SANS

Analyst Program

Product Review

Why Security Validation Matters Now: Review of the Pentera Platform

Written by **Matt Bromiley**

September 2021

PENTERA

Introduction

Information security teams face a constant uphill battle. The range of threats that organizations face continue to grow and mature daily as attackers discover new techniques and exploits to gain access to organizations. Simultaneously, enterprises are taking advantage of newer technologies to support business growth, expanding the digital attack surface at the speed of deployment. Old vulnerabilities remain unpatched while new vulnerabilities are released daily, and the ever-looming threat of ransomware promises to ruin the best-laid plans and controls.

In the face of all these hurdles, how can security teams reverse the attacker's advantage? Is it enough to implement technology and hope that, in our hour of need, they will hold the line and protect our environment? Unfortunately not. Attackers have become all too familiar with common defense techniques and deploy countermeasures with ease. Instead, organizations need to realize that continuously testing and validating to ensure your security controls *actually* do what they are supposed to is no longer a luxury. It should be a necessary part of any security program.

In this paper, we review a platform that recognizes and meets that necessity: Pentera. Formerly known as Pcysys, Pentera's platform delivers automated, continuous security control testing to augment any security team. Much more than simply testing security controls, Pentera delivers a real-time, hands-on experience that can assist defenders in deciding where to focus their efforts next.

Some of our key takeaways from Pentera's platform include:

- Real-time updates as an attack progresses through an organization, from users to systems and attacker tactics, techniques, and procedures (TTPs).
- Ranking of results and "Achievements" from testing outcomes, complete with attack patterns and mapping to Mitre's ATT&CK Matrix®.
- Outcome-specific recommendations, designed to help organizations mitigate and/or prevent threat actor techniques from being successful.

Simple control testing is only half the battle. If a control fails, security teams cannot simply stop. Ensuring that the control is rectified and functions as expected is just as critical as testing the control in the first place! With built-in remediation and validation, Pentera goes beyond security control testing and helps organizations secure their environments, with real-time testing and confirmation. Any blue team would find value in watching attacks live and adjusting controls and policy as needed in response to known, safe, and trusted activity.

If you do not test your security controls, someone else will do it for you. It is up to you to decide how much control you want over this process and the outcome!

As you work your way through our review of Pentera, we encourage you to keep a few things in mind:

- Do you currently test your security controls? ***All*** your controls?
- If so, what does that process look like? How long does it take?
- Do you rely on external parties or test internally? Or both?
- How do defenders receive the output from a test? Are changes made because of test results?

We have also sprinkled Validation Platform Tips throughout the paper to provide ways to find success with a security validation platform.

As we mentioned, testing your entire security program is no longer a luxury. However, not all organizations have found value or seized the opportunity to validate that their controls work. The problem with this position is that, eventually, someone will test your security controls. Wouldn't you rather have control over who it is?

The Pentera Platform

Before we begin our review of the Pentera platform (Pentera), it is important to quantify automated security validation. Many organizations rely on third-party tests, such as penetration tests, to help evaluate their environment. Penetration tests, when conducted by experts on offensive operations, can yield excellent results in securing your organization. Unfortunately, penetration tests often are not performed at the frequency business infrastructure changes or the blue team demands.

At the time of writing this review, dozens of organizations were dealing with an attack from an IT management software provider—an entry vector that is becoming all too common with attackers. We can assume beyond a doubt that in the wake of widespread attacks like these, organizations want to swiftly test their environments to determine if they are also vulnerable to identical or similar techniques. With automated security validation in place, they can read an article in the morning and have control test results by lunch. Defenders can make changes as needed and help confirm to executives that they are protected against the specific attacker techniques.

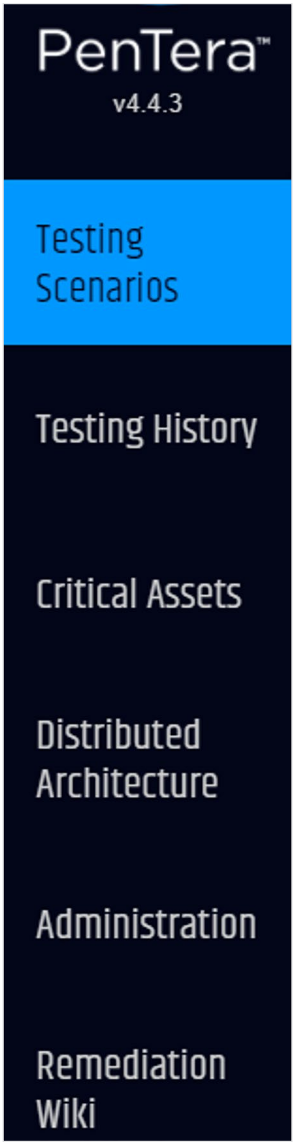
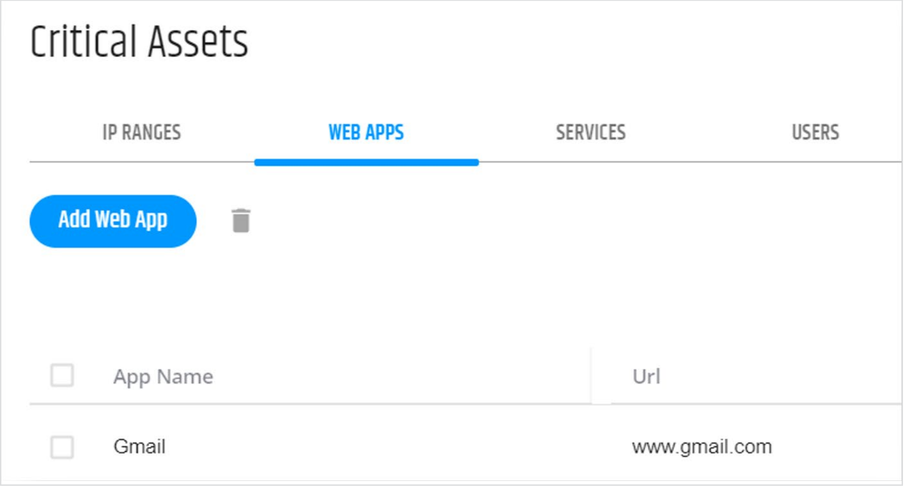


Figure 1. Initial Navigation Bar on the Pentera Homepage

Pentera's initial login screen (see Figure 1) is a simple navigation bar that allows users to access the critical functions of the platform. Depending on user privileges, they can move straight to scenarios and testing history (the primary focus of our review). However, administrators can easily configure the platform, deploy nodes, and customize Pentera to their own environment.

Aside from drilling down into the data, one of the most important links on the initial login page is the Remediation Wiki. This is a direct link to a valuable resource that helps organizations understand and mitigate against dozens of threat actor techniques and validate a security weakness was solved post-remediation. We will examine the Remediation Wiki as part of an attack later in the paper.

One area essential to effective security validation is defining the critical assets within your environment, used later for further remediation priority consideration. Pentera allows for customization of IP ranges, web applications, services, and users, as shown in Figure 2.



Critical Assets

☐	App Name	Url
☐	Gmail	www.gmail.com

Figure 2. Critical Assets Tab

When using an automated platform like Pentera, organizations should tune and customize the platform to their own environment as much as possible. This will help ensure the platform is testing areas of the environment correctly and that controls are functioning as expected.

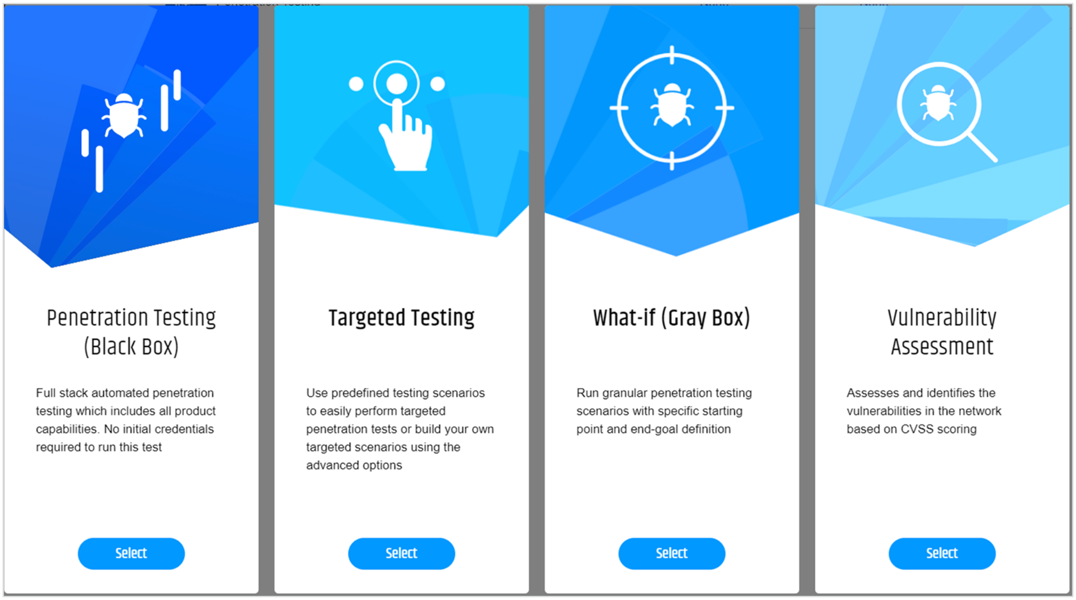
For the purposes of this review, we will focus primarily on running tests and reviewing results from Pentera. However, it is worth noting that Pentera is an automated, agentless platform. At no point during setup were we required to download or install software. Pentera is completely autonomous and orchestrates and executes all tests from the central platform. This introduces and maintains a welcome challenge for defenders: Tests use real, yet controlled, exploits to truly emulate a threat actor moving through an environment.

Validation Platform Tip #1:
Tune your security validation platform to your own environment. Provide your internal and external IP ranges and specify running services and users within the environment. These will help craft output to your environment and specific controls.

