Exklusiver Red Teaming Report

Blick hinter die Kulissen:
Das erwartet dich in deinem individuellen Report nach einem Red Team Assessment

ProSec
Security redefined.

SECURITY REPORT

Red Team Assessment

Firma XY

Klassifierung:
streng vertraulich

ProSec
Security redefined.

INHALTSVERZEICHNIS

PRÄAMBEL

Hierbei handelt es sich um die Dokumentation des durchgeführten Red-Team Assessments der ProSec GmbH für die XY.

Hinweis

Das folgende Dokument ist, aufgrund der Natur der Ausführungen und der daraus resultierenden Konsequenzen bei ungewollter Einsichtnahme, als streng vertraulich einzustufen und nur den unmittelbar am Projekt beteiligten Personen vollumfänglich zugänglich zu machen. Die Sicherstellung dessen obliegt dem Dokumentinhaber nach Übergabe.

Copyrights

Datenschutz

Auf Zustimmung durch den Auftraggeber wurden im Zuge des Assessments unvermeidbar personenbezogene Daten erhoben und zur Zielerreichung weiterverwendet. Eine langfristige Speicherung dieser Daten findet nicht statt. Mit Abschluss des Projektes und Übergabe der Dokumentation werden entsprechende Datensätze mit Ablauf von 14 Tagen nach Übergabe vernichtet.

ORGANISATORISCHES

Timeline

Datum / Uhrzeit	Topic
November/Dezember 2023	Vorgespräche / Organisation
08.12.2023	Beginn des Assessments
13.12.2023 - 10:46	Erste Rückmeldung seitens „White-Cell“
13.12.2023 - 22:12	Vollkompromittierung der Domain
18.12.2023	Statusupdate
30.01.2024	Initiales Debriefing + Workshop

Teamzusammensetzung

Die folgenden Personen waren auf Seiten der ProSec GmbH primär für die operative Durchführung des Assessments verantwortlich:

Name	Position	Spezialisierung
Chris	Red Team Lead	Koordination / Management
Robin	Red Team Assistant Lead	Active Directory - Infrastruktur
Michael	Senior Red Team Operator	Social Engineering / Physical Access
Robin C	Red Team Operator	Cloud - Infrastruktur

Die Auswahl der Teammitglieder erfolgte nach interner Rücksprache und unter Berücksichtigung der jeweiligen Spezialisierung.

EXECUTIVE SUMMARY

Überblick

Die ProSec GmbH wurde von der XY beauftragt, eine Angriffskampagne gegen die interne Infrastruktur durchzuführen. Der Durchführungszeitraum des Assessments erstreckte sich über den gesamten Monat Dezember 2023. Generelles Ziel war es, die Grundsteine für Tests gemäß „TIBER-EU" zu legen und die eigene Reaktions- und Handlungsfähigkeit auf externe Bedrohungen zu prüfen.

Um ein möglichst kohärentes Bild liefern zu können, sollten alle Testfelder, einschließlich Social Engineering und physischer Zugang, abgedeckt werden. Der physische Anteil wurde aufgrund parallel stattfindender Assessments nach Kundenrücksprache im Audit-Charakter durchgeführt. Das Social Engineering Szenario wurde nach Kundenrücksprache in einem gemeinsamen Workshop am 30.01.2024 live durchgeführt. Die Erkenntnisse hieraus lassen sich trotz des Audit-Charakters auf ein reales Assessment übertragen.

Ziel des Assessments war das Erlangen von administrativen Berechtigungen in der Active-Directory Domäne des Kunden, unter Umgehung bestehender Schutz- und Sicherheitsmaßnahmen. Es wurde im Testzeitraum keine Exfiltration von Unternehmensdaten vorgenommen. Das von der ProSec GmbH durchgeführte Assessment beinhaltete TTPs real agierender Akteure, um die im Vorfeld definierten Ziele zu erreichen.

Insgesamt wurden 13 Findings festgestellt und aufgenommen:

	High	Medium	Low	Info
Anzahl	5	4	1	3

Positive Beobachtungen

Auch wenn der primäre Fokus bei Red-Team Assessments auf den erkannten Schwachstellen liegt, konnten einige positive Beobachtungen gemacht werden:

Physical
Die physische Zutrittssicherung umfasst bereits Maßnahmen, wie eine Vereinzelungsanlage, die potentiellen Angreifern den Zutritt zum Hauptgebäude erschweren.

Technical
Mehrere erkannte Angriffstechniken seitens des Blue Teams.
Die Endpoint Protection Software hat den initialen Phishing Versuch unter Realbedingungen erfolgreich vereitelt und auch nach Umstellung des Szenarios konnte keine direkte Befehlsausführung erzielt werden.

Spezifische Beobachtungen werden in den folgenden Kapiteln detaillierter beschrieben.

Im Anschluss an das Assessment fand am dd.mm.yyyy ein gemeinsamer Tages - Workshop statt, in dem insbesondere die KillChain aufgearbeitet wurde.

Erkenntnisse

Folgende kritische Erkenntnisse konnten im Testzeitraum, sowie im anschließenden Workshop gewonnen werden:

- Viele Prozessdefinitionen und Best-Practices für Incident-Response oder administrative Tätigkeiten existieren, werden aktuell jedoch nicht „gelebt".

- Verschiedene Maßnahmen zur Härtung der Infrastruktur sind noch nicht vollumfänglich umgesetzt oder fehlen gänzlich.

