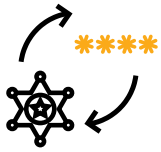
PENTERA | DATA SHEET

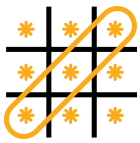
CREDENTIAL EXPOSURE-MODUL

Das Credential-Exposure-Modul (CE) von Pentera überwacht Ihre gesamte Angriffsoberfläche kontinuierlich auf gestohlene und kompromittierte Passwörter, um Einbrüchen zuvorzukommen.

Die zentralen Säulen des Moduls



Kontinuierliche Feeds
Sie haben Zugriff auf zahlreiche für Ihre Domain relevanten Streams zu aktuellen Bedrohungsszenarien beim Diebstahl von Logindaten, um sicherzustellen, dass kompromittierte Logindaten sofort entdeckt werden.



Bedrohungen aus dem Internet
Pentera nutzt seine Threat Intel und testet auf bestehende Berechtigungsprobleme und Sicherheitslücken bei Ihren externen Diensten und Active Directory, um riskante, kriminell verwertbare Logindaten zu ermitteln und zu beheben.

Logindaten in zahlreichen Formaten
Pentera prüft gehackte Logindaten in allen nur erdenklichen Formaten, ob verschlüsselt oder unverschlüsselt und unabhängig davon, ob sie Benutzernamen und Passwörter ganz oder nur teilweise anzeigen.

Auf allen Angriffsoberflächen präsent
Unsere Prüftools zu bestehenden Sicherheitslücken durchkämmen die öffentlich zugänglichen Angriffsoberflächen, einschließlich Web-Anwendungen sowie Cloud - und Perimeter-Assets.

Funktionsweise

Aufklärung und Einschätzung

Pentera kartographiert die innere und äußere Angriffsoberfläche, um potenzielle Schwachstellen sowie Angriffspunkte für die missbräuchliche Nutzung von Logindaten zu ermitteln.

Logindaten-Mapping

Pentera filtert die für eine bestimmte Domain sicherheitsrelevanten Logindaten aus seiner Datenbank für Login-Sicherheitsmaßnahmen. Typischerweise sind dies hunderttausende an Daten pro Domain.

