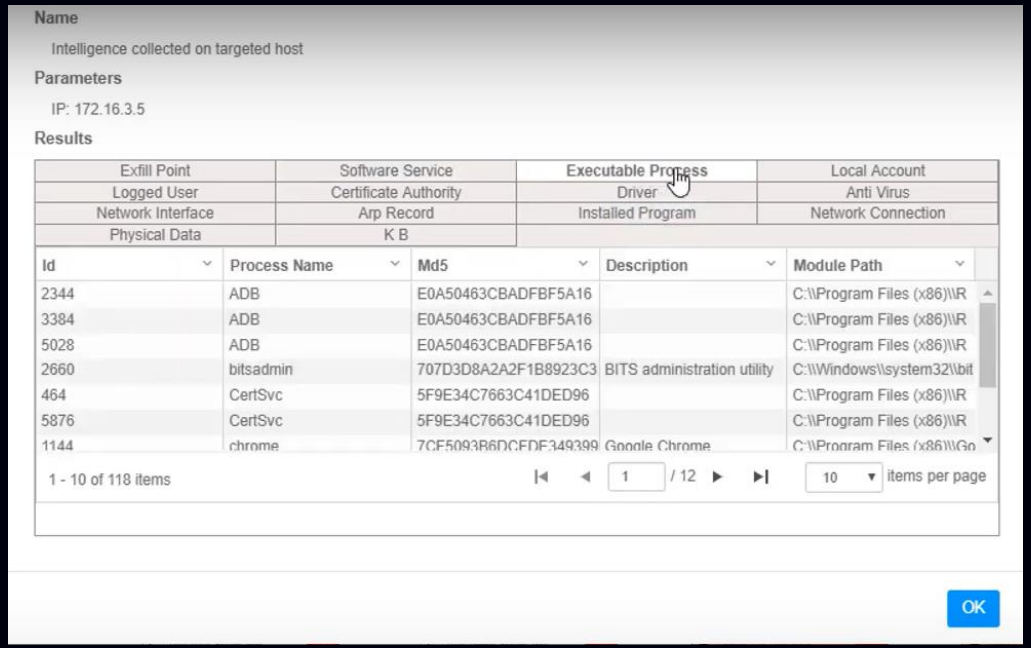
- Pentera can search for valuable files based on filenames supplied or search for content inside files, including scripts and databases.
- Regex expressions can be provided, to search for PII, credit card numbers API keys, admin account passwords, script credentials and more.

# Living Off the Land Techniques = Validating behavioural defences




- Antiviruses have gotten very good at stopping file-based attacks however fileless attacks are usually a different story. Whether the AV cannot stop them at all, or the behavioural rules cause too many issues with normal business operations, fileless attacks are a major risk to the enterprise
- For the PoV, we could pick a few test machines with different policy settings that you have within your environment and run several quick tests to see whether or not your endpoint protection is blocking out fileless attacks
- (All attacks whether file-based or fileless are SAFE and benign)