- Die Erkennung von Angriffen ist zum jetzigen Zeitpunkt noch nicht zielgerichtet und muss ausgeweitet werden. Kritische Angriffe werden nur zum Teil erkannt, jedoch mit einer falschen Kritikalität eingestuft und behandelt. Dies sorgt dafür, dass eine Triage der kritischen Angriffe erst viel zu spät durchgeführt wird.

- Passwort-Management muss Unternehmensweit betrachtet werden.

Generelle Empfehlungen auf Basis dieser Erkenntnisse werden im entsprechenden Abschnitt tiefergehend behandelt.

Auswirkungen

Aufgrund der erfolgreichen, vollständigen Kompromittierung der Active Directory Domäne sind die potentiellen Auswirkungen im Falle eines realen Angriffs vielfältig und können vom Abfließen unternehmenskritischer Informationen bis hin zur Vollverschlüsselung durch Einschleusung von Ransomware reichen. Es besteht eine konkrete Gefahr für die Reputation des Unternehmens, wie auch direkte wirtschaftliche Konsequenzen im Falle einer Kompromittierung durch reale Akteure.

EINLEITUNG

Szenario

Das Assessment folgte prinzipiell einem Assumed-Breach Ansatz, bei dem ein Innentäter simuliert wird oder eine externe Partei ein sog. „Rogue-Device“ im Zielnetzwerk platziert. Dieser initiale Zugangsvektor wurde durch das simulierte Physical Assessment untermauert.

Zur Komplettierung der Angriffskette fanden zwei koordinierte Phishing Angriffe statt. Jeweils mit dem Ziel der unerlaubten Kommandoausführung auf den Zielsystemen, sowie dem Erlangen von Benutzerdaten.

Ziele des Assessments

Für das Assessment wurden folgende Ziele definiert:

- Simulation einer nicht näher definierten fortgeschrittenen Gruppe aus Angreifern, mit dem Erklärten Ziel die interne Active Directory Domäne zu infiltrieren und durch Erlangen administrativer Berechtigungen größtmöglichen Schaden anzurichten.
- Überprüfung der Incident-Response Kapazitäten des eingesetzten Blue-Teams auf Kundenseite.
- Auffinden eines externen Einstiegsvektors durch Zuhilfenahme technischer Methoden, einschließlich physischen Zutritts.
- Testen der Widerstandsfähigkeit von Mitarbeitern gegenüber dedizierten Phishing Angriffen.

Scope / Umfang des Assessments

Der festgelegte Scope umfasste die intern genutzte Infrastruktur, maßgeblich die Active Directory Domäne, sowie extern erreichbare Systeme. Eine genaue Auflistung kann dem initial übermittelten Scoping-Sheet entnommen werden.

Eine Auswahl der externen Systeme wurden bereits im Vorfeld (Oktober 2023) in einer separaten Beauftragung geprüft. Ein dedizierter Bericht zu den Findings liegt dem Kunden bereits vor.

Methodik und Testfelder

Im Gegensatz zu traditionellen, rein technischen Penetrationstests nutzen die Red Team Operateure der ProSec GmbH aktuelle Techniken realer Bedrohungen zur Zielerreichung. Dies schließt, sofern nicht explizit untersagt, ein Testen aller zur Verfügung stehenden Prüffelder mit ein. Aus ethischen und eindeutigen strafrechtlichen Gründen wird, auch wenn die aktuellen Entwicklungen bedauerlicherweise darauf hindeuten, auf jegliche Form der physischen Gewalt gegen Personen zur Zielerreichung bewusst verzichtet. Weiterhin anzumerken ist, dass nur die Taktiken und Techniken eingesetzt werden, die unmittelbar der Zielerreichung dienen. Es werden folglich nicht alle aufgefundenen Schwachstellen auch tatsächlich ausgenutzt.

Abweichungen

Da das Physical Assessment, sowie das Social Engineering erst im Workshop nach dem Assessment und nicht unter Realbedingungen durchgeführt wurden, konnten eigenständig gesammelte Informationen nicht oder nur unvollständig zum Einsatz gebracht werden. Daher bilden diese beiden Szenarien auch keinen Teil der aufgeführten Killchain, sondern werden in separaten Abschnitten aufgearbeitet.

Weiterhin wurde im Laufe des Assessments, aufgrund von fehlender Rückmeldung seitens der eingeteilten „White-Cell", auf auffälligere Angriffsmethoden zurückgegriffen, welche einen teils erheblichen Einfluss auf das generelle Vorgehen hatten. Dies sollte bei der Bewertung der durchgeführten Maßnahmen, wie auch den daraus resultierenden Erkenntnissen einbezogen werden.

Wir empfehlen, wie im Workshop besprochen, ein realistisches Physical Assessment des Hauptstandortes oder Alternativ eines integrierten Außenstandortes nach Abschluss des Projektes. Nur so lässt sich der initiale Zugangsvektor, der im Workshop nachgewiesen werden konnte, eindeutig bestätigen und eine adäquate Risikoeinschätzung abgeben.

KILL-CHAIN-ANALYSE

Zur Übersichtlichkeit wird auf eine Auflistung sämtlicher Aktivitäten an dieser Stelle verzichtet und nur die erwähnt, welche der Zielerreichung letztendlich zuträglich und erfolgreich waren. Eine Auflistung aller abgesetzten Befehle vom Rogue Device kann dem Anhang „command_history.txt" entnommen werden. Hierunter fallen ebenfalls Kommandos, welche im Testzeitraum erfolgreich vom Blue-Team erkannt worden sind.