There are two primary functions for which red and blue teamers will use Pentera: running tests and reviewing the results of a test. We will examine each functionality, respectively.

Running a Test

Selecting Testing Scenarios from the initial navigation bar allows users to schedule tests. However, not all tests are created equal! As shown in Figure 3, Pentera includes a quartet of tests out of the box.



Penetration Testing (Black Box)

Full stack automated penetration testing which includes all product capabilities. No initial credentials required to run this test

Targeted Testing

Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options

What-if (Gray Box)

Run granular penetration testing scenarios with specific starting point and end-goal definition

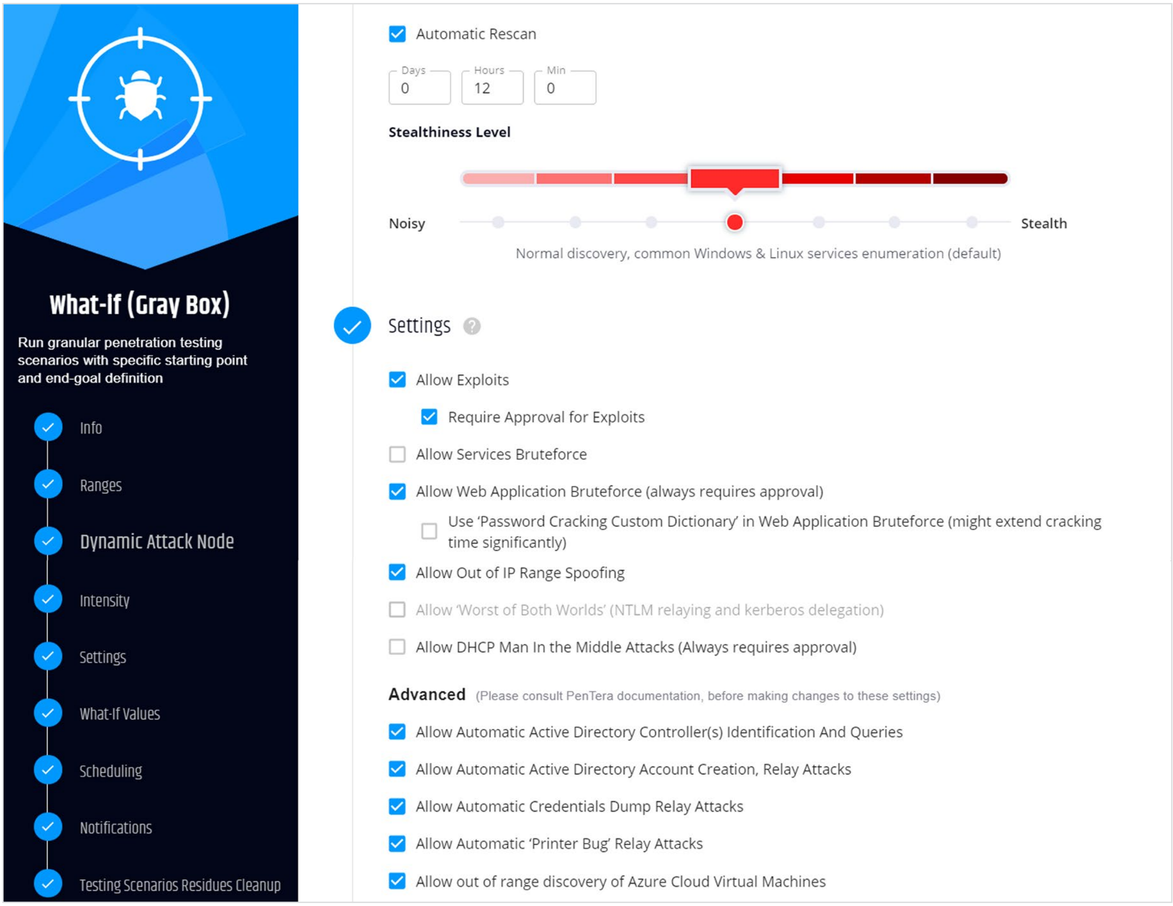
Vulnerability Assessment

Assesses and identifies the vulnerabilities in the network based on CVSS scoring

Figure 3. New Testing Scenarios

Up front, users already have enormous control over the type of tests they can run against their environment. We appreciated the control that Pentera provides to users. Test scan ranges from Black Box (fully automated) to a simple vulnerability assessment. In the middle, users can schedule targeted or What-If tests, both allowing users to select scenarios and specify starting points and/or end goals.

Validation Platform Tip #2:
Ask how much control you have over individual tests. Can you choose a starting and stopping point? Can you specify an exploit, a credential, or a system(s)? Not all tests require an entry and exit vector.



What-If (Gray Box)

Run granular penetration testing scenarios with specific starting point and end-goal definition

- ✓ Info
- ✓ Ranges
- ✓ Dynamic Attack Node
- ✓ Intensity
- ✓ Settings
- ✓ What-If Values
- ✓ Scheduling
- ✓ Notifications
- ✓ Testing Scenarios Residues Cleanup

☑ Automatic Rescan

Days	Hours	Min
0	12	0

Stealthiness Level

Noisy ○ ○ ○ ● ○ ○ ○ Stealth

Normal discovery, common Windows & Linux services enumeration (default)

✓ Settings

☑ Allow Exploits

☑ Require Approval for Exploits

□ Allow Services Bruteforce

☑ Allow Web Application Bruteforce (always requires approval)

□ Use 'Password Cracking Custom Dictionary' in Web Application Bruteforce (might extend cracking time significantly)

☑ Allow Out of IP Range Spoofing

□ Allow 'Worst of Both Worlds' (NTLM relaying and kerberos delegation)

□ Allow DHCP Man In the Middle Attacks (Always requires approval)

Advanced (Please consult PenTera documentation, before making changes to these settings)

☑ Allow Automatic Active Directory Controller(s) Identification And Queries

☑ Allow Automatic Active Directory Account Creation, Relay Attacks

☑ Allow Automatic Credentials Dump Relay Attacks

☑ Allow Automatic 'Printer Bug' Relay Attacks

☑ Allow out of range discovery of Azure Cloud Virtual Machines

Figure 4. Test Options for a Gray Box Testing Scenario

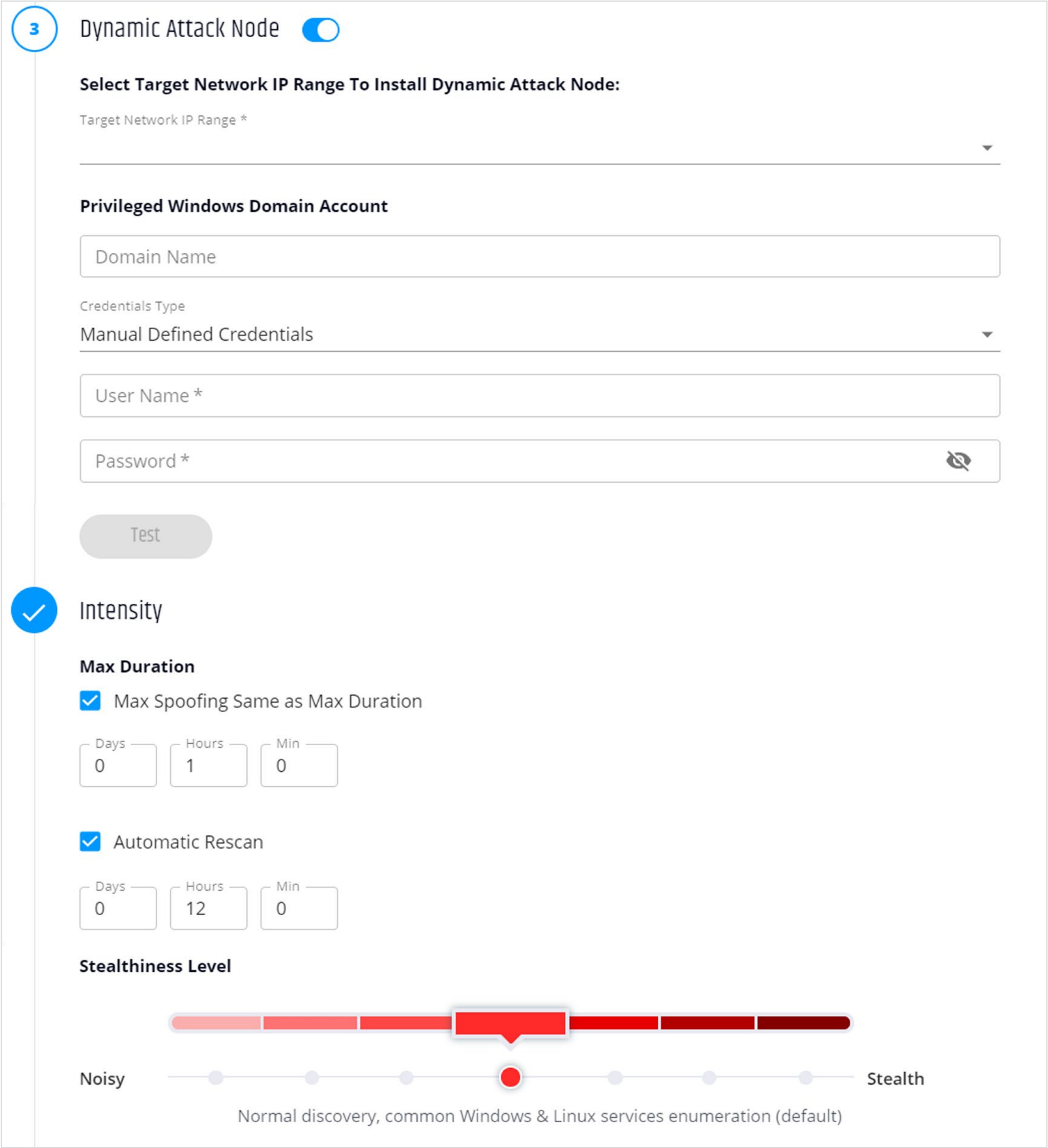
Granular control over a test is yet another value-add Pentera offers users. Not all tests require an entry or exit vector; defenders might be curious about a latter stage technique, rather than an adversary's entry mechanism. Sometimes defenders may want to test a particular application, set of credentials, or known vulnerability. Figure 4 provides a snippet of creating a What-If (Gray Box) scenario.