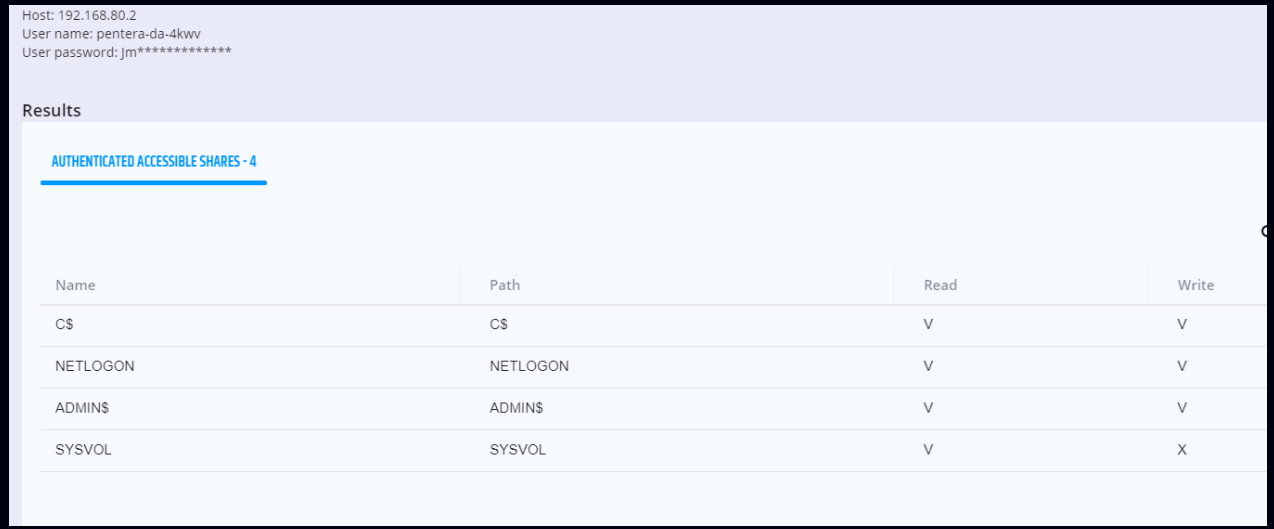
# Building Out Host Profiles = Mapping out what you have on hosts




- A Host Profile Targeted Test where Pentera's only focus is gathering as much information about the machines as possible:
  Applications installed, Network Interfaces, Antivirus, ARP Record, etc

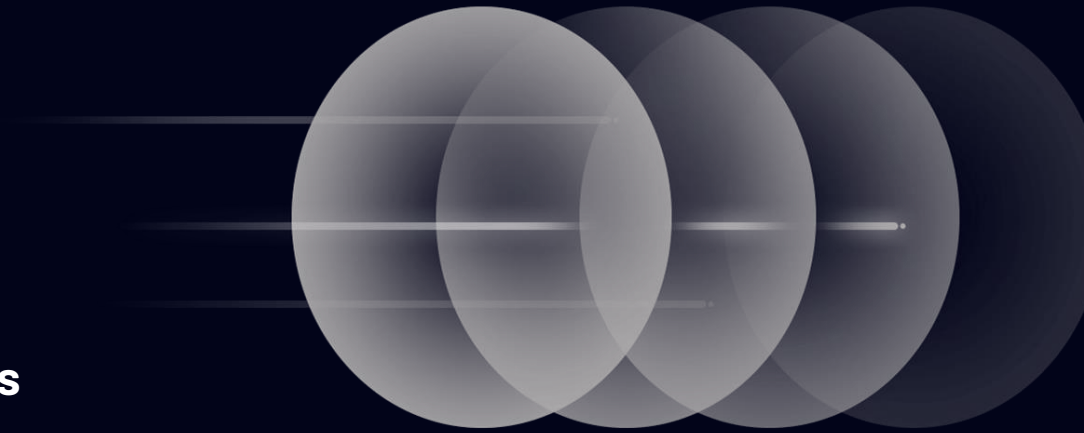
# Validate Correct Access to Data

- Have Pentera take specific credentials and identify what access those credentials have on network resources, such as shared folders.
  This helps you make sure users do not have access to any information they shouldn't have