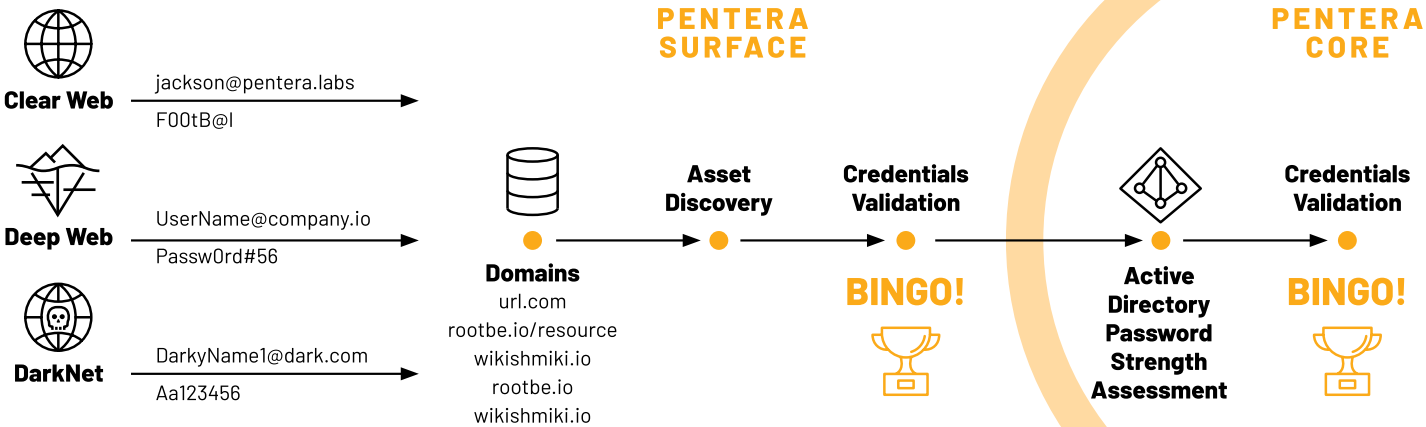
Logindaten-Prüfung

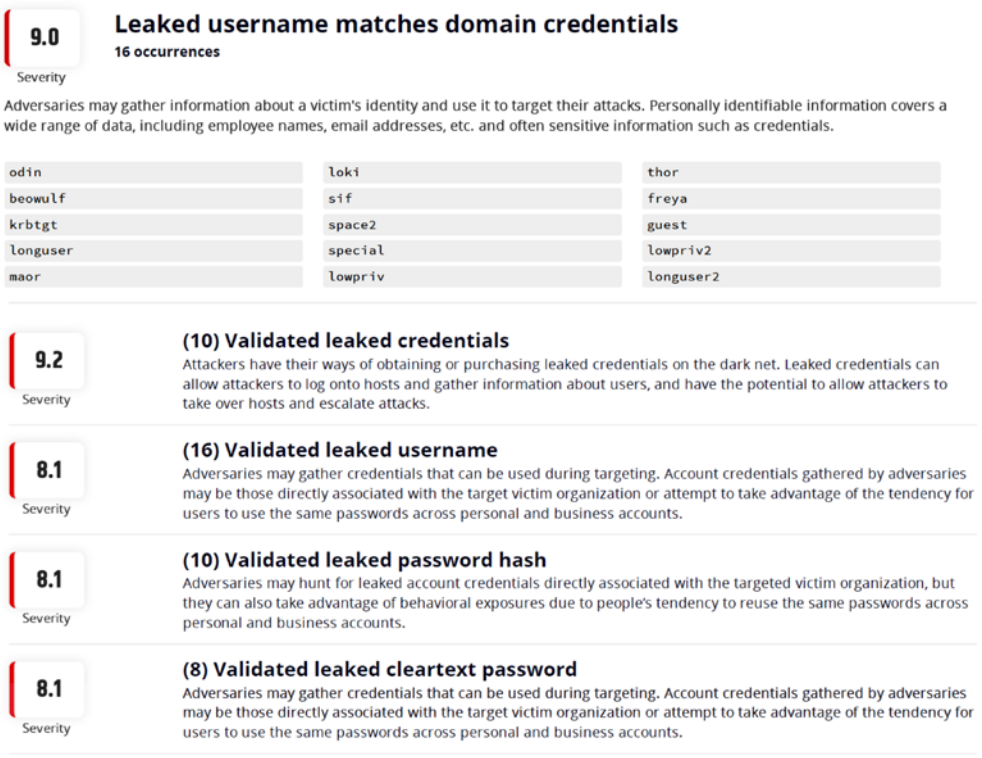
Pentera führt proaktiv verschiedene Techniken von Credential Stuffing oder Credential Relaying durch, um zu versuchen, Logindaten und Berechtigungen abzugreifen und den Angriff voranzutreiben.

Benachrichtigungen zu Sicherheitslücken

Die Sicherheitsabteilung erhält klare Reportings und Benachrichtigungen, um in Echtzeit Gegenmaßnahmen gegen Login-Raub zu treffen und dessen Folgen zu mindern.

Threat Intelligence
(basierend auf Penteras Datenquellen für Leaked Credentials)





9.0 Severity

Leaked username matches domain credentials

16 occurrences

Adversaries may gather information about a victim's identity and use it to target their attacks. Personally identifiable information covers a wide range of data, including employee names, email addresses, etc. and often sensitive information such as credentials.

odin	loki	thor
beowulf	sif	freya
krbtgt	space2	guest
longuser	special	lowpriv2
maor	lowpriv	longuser2

9.2 Severity

(10) Validated leaked credentials

Attackers have their ways of obtaining or purchasing leaked credentials on the dark net. Leaked credentials can allow attackers to log onto hosts and gather information about users, and have the potential to allow attackers to take over hosts and escalate attacks.

8.1 Severity

(16) Validated leaked username

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

8.1 Severity

(10) Validated leaked password hash

Adversaries may hunt for leaked account credentials directly associated with the targeted victim organization, but they can also take advantage of behavioral exposures due to people's tendency to reuse the same passwords across personal and business accounts.

8.1 Severity

(8) Validated leaked cleartext password

Adversaries may gather credentials that can be used during targeting. Account credentials gathered by adversaries may be those directly associated with the target victim organization or attempt to take advantage of the tendency for users to use the same passwords across personal and business accounts.

Report Screenshot

So profitieren Sie

Sie gewinnen Zeit, Risiken durch gestohlene Zugangsdaten zu mitigieren

Indem Sie geleakte und gestohlene Logindaten schnell ermitteln und Sicherheitslücken beheben, sind Sie Kriminellen immer einen Schritt voraus.

Weniger manueller Aufwand für Datenanalysten

Der Abgleich von Bedrohungsdaten mit aktiven Logindaten erfolgt vollautomatisch und kommt vollständig ohne manuelle Eingriffe aus.

Auf echter Gefahrenlage basierender Login-Diebstahl wird priorisiert

Der Fokus der Software liegt auf den 1 % geleakter Logindaten, die sich erwiesenermaßen als verwertbar herausgestellt haben.

Doppelaufwand vermeiden

Mit einer Plattform zur Überprüfung interner und externer Angriffsoberflächen zentralisieren Sie Ihren Aufwand zur Bekämpfung von Logindaten-Diebstahl.

Über Pentera

Pentera ist ein führender Anbieter im Bereich Automated Security Validation, der es jedem Unternehmen ermöglicht, sein gesamtes Cybersecurity-System problemlos zu testen und jederzeit echte, aktuelle Sicherheitslücken unabhängig von ihrer Tragweite zu enthüllen. Tausende Sicherheitsfachleute und Dienstleister im Bereich Cybersicherheit auf der ganzen Welt verlassen sich auf Pentera, um bei Abhilfemaßnahmen angeleitet zu werden und Sicherheitslücken zu schließen, bevor sie ausgenutzt werden können. Weitere Informationen finden Sie unter **Pentera.io**.