When scheduling a test, users can provide obvious values such as IP ranges and targets. What is more interesting, as shown in Figure 4, are the options available to mimic attacker activity. Within Pentera, users can control:

- Stealthiness of the attack
- Whether exploits are allowed as part of the test
- Scope of the test, and whether the test can "follow leads" outside of a specified range based on connectivity and validate controls outside of specified network segments

Perhaps two of the most interesting controls present in the different test types are the ability to control stealthiness and the use of an attack node. Shown in Figure 5, these controls extend the usefulness of the platform to more than just control testing. They allow users to control the level of "noise" created during an attack and perform tests on remote networks with a software-based dynamic attack node.

Some may argue that these values, along with others, give users too much control and do little to mimic "real" attacker activity. However, quite the opposite is true. Platforms like Pentera should be used to help structure better defenses. With advanced options such as Allow Automatic Active Directory Account Creation or Relay Attacks, users can change integral parts of the test, rather than having to *change parts of their environment*. This allows defenders to change parts of the attack, observe the effects on the environment, and adjust accordingly.



3 Dynamic Attack Node

Select Target Network IP Range To Install Dynamic Attack Node:

Target Network IP Range *

Privileged Windows Domain Account

Domain Name

Credentials Type: Manual Defined Credentials

User Name *

Password *

Test

Intensity

Max Duration

☑ Max Spoofing Same as Max Duration

Days: 0 Hours: 1 Min: 0

☑ Automatic Rescan

Days: 0 Hours: 12 Min: 0

Stealthiness Level

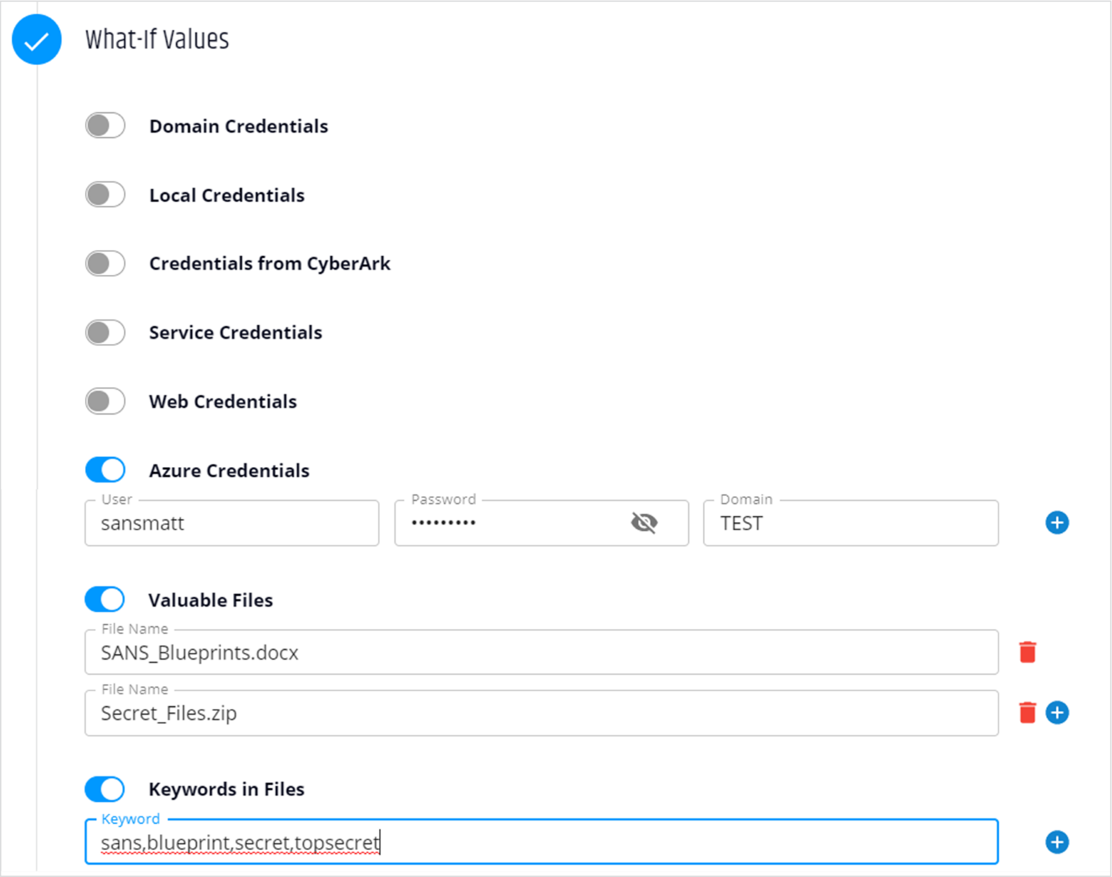
Noisy ● Stealth

Normal discovery, common Windows & Linux services enumeration (default)

Figure 5. Dynamic Attack Node and Intensity Portions of a Scheduled Test

Each test also includes options specific to the type of test. Continuing with our example of a Gray Box test, Figure 6 shows a list of the "What-If" values we may want to provide to the test.

The ability to provide values in a Gray Box test presents a unique opportunity for defenders: Testing credentials, specific files, or keywords gives them a different way to approach the frequency and usefulness of testing their controls. Not all tests should focus on the full range of attack techniques. Sometimes, defenders need to answer a simple question(s).



What-If Values

○ Domain Credentials

○ Local Credentials

○ Credentials from CyberArk

○ Service Credentials

○ Web Credentials

● Azure Credentials

User: sansmatt
Password: •••••••••
Domain: TEST

● Valuable Files

File Name: SANS_Blueprints.docx
File Name: Secret_Files.zip

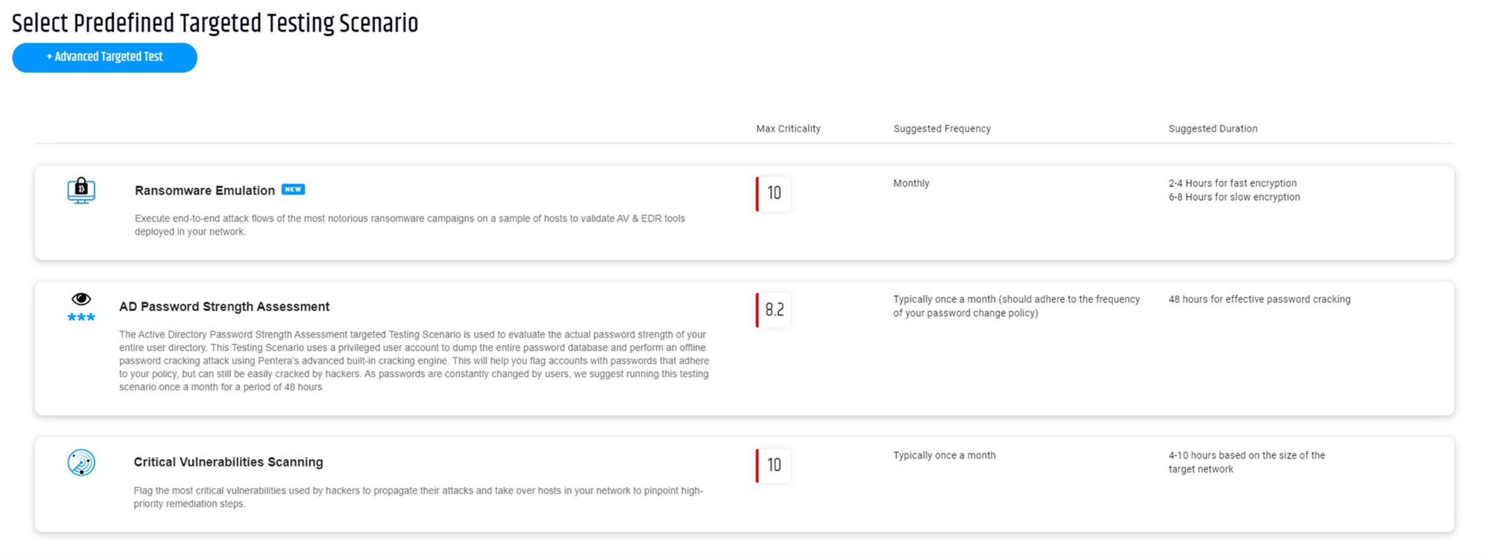
● Keywords in Files

Keyword: sans,blueprint,secret,topsecret

Figure 6. What-If Values from the Pentera Gray Box Testing Scenario

Consider, for example, a case where a defender is alerted to credentials found on the internet. Rather than try to uncover every entry vector where those credentials could be used, they could craft a quick What-If test, provide credentials, and let the automated system discover the risk for them. With a properly tuned environment, this could be done in a matter of minutes or hours—way before an attacker has a chance to find the results for them. We love this feature!

When scheduling tests, users also can select frequencies (ranging from once to daily, weekly, or monthly) and specify notifications. This can help blue teams align security validation to cadence of IT changes before and after the change. Finally, another important feature in the platform is the ability to clean up after itself. Users can provide a specific Active Directory account to clean up "test residue" and return the environment to an almost-previous state.