Es ist zu diesem Zeitpunkt nicht mehr nachvollziehbar, ob die entsprechenden Alarme bereits zum Testzeitraum erkannt wurden oder erst im Nachgang an den Workshop, nach Durchsicht der entsprechenden Logfiles durch das Blue-Team aufgefunden werden konnten.

Stage 1 - Reconnaissance			
Aktion	**TTP**	**Kritikalität**	**Reaktion**
Platzieren eines Rogue Device	T1200	High	N/A - Simuliert
Reverse DNS-Lookup	T1590.002	Low	Nicht erkannt
Aggressive Portscans	T1595.001	Medium	Erkannt
Username Enumeration via Kerberos	T1087.002	Medium	Nicht erkannt

Stage 2 - Initial Access			
Aktion	**TTP**	**Kritikalität**	**Reaktion**
Phishing 1 - Command Execution	T1566.001	High / Info	N/A - Simuliert
Phishing 2 - Credential Harvesting	T1566.002	High / Info	N/A - Simuliert
Password Spraying	T1110.003	Medium	Teilweise erkannt
Domain Enumeration	T1069.002	High	Nicht erkannt

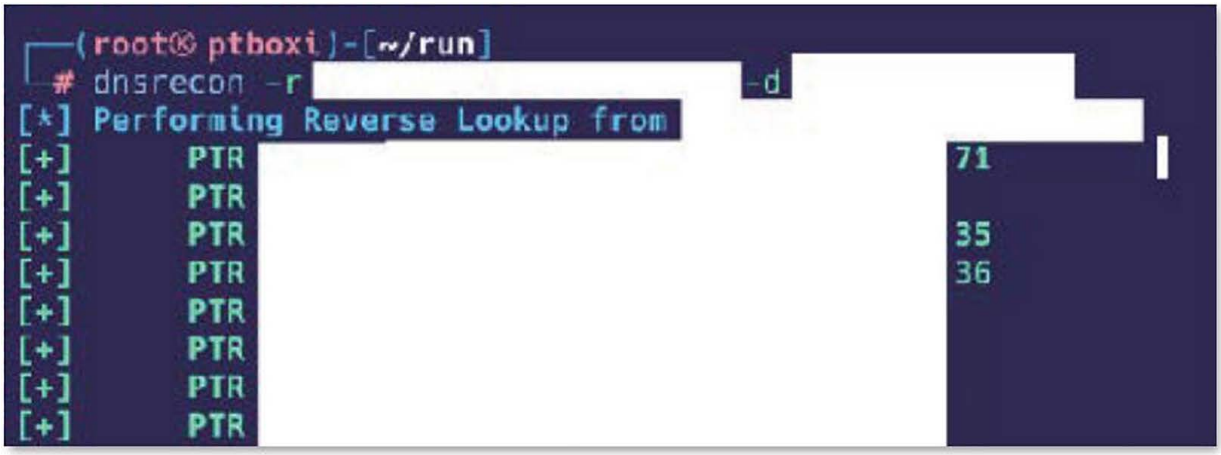
Stage 3 - Lateral Movement			
Aktion	**TTP**	**Kritikalität**	**Reaktion**
Ausbreitung via RDP, SMB und SSH	T1021.001	High	Teilweise erkannt

Stage 4 - Privilege Escalation			
Aktion	**TTP**	**Kritikalität**	**Reaktion**
Password Spraying	T1110.003	High	Nicht erkannt
Hinzufügen eines Accounts zur Domain	T1136.002	Medium	Erkannt, allerdings Log als „Info“ ohne Reaktion
Hinzufügen eines Accounts zu Domain Admins	T1098	High	Erkannt, allerdings Log als „Info“ ohne Reaktion
Abgriff der gesamten NTDS Datenbank	T1003.006	High	Erkannt, allerdings Log als „Info“ ohne Reaktion

Stage 5 - Exfiltration
Da dies im Vorfeld nicht definiert wurde, fand keine exemplarische Exfiltration von Daten statt.

KEY FINDINGS / BEOBACHTUNGEN

Reverse DNS-Lookup



Kategorie	Kritikalität	TTP	Status
Reconnaissance	Low	T1590.002	Nicht erkannt

Beschreibung:
Das Red Team benutzte den internen DNS-Server für einen groß angelegten Reverse Lookup des gesamten /8 Netzbereiches mittels „dnsrecon".

Auswirkungen:
Durch das Auflösen von validen IP Adressen im internen Netzwerk können Angreifer, ohne auf aggressive Host Discovery Scans zurückgreifen zu müssen, schnell einen Überblick über die verwendeten IP Adressen erlangen.

Abhilfe / Verbesserungen:
Einteilen der Subnetze in DNS Zonen und Einschränkung der Auflösung auf notwendige Server/Dienste mittels DNS Filter.

Referenzen:
https://learn.microsoft.com/en-gb/windows-server/networking/dns/deploy/dns-policies-overview