# Appendix

1. **Use Cases per Role**
2. **Additional optional Scenarios**



# Use Cases per Role

| As the | I want to | so that | Response |
|---|---|---|---|
| **CIO** | roll out new services on time | the business benefits the services deliver are realised | formal deployment processes often mandate a penetration test before a system can go-live. The increase in speed offered by Pentera increases the cadence of security testing and avoids unnecessary delays in deployment of essential services. |
| **CISO** | receive up to date and accurate risk related data | my risk reports to the board are up to date | Pentera allows you to run penetration tests and generate immediate reports as often as you need, rather than wait until the annual penetration test where the information is a point in time and goes stale quickly. |
| | build an iterative, continuous security program | I can consistently measure and improve my security posture | Pentera can run tests as often as necessary to meet requirements. This allows for a continuous cycle of test, remediate and retest to validate and revalidate on an ongoing basis.<br>Automating this process by integrating with SIEM and SOAR tooling increases efficiencies and finally, Pentera also maps to the MITRE ATT&CK framework to allow for measurement against a common taxonomy. |
| | know the security posture of our new acquisition before we integrate our environments | our level of risk does not increase beyond our risk appetite | As well as testing your internal network and infrastructure, Pentera can be used to validate the security posture of external entities, for example during mergers and acquisitions. |
| | validate a third party service provider who needs to store and process our business data | our sensitive data is not put at risk and our compliance obligations are met | As well as testing your internal network and infrastructure, Pentera can be used to validate the security posture of external entities, for example third party suppliers and service providers. |
| | understand the risk of a successful ransomware attack | further controls can be identified and deployed to mitigate the risk | Pentera uses the same tools and techniques as typical malware that deploys ransomware. You can use Pentera to identify the issues which allow the techniques to execute successfully, remediate those issues and then rerun Pentera to prove the techniques are no longer successful. If Pentera cannot execute the techniques, you have reduced the risk of malware running successfully. |

| As the | I want to | so that | Response |
|---|---|---|---|
| **Head of Information Security** | validate that the security controls, tools and teams we deploy are configured and operating correctly | the risks they are designed to reduce are actually being mitigated | Pentera allows you to stress test your security tools and teams in many ways. For example, endpoint protection can be tested by attempting to drop payloads onto hosts. Equally, NDR can be tested to see if it detects Pentera during the discovery and enumeration phase, plus many more scenarios can be supported. |
| | test the robustness of our password policy and also Users adherence to the policy | we can improve our policies and also identify Users with poor passwords who can then receive guidance | Pentera can harvest password hashes in a number of ways; by sniffing them off the network, extracting them from memory or pulling them all from AD. Pentera will attempt to crack them and generate a report showing the results. |
| | integrate with other security tooling in my stack | I gain maximum value from my existing technology investments | Pentera integrates with other tools including:<br>• SIEM<br>• SOAR<br>• PAM<br>• Email<br>This allows organisations not only to leverage existing tools but also allows for the automation of workflows across multiple teams to test, remediate and revalidate security issues in a continuous and iterative way. |
| **Head of IT Operations** | prioritise vulnerabilities based on exploitability and impact, particularly against critical assets | my teams workload becomes manageable, our efficiency increases and we deliver maximum value to the business | Instead of reporting on what is theoretically possible, Pentera safely exploits systems and generates achievements. These achievements are then prioritised based on impact, which is customer configurable. The smaller number of underlying vulnerabilities can then be remediated in a much more timely manner. |

| As the | I want to | so that | Response |
|---|---|---|---|
| **Head of Pen Testing** | increase the cadence at which my team deliver their services across the business | business units have visibility of their security posture in a timely manner and also we meet our compliance obligations | Pentera automates the network and infrastructure testing, works at machine speed and can run overnight and at weekends. This in itself increases the cadence of penetration testing but also allows the penetration testing team to focus on specific tests such as web app, mobile, IoT and more. |
| | reduce the costs of external penetration testing | I can meet budget constraints and/or move budget to other areas | with Pentera you can run your network and infrastructure testing as often as you like to meet you requirements. This allows you to focus third party efforts on a much smaller scope such as web app testing, reducing costs. |
| **Head of Network/Infrastructure** | validate network segmentation only allows authorised services between segments | reduce both the attack surface and the risk of lateral movement | Pentera can identify and run exploits against both hosts and services available across network segments.<br>Additionally, multi-homed devices can be exploited to move laterally into other network segments. |
| | detect shadow IT | assets can be brought under corporate management | During the discovery phase, Pentera identifies all live hosts within the given scope, discovering hosts that are not known to the IT team and not under their management and control. |
| | validate build processes are followed changing default passwords on network devices | the risk of unauthorised access to those devices is reduced | Pentera tests network devices for default passwords based on the manufacturer. Additionally, Pentera can attempt to brute force credentials on those network devices. |