Select Predefined Targeted Testing Scenario

	Max Criticality	Suggested Frequency	Suggested Duration
Ransomware Emulation NEW Execute end-to-end attack flows of the most notorious ransomware campaigns on a sample of hosts to validate AV & EDR tools deployed in your network.	10	Monthly	2-4 Hours for fast encryption 6-8 Hours for slow encryption
AD Password Strength Assessment The Active Directory Password Strength Assessment targeted Testing Scenario is used to evaluate the actual password strength of your entire user directory. This Testing Scenario uses a privileged user account to dump the entire password database and perform an offline password cracking attack using Pentera's advanced built-in cracking engine. This will help you flag accounts with passwords that adhere to your policy, but can still be easily cracked by hackers. As passwords are constantly changed by users, we suggest running this testing scenario once a month for a period of 48 hours	8.2	Typically once a month (should adhere to the frequency of your password change policy)	48 hours for effective password cracking
Critical Vulnerabilities Scanning Flag the most critical vulnerabilities used by hackers to propagate their attacks and take over hosts in your network to pinpoint high-priority remediation steps.	10	Typically once a month	4-10 hours based on the size of the target network

Figure 7. Predefined Scenarios Available in Pentera's Targeted Testing

The Targeted Testing option within Pentera provides the easiest and quickest way for defenders to test their environment. Predefined scenarios, two of which are shown in Figure 7, save defenders from having to craft tests and instead launch fruitful tests against their environment.

The scenarios listed in Figure 7 continue to further the value that Pentera provides for users:

- **Ransomware Emulation** executes end-to-end attack flows of the most notorious ransomware campaigns to validate readiness for a large-scale ransomware attack.
- **AD Password Strength Assessment** is a full Active Directory testing scenario that evaluates the password strength of your entire user directory.
- **Critical Vulnerabilities Scanning** helps identify critical vulnerabilities actively exploited by adversaries.

As shown on the right side of Figure 7, these tests also can be scheduled at required frequencies and for specific durations.

Hopefully, the value here is obvious. Every organization has pondered the question "How would we stack up against a ransomware attack?" Pentera can help answer this question. The second test, Active Directory Password Strength, is a test we feel should be run in every Windows environment *continuously*. Weak passwords represent some of the lowest hanging fruit attackers like to take advantage of. Discovering and mitigating weak passwords before attackers do would severely hinder an attacker's chance of easily stealing and abusing credentials in your environment, even if they gained access.

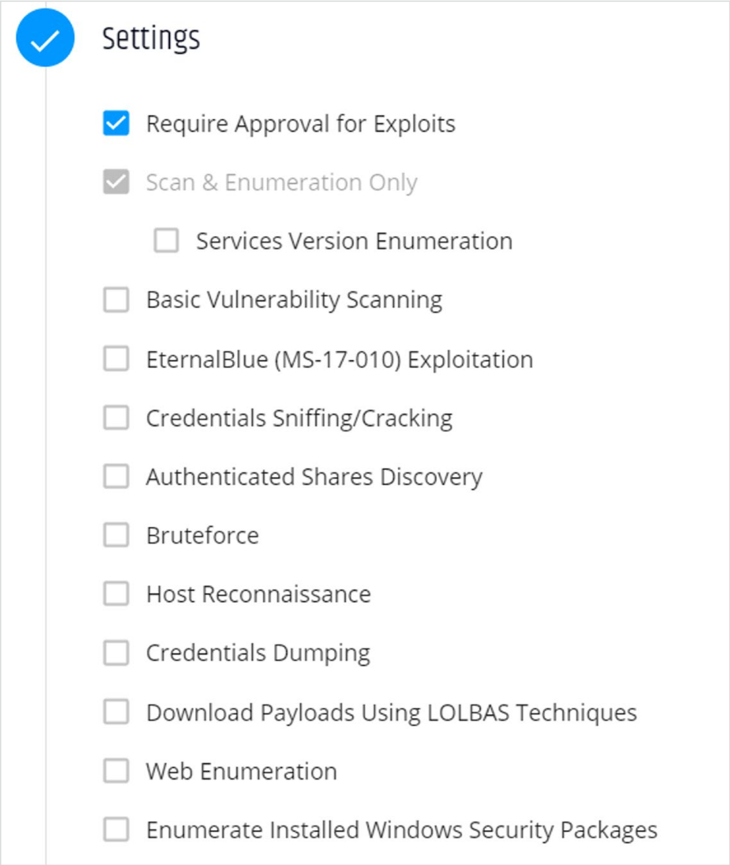
Validation Platform Tip #3:
Ask if your platform can do more than just quality controls. Can it also help you detect exploitable vulnerabilities in the environment or crack passwords? These activities should not only be available, but they should also be automated and help your team determine your current levels of resilience.

As shown in Figure 7, users also can create their own Advanced Targeted Test. These tests present unique options to users. For example, in addition to stealthiness, users can configure Targeted Tests to use specific techniques or vulnerabilities (see Figure 8).

These specific techniques include various types of enumeration, credential harvesting, vulnerability testing, and/or the use of LOLBAS[1] binaries. These granular controls are key to designing effective tests and changing attacker techniques without having to modify the entire environment.

As we mentioned earlier, the various tests Pentera offers immediately augment defenders and provide them enormous value up front. We enjoyed the flexibility Pentera provides. Defenders can run full, end-to-end tests that stress the entire environment, or they can run small, dedicated tests that focus on a system, a technique, or credentials, to name a few among many.

Of course, running tests in a safe-by-design manner is only half the battle. The next step for defenders is to utilize that output to make their environment stronger.



Settings

☑ Require Approval for Exploits

☑ Scan & Enumeration Only

□ Services Version Enumeration

□ Basic Vulnerability Scanning

□ EternalBlue (MS-17-010) Exploitation

□ Credentials Sniffing/Cracking

□ Authenticated Shares Discovery

□ Bruteforce

□ Host Reconnaissance

□ Credentials Dumping

□ Download Payloads Using LOLBAS Techniques

□ Web Enumeration

□ Enumerate Installed Windows Security Packages

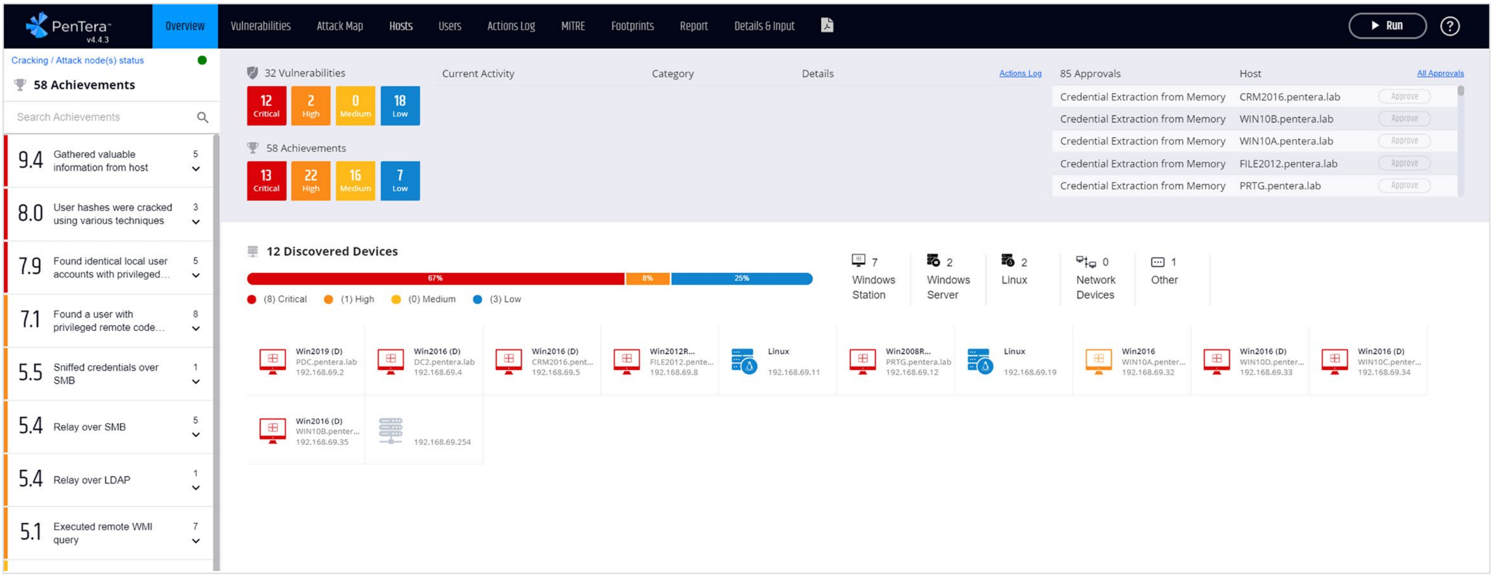
Figure 8. Targeted Tests

Test Results

While we were thoroughly impressed with Pentera's automated testing capabilities, its reporting and real-time tracking capabilities provide perhaps some of the best insight into a security control test.

Before we examine test results, it is important to note that screenshots provided will show a "point in time" snapshot of a feature, menu, or data point. However, during an active test, Pentera's platform is entirely dynamic and self-updates in real time. For example, as a validation is initiated, assets and vulnerabilities are exposed. Once a particular technique is executed, successes are recorded as Achievements, and are viewable by users as they occur. Furthermore, Pentera automatically rates and ranks these achievements as the test occurs. This provides real-time insight for defenders as to where the platform has succeeded and where they should focus defenses next. Figure 9 on the next page provides a screenshot of a test dashboard and will serve as a guide for the rest of this section.