Aggressive PortScans

Kategorie	Kritikalität	TTP	Status
Reconnaissance	Medium	T1595.002	Erkannt

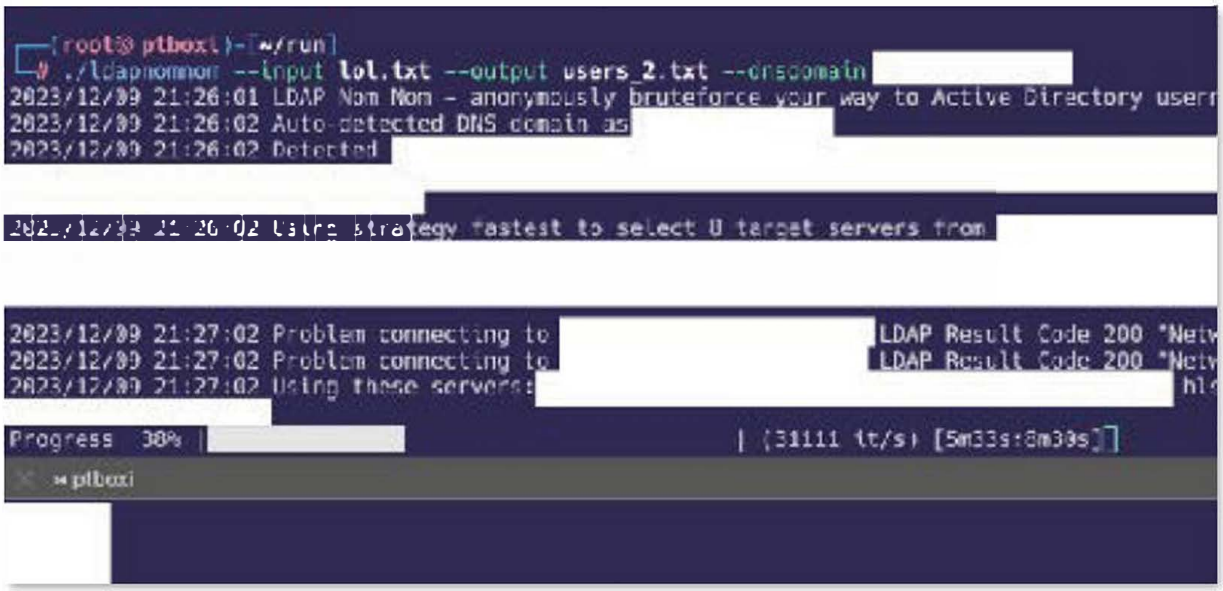
Beschreibung:
Das Red-Team führte, nachdem auf bisherige Aktionen keine Reaktion erfolgte, großangelegte PortScans mittels des Tools „nmap" zur Verifizierung der Aufmerksamkeit des Blue-Teams durch. Dies wurde erfolgreich erkannt und im gemeinsamen Workshop bereits aufgearbeitet.

Auswirkungen:
Keine direkten Auswirkungen, da der Angriff erkannt wurde.

Abhilfe / Verbesserungen:
Automatisches Trennen von unbekannten oder bekannten Netzwerkgeräten, die unüblichen Traffic in großen Mengen zu verschiedenen Zielen verursachen.

Referenzen:
https://www.fortinet.com/resources/cyberglossary/what-is-port-scan

Username Enumeration via Kerberos



Kategorie	Kritikalität	TTP	Status
Reconnaissance	Medium	T1087.002	Nicht erkannt

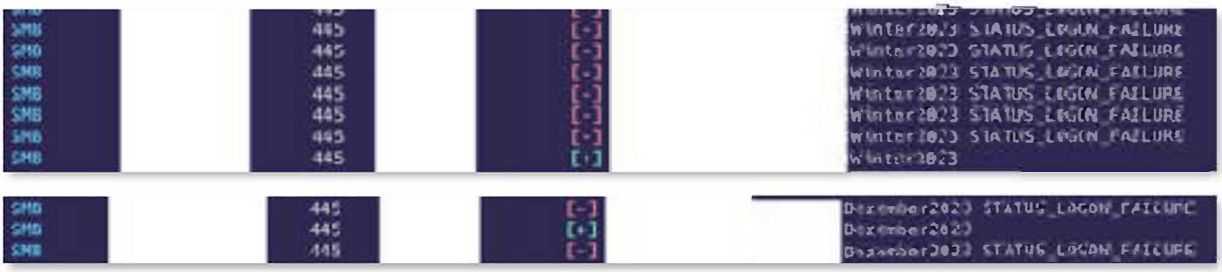
Beschreibung:
Das Red Team führte mittels des Tools „ldapnomnom" mehrfach eine Enumeration bestehender Nutzerkonten im Active Directory durch.

Auswirkungen:
Durch Ermittlung des verwendeten Namensschemas wurde der Grundstein für Password-Spraying Angriffe gelegt.

Abhilfe / Verbesserungen:
Ausweitung der Netzwerküberwachung, sowie Windows Event Monitoring.

Referenzen:
https://www.prosec-networks.com/en/blog/kerberos-attacks

Mehrere Password Spraying Angriffe



Kategorie	Kritikalität	TTP	Status
Initial Access / Privilege Escalation	Medium / High	T1110.003	Teilweise erkannt

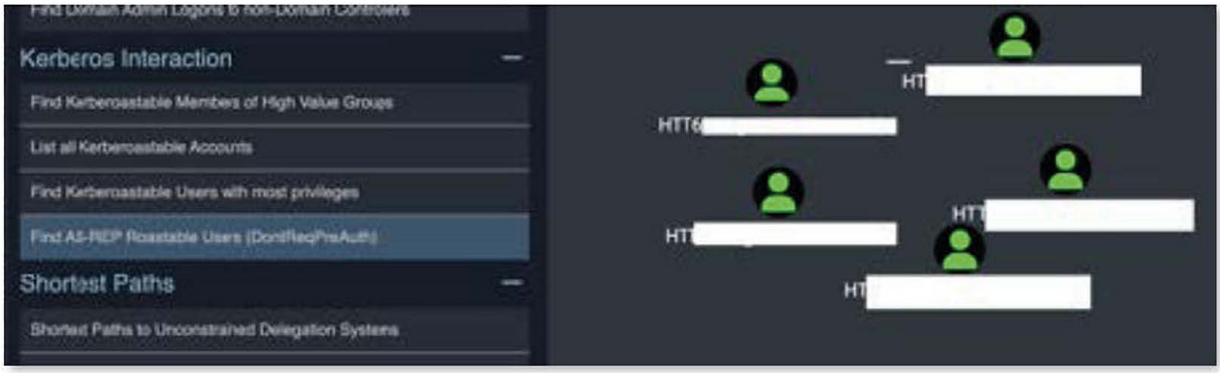
Beschreibung:
Das Red Team führte mittels des Tools „NetExec“ mehrere erfolgreiche Password-Spraying Angriffe durch. Das Sprayen von anonymen Authentifizierungen gegen mehrere Ziele wurde erfolgreich erkannt. Das schwerwiegendere Passwort-Spraying gegen den Domain Controller allerdings nicht.