# Scenarios

| Scenario | Target | Purpose |
|---|---|---|
| **Cross environment connectivity (cloud to on-prem)** | Given access to my cloud environment, is it possible to extend the attack into my on-prem environment? | A well known attack vector is to steal creds, API keys etc and gain access to an organisations cloud environment. From there, the attacker can gain access to cloud hosted servers, create Users etc. With that in mind, is it possible to move laterally from there into the on-prem infrastructure particularly if I have access to credentials. This could be even more important for those organisations that purposefully keep sensitive data away from their cloud environment. |
| **Cross environment connectivity (dev to prod)** | From a dev (or any lower) environment, is it possible to extend an attack into my corporate environment? | Lower environments tend to be in a different security state than production systems. Unpatched, high privilege users (devs love having admin access), internet facing etc. If I can gain access to that environment (or even just assume it is possible) then can I not only exploit that environment but can I move laterally into more sensitive network segments and access/exfil sensitive data? Consider also source code, intellectual property etc. |
| **Due diligence of third party** | Validate security posture of third party | This scenario supports a couple of different purposes. Firstly, the due diligence period as part of M&A to define the change in risk of connecting to the third party. Secondly, confirm the security posture of a third party before providing access to company assets such as sensitive data, again pointing to supply chain risk. |
| **Regular testing of security providers** | MSSP, MDR etc | On a regular cadence I want to conduct an activity that tests the ability of these teams to perform. I will also want to test this out of ours to validate any alerting system provides the level of service we are paying for. |

| Scenario | Target | Purpose |
|---|---|---|
| **DMZ hosted server compromised using an application vulnerability, dropping a web shell etc.** | From the DMZ, an attacker will want to move laterally both across hosts within the DMZ and also into other network segments (e.g. management network, database network or internal network) | By attacking other hosts within the DMZ access to company data is possible (where applications do not logically separate tiers). For example, User data or credit card data stored in local databases.<br>Lateral movement into other network segments allows an attacker to advance their attack deeper into the customer environment. |
| **User triggered malware download and execution** | From a compromised internal host, malware will attempt the full attack lifecyle starting with the Users creds. | This scenario can lead to many outcomes. One of the most prevalent is ransomware. The malware triggered by the User action will download further modules executing the entire kill chain, including dropping ransomware on the box and others as it spreads laterally. |
| **Stolen creds used to access via VPN** | Assume the VPN endpoint is now connected to the internal network, possibly in a VPN entry network segment. From this starting point, an attacker will want to exploit the host, move laterally and continue the attack. | This scenario is based on a successful remote entry to the network, with prior access to credentials. From there, the full attack lifecycle commences, advancing the attack as deep as possible into the customer environment. |
| **Unauthorised device plugged into network** | Rather than a compromised internal host, this is a malicious (or non-managed) host gaining access to the network. Once network access is gained, then an attacker will attempt to advance the attack throughout the network, access and exfil data etc. | This scenario is based on validating network access control works correctly and also maps to real world tests undertaken by red teamers. Can I walk into an organisation and connect my device? So it is a valid exercise to think about the physical environment, what is physically accessible, are there network ports there? What can I see once I have connected the device and if I can gain network access, how far can I get in the attack lifecycle? |
| **Cross environment connectivity (inbound from a third party)** | From the network of a trusted third party, such as a service provider or a collaboration partner, what access can I gain to my network? | This scenario is related to validating third party access is locked down to the correct level to achieve the business purpose but not open the attack surface wider than it needs to be. |

# THANK YOU