[1] https://lolbas-project.github.io



Cracking / Attack node(s) status

58 Achievements

9.4	Gathered valuable information from host	5
8.0	User hashes were cracked using various techniques	3
7.9	Found identical local user accounts with privileged…	5
7.1	Found a user with privileged remote code…	8
5.5	Sniffed credentials over SMB	1
5.4	Relay over SMB	5
5.4	Relay over LDAP	1
5.1	Executed remote WMI query	7

32 Vulnerabilities

12 Critical	2 High	0 Medium	18 Low

58 Achievements

13 Critical	22 High	16 Medium	7 Low

Current Activity	Category	Details

85 Approvals	Host	
Credential Extraction from Memory	CRM2016.pentera.lab	Approve
Credential Extraction from Memory	WIN10B.pentera.lab	Approve
Credential Extraction from Memory	WIN10A.pentera.lab	Approve
Credential Extraction from Memory	FILE2012.pentera.lab	Approve
Credential Extraction from Memory	PRTG.pentera.lab	Approve

12 Discovered Devices

67% 8% 25%

● (8) Critical ● (1) High ● (0) Medium ● (3) Low

7	2	2	0	1
Windows Station	Windows Server	Linux	Network Devices	Other

Win2019 (D)	PDC.pentera.lab	192.168.69.2
Win2016 (D)	DC2.pentera.lab	192.168.69.4
Win2016 (D)	CRM2016.pent…	192.168.69.5
Win2012R…	FILE2012.pente…	192.168.69.8
Linux		192.168.69.11
Win2008R…	PRTG.pentera.lab	192.168.69.12
Linux		192.168.69.19
Win2016	WIN10A.penter…	192.168.69.32
Win2016 (D)	WIN10D.penter…	192.168.69.33
Win2016 (D)	WIN10C.penter…	192.168.69.34
Win2016 (D)	WIN10B.penter…	192.168.69.35
		192.168.69.254

Figure 9. Dashboard from a Pentera Test

First, it is worth noting that the initial screen provides so much context and insight that analysts could easily operate from this screen alone. The dashboard for each test includes details such as:

- Vulnerabilities identified during the test, sorted by criticality
- Achievements[2] identified during the test, also sorted by criticality
- Devices discovered during the test, including criticality of each device with respect to vulnerabilities and achievements
- Current activity (if the test is live)
- Approvals for exploitation, if requested

Considering all the options available during the scheduling of a test, it is quite a feat to see how much content Pentera includes on one screen. Users also should note that the dashboard is laid out in a way that drives one toward the most important findings of the test—the things that need to be fixed now.

In the present test, a total of 58 Achievements, 32 vulnerabilities, and 12 devices are identified. Each data point is provided with criticality, underlining both its importance to the success of the test *and* its current state of vulnerability and/or potential attacker abuse. Achievements also encompass multiple systems if a test can perform an activity against multiple systems.

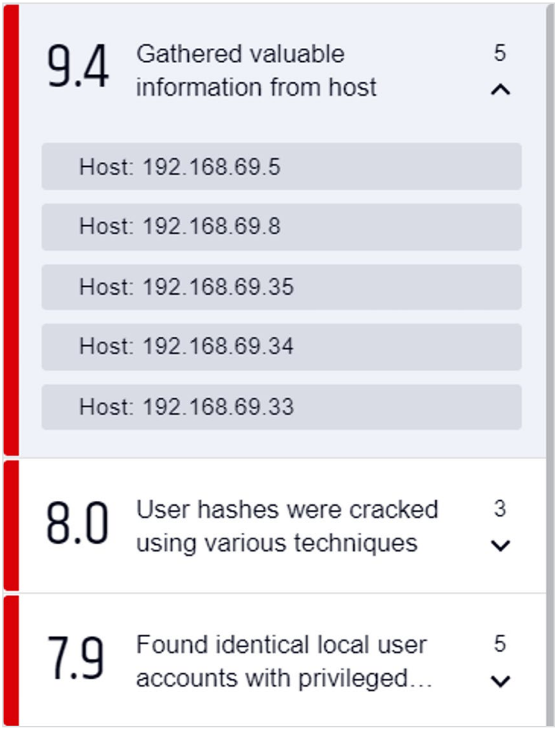
[2] In Pentera speak, Achievements are a goal accomplished during a test. An achievement may include sniffing credentials over SMB or exploiting a user with high privileges. Many achievements are possible due to vulnerabilities; however, Achievements also may include things like enumeration or validating of credentials.

For example, let us examine the critical Achievements from the current example. As seen in Figure 10, Pentera ranks the following three Achievements as critical:

- Gathering valuable information from a host
- User hashes were cracked using password-cracking techniques
- Identification of local user accounts with privileged remote code execution permissions

Figure 10 also expands and shows that during this test, Pentera was able to gather valuable information from five unique systems, expanding the scope of this potential technique within our test environment. Similarly, the second and third critical Achievements were found on three and five systems, respectively.

These data points are extremely valuable for defenders. First, simply *identifying* a vulnerability, weakness, or misconfiguration within an environment does little to help the security team apply patches or mitigations. A slightly better second option would include specific systems with a vulnerability. However, this is entirely dependent on the path a penetration tester has taken. Pentera trumps these options by including *all systems* within scope. If a vulnerability is found on one system, it will check for the others—even if those systems are not part of the critical attack path.



9.4 Gathered valuable information from host 5

Host: 192.168.69.5

Host: 192.168.69.8

Host: 192.168.69.35

Host: 192.168.69.34

Host: 192.168.69.33

8.0 User hashes were cracked using various techniques 3

7.9 Found identical local user accounts with privileged… 5

Figure 10. Critical Achievements

This is relevant for defenders who must take test results and go patch the environment. If they only know of a handful of impacted systems, then the scope of the path may be limited. Pentera provides a more comprehensive viewpoint of weaknesses in the environment, thus allowing for better scoping and patch application.

Validation Platform Tip #4:
Findings are not actionable if they only include one system and ignore the rest of the environment, nor does one system's findings apply to a heterogenous infrastructure. Ask how quickly a platform can search for one weakness, misconfiguration, or vulnerability across the entire enterprise, so defenders can scope remediation appropriately.

However, the Achievements menu is much more than simple high-level statistics. Figure 11 includes a screenshot of the same critical Achievement with all five systems included.

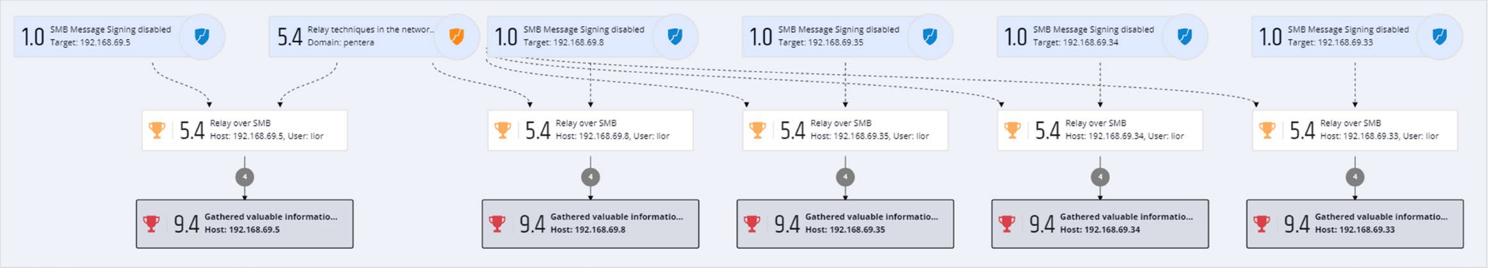

1.0 SMB Message Signing disabled Target: 192.168.69.5
5.4 Relay techniques in the networ.. Domain: pentera
1.0 SMB Message Signing disabled Target: 192.168.69.8
1.0 SMB Message Signing disabled Target: 192.168.69.35
1.0 SMB Message Signing disabled Target: 192.168.69.34
1.0 SMB Message Signing disabled Target: 192.168.69.33
5.4 Relay over SMB Host: 192.168.69.5, User: lior
5.4 Relay over SMB Host: 192.168.69.8, User: lior
5.4 Relay over SMB Host: 192.168.69.35, User: lior
5.4 Relay over SMB Host: 192.168.69.34, User: lior
5.4 Relay over SMB Host: 192.168.69.33, User: lior
4
9.4 Gathered valuable informatio... Host: 192.168.69.5
9.4 Gathered valuable informatio... Host: 192.168.69.8
9.4 Gathered valuable informatio... Host: 192.168.69.35
9.4 Gathered valuable informatio... Host: 192.168.69.34
9.4 Gathered valuable informatio... Host: 192.168.69.33

Figure 11. Systems Impacted and the Attack Path for Gathering Valuable Host Information

Pentera does more than just report Achievements or vulnerabilities. As seen in Figure 11, Pentera also provides insight into the attack path and series of adversary techniques that allowed a particular Achievement to succeed. Figure 11 shows us that each of the five systems suffered a Relay over SMB attack, which led to the Achievement success (note that Relay over SMB is itself an Achievement, with a score of 5.4).

Within the platform, we also can "zoom in" on a particular system to further understand what occurred during the test. Figure 12 shows a more elaborate set of attack paths, with emphasis on systems that also had accounts with remote code execution privileges enabled.

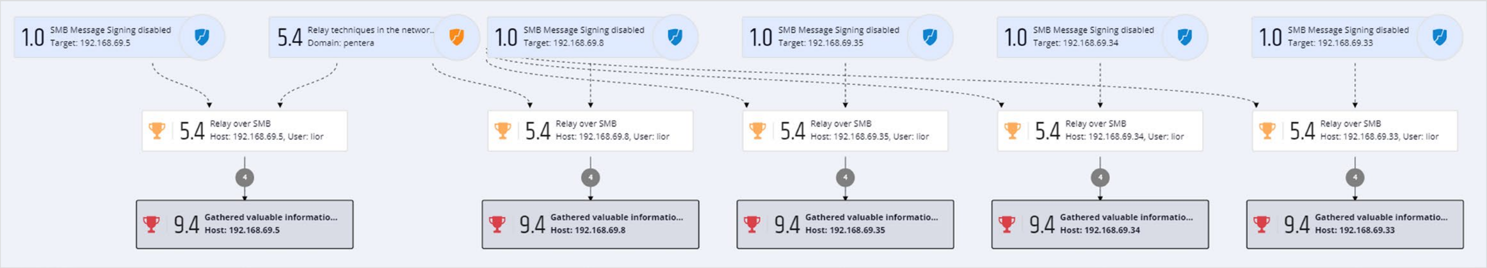

1.0 SMB Message Signing disabled Target: 192.168.69.5
5.4 Relay techniques in the networ.. Domain: pentera
1.0 SMB Message Signing disabled Target: 192.168.69.8
1.0 SMB Message Signing disabled Target: 192.168.69.35
1.0 SMB Message Signing disabled Target: 192.168.69.34
1.0 SMB Message Signing disabled Target: 192.168.69.33
5.4 Relay over SMB Host: 192.168.69.5, User: lior
5.4 Relay over SMB Host: 192.168.69.8, User: lior
5.4 Relay over SMB Host: 192.168.69.35, User: lior
5.4 Relay over SMB Host: 192.168.69.34, User: lior
5.4 Relay over SMB Host: 192.168.69.33, User: lior
4
9.4 Gathered valuable informatio... Host: 192.168.69.5
9.4 Gathered valuable informatio... Host: 192.168.69.8
9.4 Gathered valuable informatio... Host: 192.168.69.35
9.4 Gathered valuable informatio... Host: 192.168.69.34
9.4 Gathered valuable informatio... Host: 192.168.69.33