Auswirkungen:
Durch das Erbeuten valider Authentifizierungen konnte letztendlich ein Foothold innerhalb der Domäne geschaffen werden, was eine Ausbreitung im Netzwerk ermöglichte. Weiterhin erlaubte ein Passwort Spraying Angriff die Übernahme eines privilegierten Accounts

Abhilfe / Verbesserungen:
Ausweitung der Netzwerküberwachung, sowie Windows Event Monitoring, sowie Einführung einer Fine-Grained Password Policy. Die aktuelle Password Policy erlaubt die Verwendung von äußerst schwachen Passwörtern.

Referenzen:
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-password-spray
https://www.techtarget.com/searchsecurity/tutorial/How-to-enable-Active-Directory-fine-grained-password-policies

Domain Enumeration mittels BloodHound



Kategorie	Kritikalität	TTP	Status
Reconnaissance	High	T1069.002	Nicht erkannt

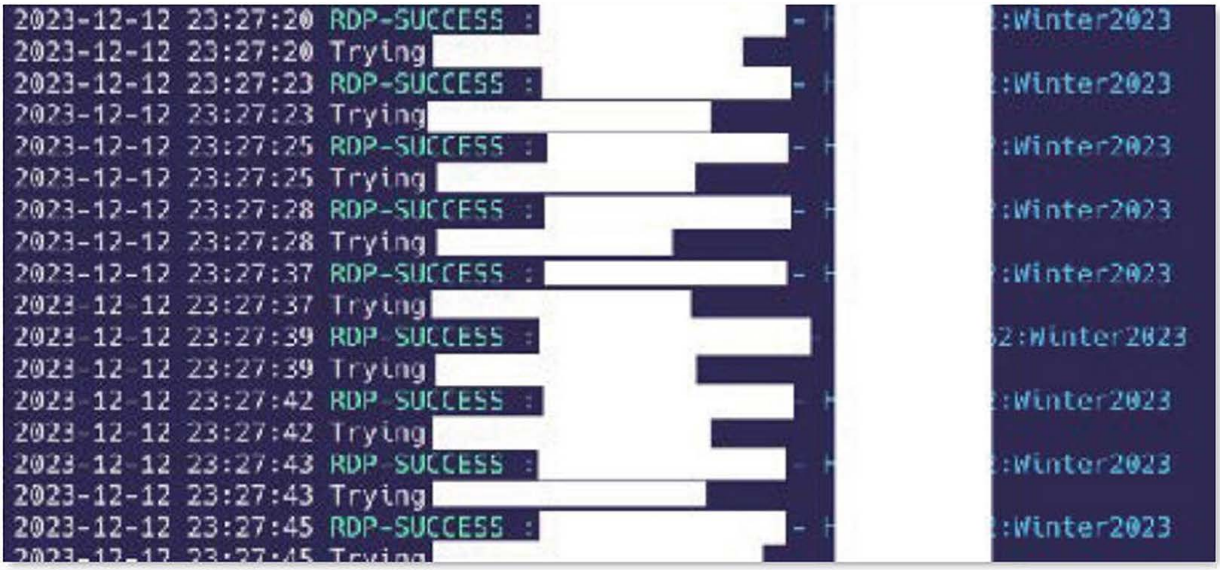
Beschreibung:
Das Red Team führte mit „bloodhound-python" eine großflächige Enumeration der gesamten Active Directory Infrastruktur durch.

Auswirkungen:
Jeder authentifizierte Domänenbenutzer darf sich bestimmte Informationen über die Infrastruktur beschaffen. Dies schließt Benutzer, Gruppen, Computeraccounts, sowie die jeweils zugewiesenen Berechtigungen mit ein. Ein möglichst dichtes Lagebild hilft dem Angreifer, weitere Angriffspfade zu erkennen und auszunutzen.

Abhilfe / Verbesserungen:
Einführung von Honeypot-Accounts mit minimalen Berechtigungen, von denen eine Alarmierung ausgeht, sobald die entsprechenden Objekte per LDAP angefragt werden. Weiterhin kann der LDAP Traffic selbst überwacht werden und potentielle Anstiege im Trafficvolumen aus ungewöhnlichen Quellen hervorgehoben werden.