Figure 12. Attack Path for Systems with Multiple Achievements and MITRE ATT&CK Techniques

Figure 12 provides an enormous amount of context and technical information. As we have discussed, simply informing a security team that their environment is vulnerable or prone to attack is no longer enough. Pentera goes a step further and clearly outlines the attack path and how vulnerabilities can lead to larger, more significant events. For example, as seen in Figure 12, the disabling of SMB Message Signing led all the way to two critical and two high Achievements. This is a very true representation of threat actors, who often can pivot from a seemingly inconsequential weakness to a larger scale attack operation. Pentera also maps Achievements and techniques directly to MITRE's ATT&CK framework, as we can see in Figure 13. In addition, analysts can enrich Achievements with ATT&CK mapping the adversary level (based on actions observed) or action time, with respect to the ongoing "attack."

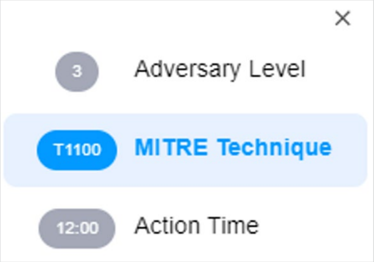
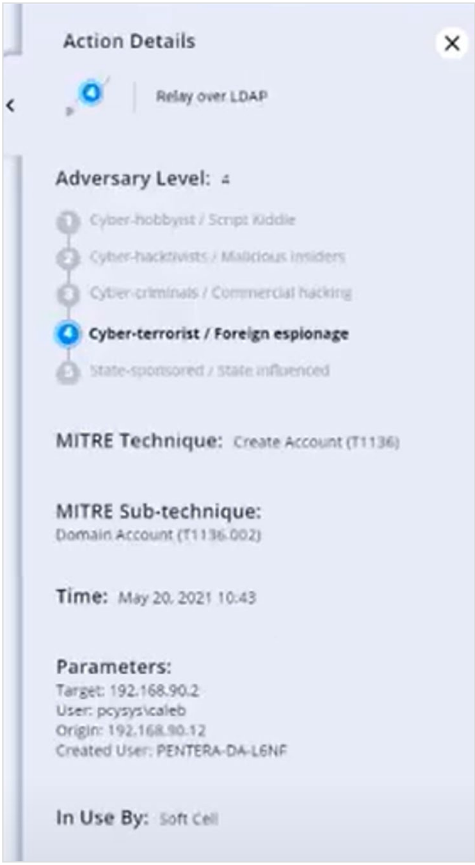


Figure 13. Snippet of Selections Available for Enriching Achievements Within the Linked Display

From here, analysts have multiple options. To the right of the screen, as shown in Figure 14, analysts can view more details about a particular achievement. These data points may include parameters of an attack, a summary of the Achievement, and hosts impacted—and perhaps of most value, insight into the impact of a particular technique.


Action Details

Relay over LDAP

Adversary Level: 4

1 Cyber-hobbyist / Script Kiddie
2 Cyber-hacktivists / Malicious insiders
3 Cyber-criminals / Commercial hacking
4 Cyber-terrorist / Foreign espionage
5 State-sponsored / State influenced

MITRE Technique: Create Account (T1136)

MITRE Sub-technique:
Domain Account (T1136.002)

Time: May 20, 2021 10:43

Parameters:
Target: 192.168.90.2
User: pcysys\caleb
Origin: 192.168.90.12
Created User: PENTERA-DA-L6NF

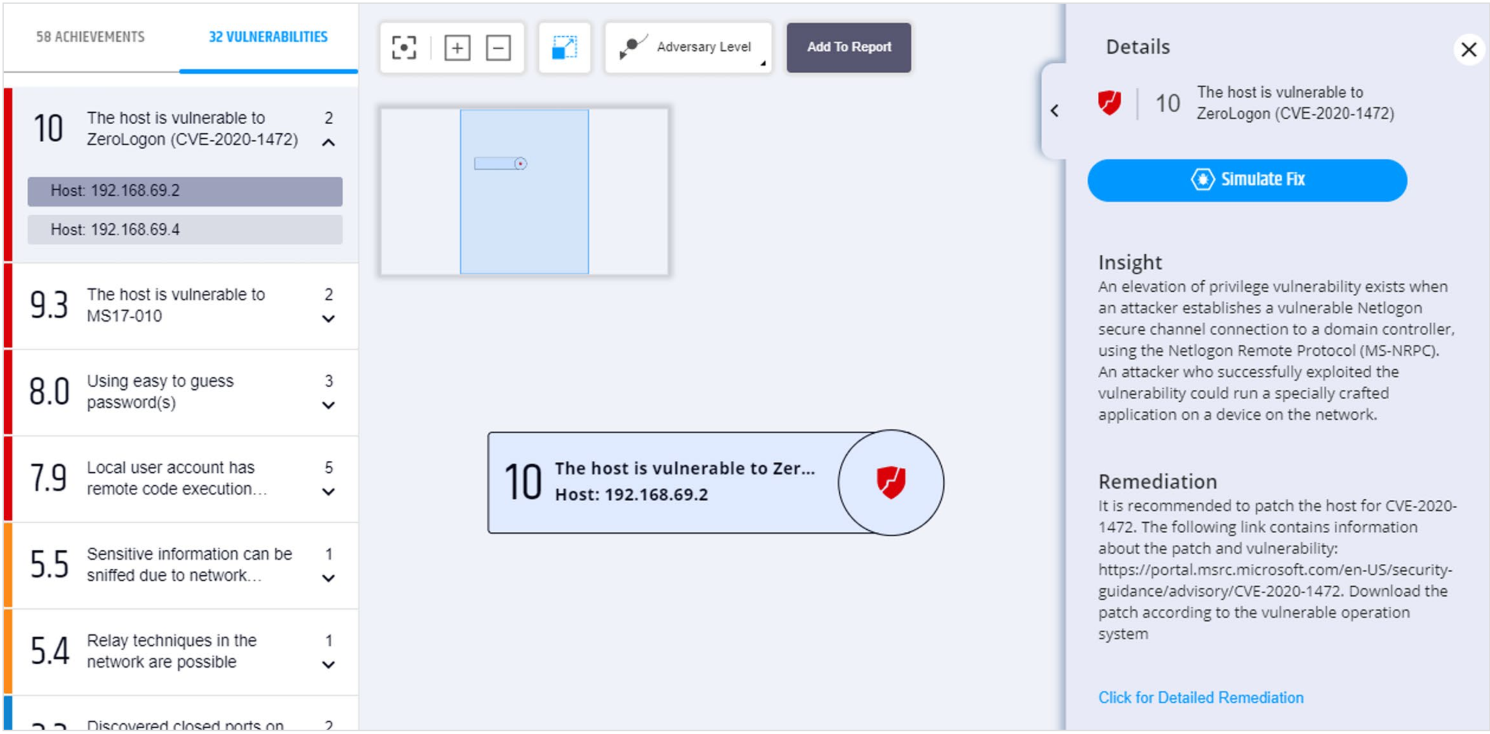
In Use By: Soft Cell

Figure 14. Action Details from the Pentera Attack Map

The Action Details for each Achievement provides visibility into how an attacker may use a particular technique, achievement, vulnerability, etc. to abuse or maintain a foothold in an environment. So, all in one screen, defenders can see:

- What techniques were successful during a particular test
- Which MITRE ATT&CK tactics and techniques were used
- How those techniques were chained together to achieve a result
- How and what (else) attackers may use these Achievements for
- The number of systems impacted by *each* of the above

However, Pentera is not yet done providing value. Instead of looking at test results as Achievements, let us instead view the vulnerabilities that were successful during the test.



10 The host is vulnerable to ZeroLogon (CVE-2020-1472) 2
Host: 192.168.69.2
Host: 192.168.69.4

9.3 The host is vulnerable to MS17-010 2

8.0 Using easy to guess password(s) 3

7.9 Local user account has remote code execution... 5

5.5 Sensitive information can be sniffed due to network... 1

5.4 Relay techniques in the network are possible 1

Discovered closed ports on 2

10 The host is vulnerable to Zer...
Host: 192.168.69.2

10 The host is vulnerable to ZeroLogon (CVE-2020-1472)

Insight
An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network.

Remediation
It is recommended to patch the host for CVE-2020-1472. The following link contains information about the patch and vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472. Download the patch according to the vulnerable operation system

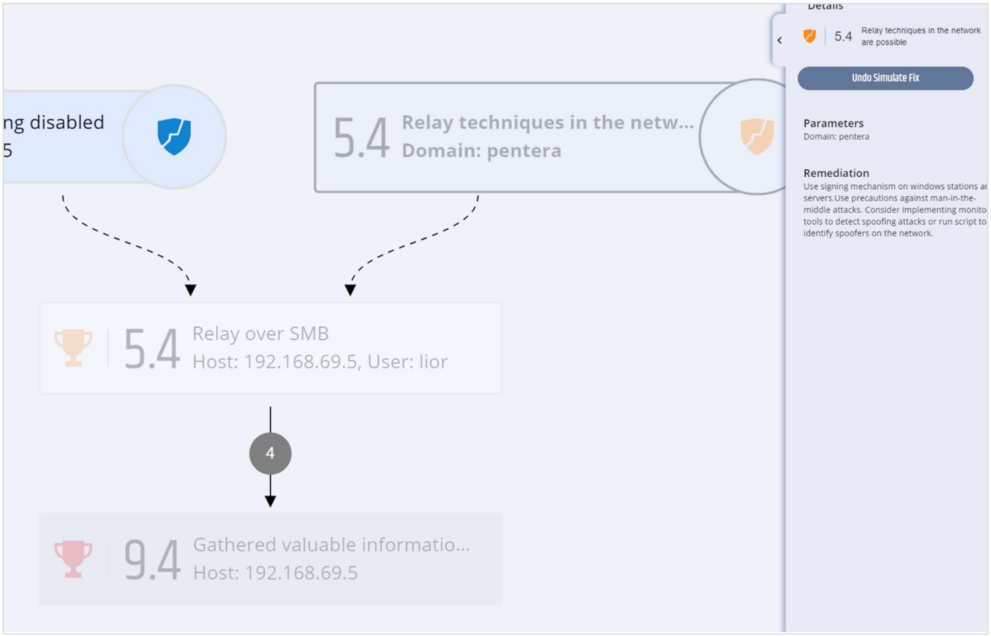
Click for Detailed Remediation

Figure 15. Pentera Attack Map Focused on Vulnerabilities Identified During a Test

Figure 15 provides a snippet with the Attack Map focused on Vulnerabilities rather than Achievements.

Note that the display is like the Achievements menu; we can see the quantity of systems and vulnerabilities are organized by criticality. However, there is one key difference. Within the right Details bar, users are provided with deep insight into the Vulnerability. Note that Pentera also includes information about Remediation (based on defined priority, not that of CVSS)! Clicking *Detailed Remediation* navigates us to the Remediation Wiki, which contains thorough details about how to remediate a particular vulnerability. This is perhaps some of the most impactful data provided in the platform. Not only are defenders aware of a Vulnerability, they also can view, in real time, remediation instructions.

You also may have noticed in Figure 15 there is a Simulate Fix button. This option is available for both certain Achievements and Vulnerabilities. When utilized, this button nullifies an Achievement or Vulnerability from an attack path, showing defenders how a simple fix can disrupt an entire attack chain as well as directly implying risk and impact reduced. Figure 16 provides an example of nullifying relay techniques in an attack path.



ng disabled
5

5.4 Relay techniques in the netw...
Domain: pentera

5.4 Relay over SMB
Host: 192.168.69.5, User: lior

9.4 Gathered valuable informatio...
Host: 192.168.69.5

5.4 Relay techniques in the network are possible

Parameters
Domain: pentera

Remediation
Use signing mechanism on windows stations ar servers.Use precautions against man-in-the-middle attacks. Consider implementing monito tools to detect spoofing attacks or run script to identify spoofers on the network.

Figure 16. Attack Path with the Relay Technique Fix Simulated

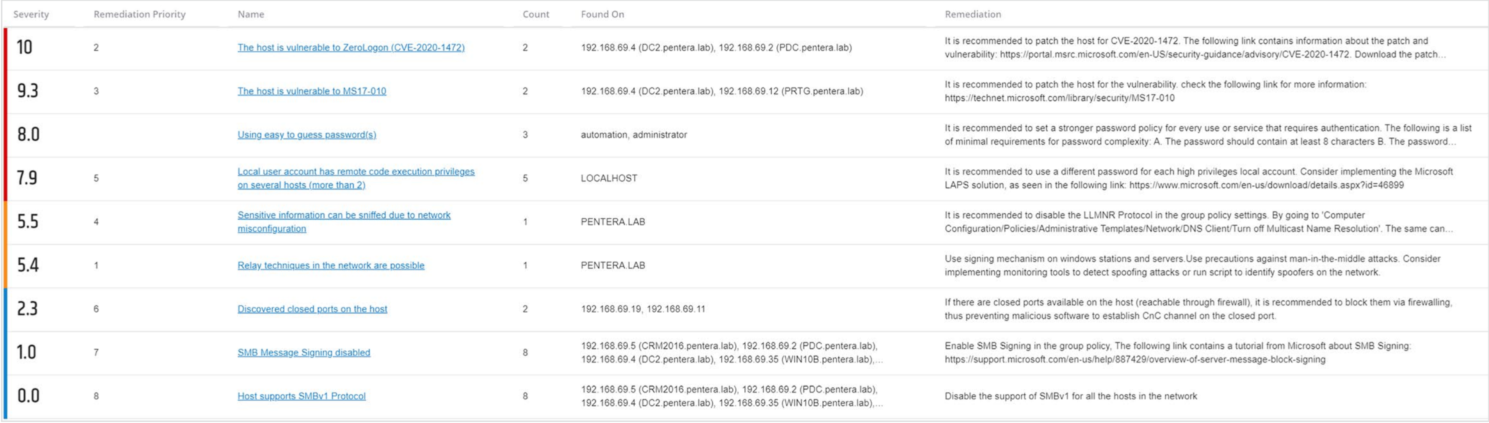
Notice that if the relay techniques were not available, the attacker would not have been able to launch a Relay over SMB attack and thus harvest details from the target system(s). While relatively subtle, this is a huge feature of the platform. It allows defenders to prioritize and visualize remediations and mitigations within the environment, backed by data linked to adversary techniques.

The Overview and Attack Map screens end up being enough that most users can effectively assess the results of a test and determine what to do next. However, Pentera breaks test results down into more actionable parts, which we will briefly examine next.

Validation Platform Tip #5:
Knowing that something needs to be fixed is half the battle. Actually *fixing the issue* and then reviewing how those fixes impact your environment provides valuable insight to the blue team. Look for this capability, it will help your team implement better protection strategies.

Vulnerability Scanning

As we have mentioned before, Pentera is not just automated security control testing. It also includes automated vulnerability scanning as part of an active test. If a user wishes to view just the Vulnerability results without an Attack Map, there is a dedicated screen (see Figure 17).



Severity	Remediation Priority	Name	Count	Found On	Remediation
10	2	The host is vulnerable to ZeroLogon (CVE-2020-1472)	2	192.168.69.4 (DC2.pentera.lab), 192.168.69.2 (PDC.pentera.lab)	It is recommended to patch the host for CVE-2020-1472. The following link contains information about the patch and vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472. Download the patch...
9.3	3	The host is vulnerable to MS17-010	2	192.168.69.4 (DC2.pentera.lab), 192.168.69.12 (PRTG.pentera.lab)	It is recommended to patch the host for the vulnerability. check the following link for more information: https://technet.microsoft.com/library/security/MS17-010
8.0		Using easy to guess password(s)	3	automation, administrator	It is recommended to set a stronger password policy for every use or service that requires authentication. The following is a list of minimal requirements for password complexity: A. The password should contain at least 8 characters B. The password...
7.9	5	Local user account has remote code execution privileges on several hosts (more than 2)	5	LOCALHOST	It is recommended to use a different password for each high privileges local account. Consider implementing the Microsoft LAPS solution, as seen in the following link: https://www.microsoft.com/en-us/download/details.aspx?id=46899
5.5	4	Sensitive information can be sniffed due to network misconfiguration	1	PENTERA.LAB	It is recommended to disable the LLMNR Protocol in the group policy settings. By going to 'Computer Configuration/Policies/Administrative Templates/Network/DNS Client/Turn off Multicast Name Resolution'. The same can...
5.4	1	Relay techniques in the network are possible	1	PENTERA.LAB	Use signing mechanism on windows stations and servers.Use precautions against man-in-the-middle attacks. Consider implementing monitoring tools to detect spoofing attacks or run script to identify spoofers on the network.
2.3	6	Discovered closed ports on the host	2	192.168.69.19, 192.168.69.11	If there are closed ports available on the host (reachable through firewall), it is recommended to block them via firewalling, thus preventing malicious software to establish CnC channel on the closed port.
1.0	7	SMB Message Signing disabled	8	192.168.69.5 (CRM2016.pentera.lab), 192.168.69.2 (PDC.pentera.lab), 192.168.69.4 (DC2.pentera.lab), 192.168.69.35 (WIN10B.pentera.lab),...	Enable SMB Signing in the group policy, The following link contains a tutorial from Microsoft about SMB Signing: https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing
0.0	8	Host supports SMBv1 Protocol	8	192.168.69.5 (CRM2016.pentera.lab), 192.168.69.2 (PDC.pentera.lab), 192.168.69.4 (DC2.pentera.lab), 192.168.69.35 (WIN10B.pentera.lab),...	Disable the support of SMBv1 for all the hosts in the network

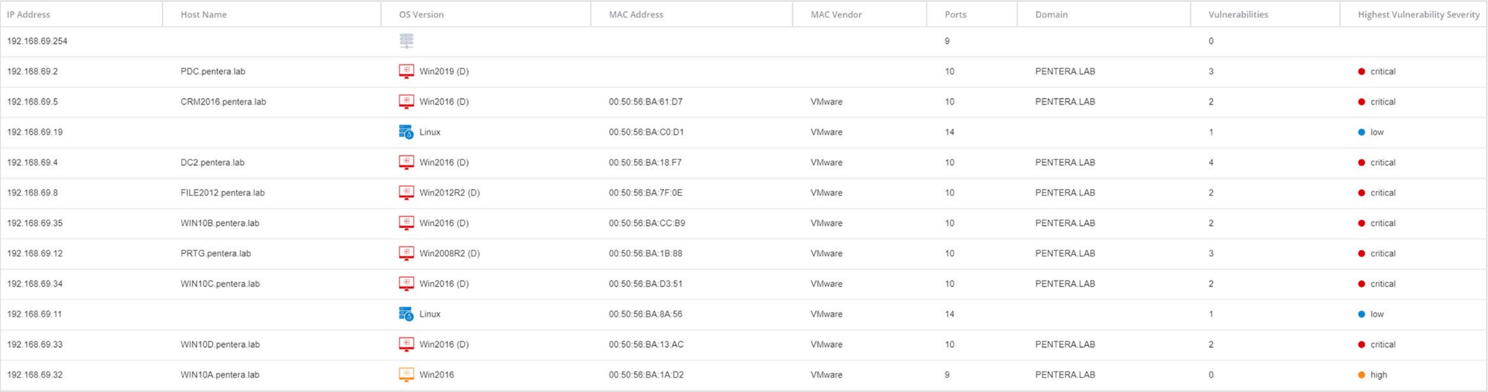
Figure 17. Vulnerabilities Screen

The value in this sub-screen is immediately apparent. Rather than having to walk through the attack map, users can quickly see how many vulnerabilities were identified in the environment, the key findings (users, systems, domains, etc.), and recommendations for remediation. This screen could easily be exported and shared among security teams at a regular interval to help prioritize where and what to patch.