Referenzen:
https://medium.com/securonix-tech-blog/detecting-ldap-enumeration-and-bloodhound-s-sharphound-collector-using-active-directory-decoys-dfc840f2f644

Ausbreitung via RDP, SMB und SSH



Kategorie	Kritikalität	TTP	Status
Lateral Movement	High	T1021.001	Teilweise erkannt

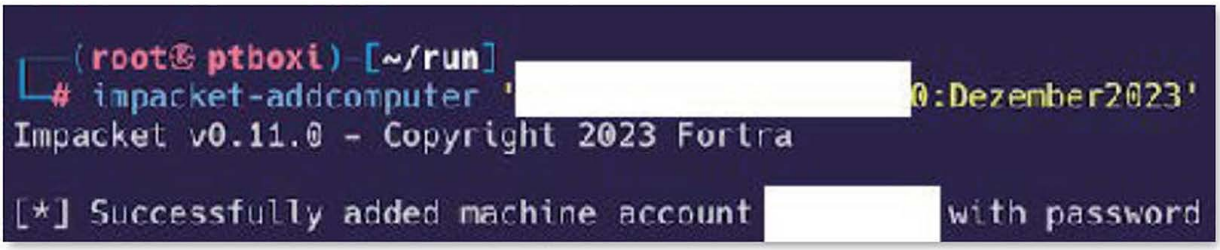
Beschreibung:
Das Red Team führte mit unterschiedlichen Tools, wie „crowbar" und „NetExec" eine Enumeration erreichbarer Dienste durch. Es konnte hierdurch eine Vielzahl von Zugängen zu unterschiedlichen Systemen erlangt werden.

Auswirkungen:
Erfolgreiches Lateral Movement dient dem Angreifer sich im Netzwerk auszubreiten, vorher unerreichbare Netzsegmente zugänglich zu machen, Informationen für weitere Angriffe zu sammeln und die eigene Präsenz durch Tunnel zu verbergen.

Abhilfe / Verbesserungen:
Ausweitung der Überwachung erfolgreicher Logon-Sessions auf verschiedene Dienste. Weiterhin sollten bestehende Berechtigungen neu evaluiert werden.

Referenzen:
https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events

Hinzufügen eines Computerkontos zur Domain



Kategorie	Kritikalität	TTP	Status
Persistence / Privilege Escalation	Medium	T1136.002	Nicht erkannt

Beschreibung:
Das Red Team fügte der Domain via „impacket-addcomputer" ein neues Computerkonto hinzu und sicherte sich so einen persistenten, authentifizierten Zugang.

Auswirkungen:
Computerkonten haben, durch die Mitgliedschaft der Gruppe „Domain Computers" und „Authenticated Users" in der Regel nur beschränkte Berechtigungen innerhalb der Domain, dienen jedoch als „Checkpoint", falls ein kompromittierter Benutzer sein Passwort ändert. Weiterhin kommen sie häufig als Dreh- und Angelpunkt für Angriffe, die einen Account mit SPN voraus setzen zum Einsatz.

Abhilfe / Verbesserungen:
Der erste Schritt durch das Herabsetzen der Machine Account Quota auf null ist bereits getan. Als Verbesserung könnte man das Privileg, Computerkonten zu erstellen nur einem einzelnen spezifischen Service Account zusprechen. Weiterhin sollte das ungeplante hinzufügen von Objekten im Active Directory Alarmierungen nach sich ziehen.

Referenzen:
-

Hinzufügen des Computerkontos zu Domain Admins

Kategorie	Kritikalität	TTP	Status
Privilege Escalation	High	T1098	Erkannt, aber nur Log ohne Reaktion

Beschreibung:
Das Red Team fügte via „net rpc“ das neue Computerkonto der Gruppe Domain Admins hinzu und erlangte somit Vollzugriff über die gesamte Active Directory Domain.

Auswirkungen:
Da den Domain Admins in der Regel sämtliche Berechtigungen innerhalb der Active Directory Infrastruktur zustehen, ist ab diesem Zeitpunkt von einer Vollkompromittierung der Infrastruktur auszugehen. Die Konsequenzen reichen vom Datenabfluss bis hin zur Verschlüsselung durch Ransomware.

Abhilfe / Verbesserungen:
Strikte Überwachung der Mitglieder privilegierter Gruppen. Sofortige Alarmierung bei nicht abgesprochenen Veränderungen dieser Struktur. Dies betrifft nicht nur die Domain Admins, sondern alle Gruppen, denen besondere Privilegien zuerkannt werden.

Referenzen:
-

Abgriff der gesamten NTDS Datenbank

Kategorie	Kritikalität	TTP	Status
Privilege Escalation	High	T1003.006	Nicht erkannt

Beschreibung:
Das Red Team sicherte sich sämtliche Benutzerauthentifizierungen in gehashter Form durch das Abgreifen der NTDS Datenbank eines Domain Controllers mithilfe von „impacket-secretsdump".

Auswirkungen:
Durch das Abgreifen sämtlicher Benutzerauthentifizierungen sind alle Dienste verwendbar, die eine NTLM Authentifizierung erfordern. Weiterhin kann dieser NTDS Dump mithilfe einer Dictionary-Attack geknackt werden, um an die entsprechenden Klartextkennwörter der Benutzer zu gelangen.

Abhilfe / Verbesserungen:
Überwachung der Domaincontroller auf „dcsync" Operationen, die nicht von einem anderen Domain Controller ausgehen oder abweichend vom Zeitplan der autorisierten Domain Replikation sind.

Referenzen:
https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection

WEITERE FINDINGS

Platzieren eines Rogue Device

Kategorie	Kritikalität	TTP	Status
Initial Access	High	T1200	N/A

Beschreibung:
Das Red Team war während des simulierten Physical Assessments in der Lage die bestehende Port-Security und Network Access Control mittels der gespooften MAC Adresse eines Druckers zu umgehen und konnte ein Fremdgerät ins Netzwerk einschleusen. Bestehende Möglichkeiten zum „Fingerprinting" zur Verifizierung von Geräten scheinen nicht voll funktionsfähig implementiert zu sein.