The second column in Figure 17 also is unique to the Pentera platform. Pentera provides a Remediation Priority, which helps defenders focus on root vulnerabilities that may lead to high-severity Achievements. Rather than simply prioritizing remediations based on CVSS levels, this metric allows defenders to remediate based on where attackers will find the most success—knocking down attacker success rates even faster. Per Pentera, this score is generated using asset criticality, adversary sophistication, techniques used, and impact to the environment.

Host by Host, User by User

As we mentioned earlier, Pentera also groups test findings by host. Figure 18 provides insight into host-based classification.



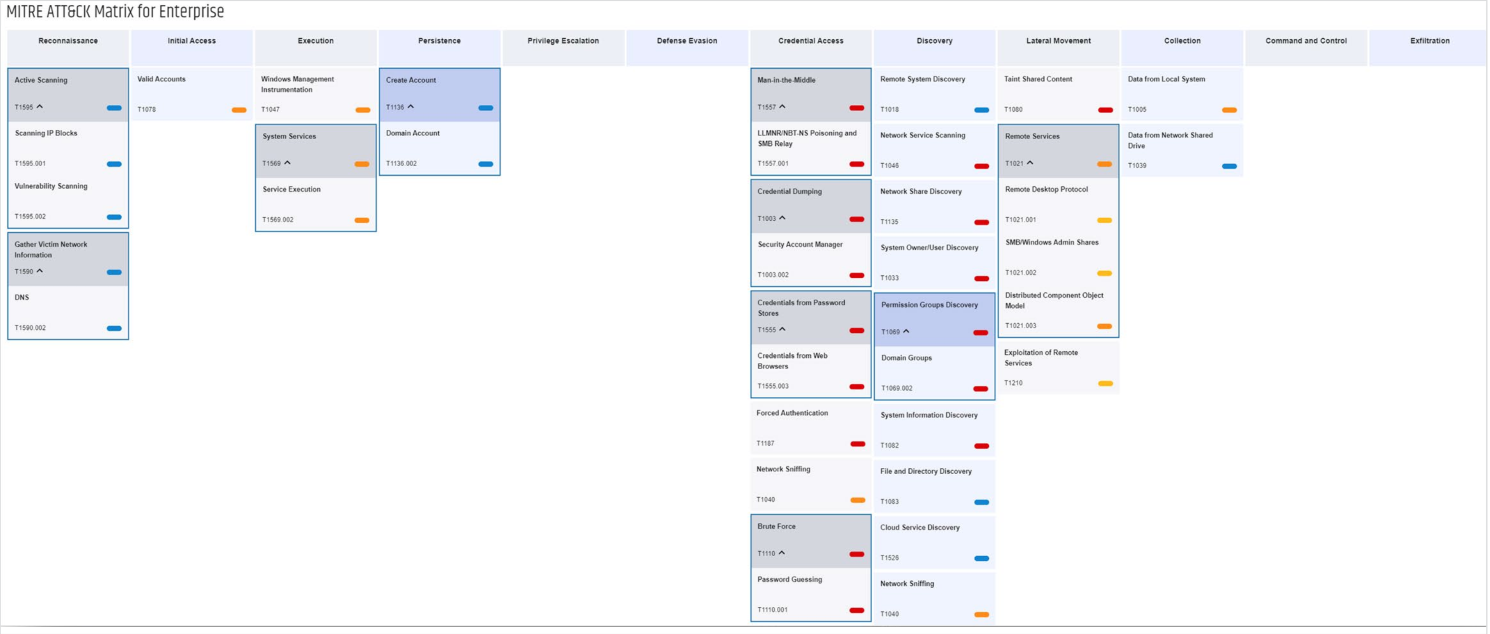
IP Address	Host Name	OS Version	MAC Address	MAC Vendor	Ports	Domain	Vulnerabilities	Highest Vulnerability Severity
192.168.69.254					9		0	
192.168.69.2	PDC.pentera.lab	Win2019 (D)			10	PENTERA.LAB	3	● critical
192.168.69.5	CRM2016.pentera.lab	Win2016 (D)	00:50:56:BA:61:D7	VMware	10	PENTERA.LAB	2	● critical
192.168.69.19		Linux	00:50:56:BA:C0:D1	VMware	14		1	● low
192.168.69.4	DC2.pentera.lab	Win2016 (D)	00:50:56:BA:18:F7	VMware	10	PENTERA.LAB	4	● critical
192.168.69.8	FILE2012.pentera.lab	Win2012R2 (D)	00:50:56:BA:7F:0E	VMware	10	PENTERA.LAB	2	● critical
192.168.69.35	WIN10B.pentera.lab	Win2016 (D)	00:50:56:BA:CC:B9	VMware	10	PENTERA.LAB	2	● critical
192.168.69.12	PRTG.pentera.lab	Win2008R2 (D)	00:50:56:BA:1B:88	VMware	10	PENTERA.LAB	3	● critical
192.168.69.34	WIN10C.pentera.lab	Win2016 (D)	00:50:56:BA:D3:51	VMware	10	PENTERA.LAB	2	● critical
192.168.69.11		Linux	00:50:56:BA:8A:56	VMware	14		1	● low
192.168.69.33	WIN10D.pentera.lab	Win2016 (D)	00:50:56:BA:13:AC	VMware	10	PENTERA.LAB	2	● critical
192.168.69.32	WIN10A.pentera.lab	Win2016	00:50:56:BA:1A:D2	VMware	9	PENTERA.LAB	0	● high

Figure 18. Hosts Tab from the Pentera Platform Test Results

Figure 18 classifies findings and criticalities by system. Although this data is represented individually in the attack map, this view provides another way for defenders to identify the most vulnerable systems discovered in the environment and help prioritize patching and remediation. Pentera also includes a view of users, with insight into password vulnerabilities and how easy it was for the platform to crack the user's password.

Mapping to MITRE ATT&CK

Last, but certainly not least, Pentera includes a really nifty MITRE ATT&CK mapping capability (see Figure 19).



MITRE ATT&CK Matrix for Enterprise

Reconnaissance
- Active Scanning T1595
- Scanning IP Blocks T1595.001
- Vulnerability Scanning T1595.002
- Gather Victim Network Information T1590
- DNS T1590.002

Initial Access
- Valid Accounts T1078

Execution
- Windows Management Instrumentation T1047
- System Services T1569
- Service Execution T1569.002

Persistence
- Create Account T1136
- Domain Account T1136.002

Privilege Escalation

Defense Evasion

Credential Access
- Man-in-the-Middle T1557
- LLMNR/NBT-NS Poisoning and SMB Relay T1557.001
- Credential Dumping T1003
- Security Account Manager T1003.002
- Credentials from Password Stores T1555
- Credentials from Web Browsers T1555.003
- Forced Authentication T1187
- Network Sniffing T1040
- Brute Force T1110
- Password Guessing T1110.001

Discovery
- Remote System Discovery T1018
- Network Service Scanning T1046
- Network Share Discovery T1135
- System Owner/User Discovery T1033
- Permission Groups Discovery T1069
- Domain Groups T1069.002
- System Information Discovery T1082
- File and Directory Discovery T1083
- Cloud Service Discovery T1526
- Network Sniffing T1040

Lateral Movement
- Taint Shared Content T1080
- Remote Services T1021
- Remote Desktop Protocol T1021.001
- SMB/Windows Admin Shares T1021.002
- Distributed Component Object Model T1021.003
- Exploitation of Remote Services T1210

Collection
- Data from Local System T1005
- Data from Network Shared Drive T1039

Command and Control

Exfiltration

Figure 19. MITRE ATT&CK Framework, Highlighted with Respect to the Completed Test

You might notice that the MITRE Framework in Figure 19 seems incomplete. This is by design. Pentera reshapes and displays *only* the adversary techniques present in the current test. Once again, Pentera has crafted a view to provide value to defenders based on the data available. As the test is conducted, and more techniques are exposed, this map adjusts accordingly.

It is worth noting again that among all the various screens and capabilities analyzed in Figure 19, Pentera provides unique value for defenders in each screen. Continuously testing one's environment can be a task that yields a great amount of data—so much so, that defenders might not be able to figure out what to act on. The opposite is true with Pentera. The outcomes of every test are clear and straightforward and provide an easy next step for defenders to secure their environment.

Conclusion

As of the writing of this paper, dozens of organizations are dealing with an attack from an IT management software provider—yet another angle that attackers are seizing on to infiltrate multiple organizations simultaneously. Coupled with the ever-looming threat of ransomware, security teams can easily feel overwhelmed and that their defenses are unable to protect their environment. The Pentera platform helps defenders evaluate the organization's security program resilience and cyberattack readiness.

The answer to these woes cannot be achieved without security controls. However, controls cannot simply be placed into an environment. They must be tuned to each environment and continuously tested to ensure that they are acting appropriately. A security team cannot rely on a security control if they are unaware of its ability to detect and/or prevent attacks.

In this paper, we examined Pentera, a platform to help ease the necessity of security validation. Organizations and attackers alike take advantage of more and more technologies daily, and one-off, manual testing methods can no longer be expected to effectively test an environment. Continuous, automated testing not only keeps up with the business, it takes the burden off the security team and helps them prioritize where the environment needs attention the most.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a principal consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

PENTERA