Auswirkungen:
Durch das Einbringen von Fremdgeräten erlangt ein Angreifer initialen Zugang zum Unternehmensnetzwerk und legt den Grundstein für die weitere Killchain.

Abhilfe / Verbesserungen:
Erneute Überprüfung und Korrektur der eingesetzten Maßnahmen zur Absicherung von Netzwerkports. Koordination mit eingesetztem Personal oder externen Dienstleistern zur Beseitigung der Mängel.

Referenzen:
-

Phishing Versuch 1 - Command Execution

Kategorie	Kritikalität	TTP	Status
Initial Access	High	T1566.001	N/A

Beschreibung:
Das Red Team versuchte über eine zum Download bereitgestellte .iso Datei, Nutzer zur Ausführung zu bewegen und Zugang zum Unternehmensnetzwerk zu erhalten. Der vorgeschaltete Webfilter verhinderte den Download erfolgreich. Nach Umstellung auf eine .zip Datei konnte die Datei heruntergeladen werden. Eine Ausführung wurde von der eingesetzten Endpoint Protection verhindert. Im späteren Verlauf stellte sich heraus, dass die Endpoint Protection nur die lokalen Laufwerke überwacht, jedoch nicht via SMB angeschlossene Laufwerke. Viele Benutzer haben das Default Downloadverzeichnis allerdings auf genau diese Netzlaufwerke verlegt, sodass letztendlich simuliert eine erfolgreiche Ausführung der Malware demonstriert werden konnte.

Auswirkungen:
Erfolgreiche Command Execution via Phishing auf Clientsystemen legt, neben dem platzieren eines Rogue Device den Grundstein für weitere Angriffe und eine potentielle Killchain.

Abhilfe / Verbesserungen:
Phishing ist, zum heutigen Zeitpunkt, immer noch der primäre Einstiegsvektor in Unternehmensnetzwerke. Da dieser Phishing Versuch nur simuliert wurde, kann keine valide Aussage zur User Awareness getroffen werden. Allerdings wird dringend empfohlen, die Überwachung der angeschlossenen SMB Shares, besonders Home-Laufwerke von Benutzern in die Überwachung zu integrieren. Weiterhin empfehlen sich Beschränkungen für die Wahl der Downloadverzeichnisse, sowie das Blockieren weiterer, potentiell gefährlicher Dateiendungen.

Referenzen:
-

Phishing Versuch 2 - Credential Harvesting

Kategorie	Kritikalität	TTP	Status
Initial Access	High	T1566.002	N/A

Beschreibung:
Das Red Team sendete in Abstimmung mit dem vorhandenen Personal eine Phishing Nachricht an einen ausgewählten Teilnehmerkreis. Vorgegeben wurde die Einführung eines unternehmensweiten Benefitportals. Ziel war das Abgreifen von validen Benutzerdaten. Es konnten während des Tests insgesamt elf valide Benutzerkennungen erbeutet werden.

Auswirkungen:
Abgefangene Benutzerdaten können von Angreifern auf verschiedene Arten wiederverwendet werden. Bei Vorhandensein eines Rogue-Devices dienen Sie parallel als Einstiegspunkt ins Netzwerk.

Abhilfe / Verbesserungen:
Phishing ist, zum heutigen Zeitpunkt, immer noch der primäre Einstiegsvektor in Unternehmensnetzwerke. Da dieser Phishing Versuch nur simuliert wurde, kann keine valide Aussage zur User Awareness getroffen werden. Dennoch wird dringend empfohlen, regelmäßige Security Awareness Kampagnen zu initiieren, um das bestehende Risiko zu minimieren.

Referenzen:
-

VORLÄUFIGE URSACHENANALYSE

Ziel dieser Analyse ist es, einen ganzheitlichen Blick auf die zugrunde liegenden Probleme zu werfen, die zu den festgestellten Schwachstellen beigetragen haben.

Die Ermittlung einer genauen Ursache ist in diesem expliziten Beispiel schwierig, da mehrere Faktoren unmittelbaren Einfluss auf die Situation hatten. Beispielsweise fanden das Social Engineering, wie auch der physische Zutritt nicht unter Realbedingungen statt. Diese finden daher im weiteren Verlauf auch keine Betrachtung. Aufgrund dessen ist die abschließende Einstufung nach Kritikalität nur bedingt möglich und wird hierbei nicht vorgenommen.

Menschen

Mangelndes Bewusstsein für Cybersicherheit und mangelnde Schulung der Mitarbeiter haben maßgeblich zur erfolgreichen Durchführung von Passwort-Spraying Angriffen beigetragen. Die Mitarbeiter verwenden schwache oder gebräuchliche Passwörter, weil sie nicht wissen, wie man sichere Passwörter verwendet oder das entsprechende Sicherheitsbewusstsein fehlt. Im Workshop kristallisierte sich ebenfalls heraus, dass die Supportmitarbeiter diese schwachen Passwörter im Rahmen einer Kennwortzurücksetzung vergeben.

Prozesse

Die Ergebnisse deuten darauf hin, dass es möglicherweise unzureichende Sicherheitsrichtlinien und -verfahren in Bezug auf Kontoverwaltung, Zugangskontrolle und Netzwerksegmentierung gibt oder diese nicht konsequent umgesetzt werden. Die Möglichkeiten für Lateral Movement und Privilege Escalation, deuten auf eine mangelnde Durchsetzung des Prinzips der geringsten Privilegien und unzureichende Netztrennung hin.

Technologie

Die Tatsache, dass grundlegende Angriffe wie die Enumeration der gesamten Domäne, sowie das Abgreifen der NTDS Datenbank nicht erkannt wurden untermauern die Vermutung, dass es teilweise blinde Flecken in der Überwachung gibt. Im Workshop stellte sich ebenfalls heraus, dass einige Angriffe durchaus protokolliert, jedoch aufgrund unzureichender Kritikalität nicht alarmiert wurden. Weiterhin existieren derzeit zu viele „Whitelistings" in der Überwachung und werden scheinbar unkontrolliert eingerichtet bzw. erteilt. Dies erschwert eine effiziente Überwachung und sorgt letztendlich dafür, dass die Mitarbeiter der defensive kaum abschätzen können, ob eine Bedrohung real ist oder nur das Resultat eines fehlerhaften Dienstes.

ARTEFAKTE

Auflistung

Im Testzeitraum wurden keine physischen Artefakte oder Malware hinterlassen. Es wurden jedoch Änderungen an der Active Directory Infrastruktur vorgenommen. Diese Änderungen sollten schnellstmöglich beseitigt werden, um das Risiko einer erneuten Kompromittierung zu verringern.

Folgende Objekte sind betroffen:

- Selbstständig angelegtes Computerkonto xxxxxxx$
- Selbstständig angelegtes Computerkonto xxxxxxx$
- Gruppe der Domain Admins

Beseitigung

Zur Beseitigung der Artefakte genügt die Löschung der angelegten Computerkonten, sowie das Entfernen des Computerkontos „xxxxxxx$" aus der Gruppe der Domain Admins.

EMPFEHLUNGEN

Quick Wins

Zur schnellen Erhöhung der Sicherheit lassen sich folgende Maßnahmen unmittelbar anwenden:

- Änderung aller Benutzerkennwörter nach Abschluss des Assessments
- Änderung der Kritikalität von identifizierten Meldungen im Testzeitraum, insbesondere bei Änderungen der Infrastruktur wie dem hinzufügen eines Nutzers zu einer administrativen Gruppe
- Einführung von Honeypot-Accounts zur Erkennung von AD Enumerationen

Langfristige Sicherheitsverbesserungen

Folgende Lösungsansätze dienen der langfristigen Verbesserung der Unternehmenssicherheit und beziehen sich auf Findings, deren Abstellung entweder technisch oder organisatorisch nicht kurzfristig umsetzbar ist.

- Einführung oder Ausbau regelmäßiger Personalschulungen zur Steigerung und Aufrechterhaltung der Wachsamkeit gegenüber Phishing Attacken, sowie der Vergabe sicherer Kennwörter
- Ausweitung und Zentralisierung des Monitorings, sowie Entschlackung bestehender Whitelistings
- Einführung bzw. Überarbeitung von Prozessen zur Erstellung und regelmäßiger Kontrolle bestehender, sowie zukünftiger Whitelistings im Monitoring
- Überprüfung des bestehenden Rollen- und Rechtekonzeptes auf Aktualität, sowie Einführung von Prozessen zur regelmäßigen Kontrolle
- Erstellung bzw. Überprüfung der bestehenden Netztrennung nach Least-Privilege Prinzip
- Umsetzung von weiterführenden Härtungsmaßnahmen im Active-Directory. Hierzu existieren verschiedene Best-Practice Guides, an denen man sich exemplarisch für die Umsetzung orientieren kann.

ANHÄNGE

Alle relevanten Screenshots, sowie die Kommandohistorie der PentestBox befinden sich im beiliegenden .zip Archiv.

Glossar

Abkürzung / Begriff	Bedeutung
TIBER-EU	Threat Intelligence Based Ethical Red-Teaming
TTP	Tactics, Techniques and Procedures
DNS	Domain Name System
RDP	Remote Desktop Protokoll
SSH	Secure Shell
SMB	Server Message Block
NTDS	New Technology Directory Services
NTLM	New Technology Lan Manager
SPN	Service Principal Name

REFERENZEN

Quellenangaben

- https://www.fortinet.com/resources/cyberglossary/what-is-port-scan
- https://learn.microsoft.com/en-gb/windows-server/networking/dns/deploy/dns-policies-overview
- https://learn.microsoft.com/en-gb/windows-server/networking/dns/deploy/apply-filters-on-dns-queries
- https://www.prosec-networks.com/en/blog/kerberos-attacks/https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-password-sprayhttps://www.techtarget.com/searchsecurity/tutorial/How-to-enable-Active-Directory-fine-grained-password-policies
- https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-logon-events
- https://medium.com/securonix-tech-blog/detecting-ldap-enumeration-and-bloodhound-s-sharphound-collector-using-active-directory-decoys-dfc840f2f644
- https://www.alteredsecurity.com/post/a-primer-on-dcsync-attack-and-detection
- https://www.dnb.nl/media/tu3ageri/tiber-eu-guidance-for-the-red-team-test-report.pdf

ProSec
Security redefined.

WHO WE ARE

2016
gegründet

50+
Team-Mitglieder

1000+
durchgeführte Assessments

100%
Systemübernahmen

UNSERE MISSION

Menschenleben retten und schützen, indem wir die digitale Infrastruktur von Unternehmen nachhaltig sicher machen.

UNSERE VISION

Wir wollen IT Security viral gehen lassen.

HOW WE SUPPORT YOUR INFORMATION SECURITY

Penetration Testing IT Security Consulting Ethical Hacker Courses

„IT Security aus der Eifel
für Kunden weltweit."