

1

1. Detect Password Spraying via Windows Event

Executive Summary

Adversaries may attempt to creatively brute force many accounts on a network by increasing the time between login attempts, preventing automatic account locking. Since waiting more time impacts speed of the attack, adversaries typically target more than one account simultaneously.

Name

Detect Password Spraying via Windows Events

1

Problem Statement

Password spraying targets the human tendency to both use weak password and reuse them. Adversaries attempt to avoid brute force detection and prevention by increasing time between password attempts. To account for the significant reduction in the speed of the attack, multiple accounts are targeted in parallel. Each of these parallel attacks are progressed slow enough to keep the account from reaching the failed attempts lockout policy.

Objectives

- Detect low and slow brute force method known as password spraying

tool-manageme...zip ^



1



Analysis

Password spraying uses one password (e.g. 'Password01'), or a small list of passwords, that matches the complexity policy of the domain and may be a commonly used password. Logins are attempted with that password and many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords.

I 2

Recommended Response Action(s)

- Determine source and destination account/systems
- Collect and analyze surrounding events
- Issue password change requirement to account owner(s)
- Determine if source/destination accounts/systems are compromised
- Consider quarantining, isolating, or disabling compromised accounts/systems

Data Stream Analysis

- Windows Security Event ID 4624
- Windows Security Event ID 4625
- Windows Security Event ID 4648

tool-manageme...zip



1

- Collect and analyze surrounding events
- Issue password change requirement to account owner(s)
- Determine if source/destination accounts/systems are compromised
- Consider quarantining, isolating, or disabling compromised accounts/systems

Data Stream Analysis

- Windows Security Event ID 4624
- Windows Security Event ID 4625
- Windows Security Event ID 4648

I

2. SIEM Use Cases based on Layer 3 Firewalls

Traffic from Printers to Servers/Workstations

- Blacklist Alert

Traffic from Servers to Workstations

- Blacklist Alert

Traffic from Workstations to Workstations

- Rolling Whitelist Alert

Unauthorized Egress DNS Traffic

3

t 1



- Blacklist Alert
- Port 53
- Could indicate DNS Tunneling

Unauthorized Egress NTP Traffic

- Blacklist Alert
- Port 123

OS Update Requests to Non-Company Servers

- Blacklist Alert
- Accessing default Windows, Ubuntu, etc update IP addresses could indicate a rogue device

Newly Observed Port Use

- Rolling Whitelist Alert
- Ideally separate system types into different rolling whitelists (printers, servers, workstations)

Known-bad Port Observed

- Blacklist Alert

4



IP ADDRESS OBSERVED

tool-manage.zip

t 1

1 day ago



Unauthorized Egress NTP Traffic

- Blacklist Alert
- Port 123

OS Update Requests to Non-Company Servers

- Blacklist Alert
- Accessing default Windows, Ubuntu, etc update IP addresses could indicate a rogue device

Newly Observed Port Usage

- Rolling Whitelist Alert
- Ideally separate system types into different rolling whitelists (printers, servers, workstations)

Known-bad Port Observed

- Blacklist Alert

Known-bad IP Address Observed

- Blacklist Alert

Newly observed UDP Traffic

- Rolling Whitelist Alert

Spike in Outbound Denies

- Threshold Alert

Spike in Egress Sessions

5

school-manageme...zip

6

- Threshold Alert

Anomalous Upload/Download Ratio

- Threshold Alert

Unauthorized Egress Email Traffic

- Blacklist Alert
- Ports include 25, 143, 587, 110, etc

Unauthorized Egress Web Requests

- Not originating from company proxy
- Blacklist

Border Firewall Egress Default Deny Blocks

- Rolling Whitelist Alert

3. SIEM Use Cases for Laver

el-wp-lite.1.3.10.zip



school-manageme...zip



rt 1

26 minutes ago



3. SIEM Use Cases for Layer 7 Firewalls. Note that Layer 3 Firewall use cases also apply here.

Abnormal Expired Certificates

- Aggregate Count

Abnormal Self-Signed Certificates

- Aggregate Count

Abnormal certificate Algorithms/Sizes

7

- Aggregate Count

Abnormal Certificates Validity Length

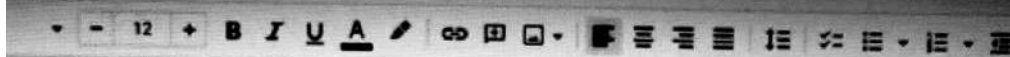
hotel-wp-lite.1.3.10.zip

school-manageme...zip



s Part 1

help Last edit was 29 minutes ago



• Aggregate Count

Abnormal Certificates Validity Length

- Blacklist Alert
- Suggest looking for 5 years and older

Certificates with Abnormal Common Name Fields

- Blacklist Alert

Certificates with Blank Fields that are Commonly Filled

- Blacklist Alert

Certificates with Invalid Country Codes / States

- Blacklist Alert

Newly-observed Protocol in Use

- Rolling Whitelist

Protocol Use Over Non-Standard Port

- Blacklist

Web requests Directly to IP Address

- Blacklist Alert
- AKA Naked IP

Newly Observed File Transfer Protocol Use

- Rolling Whitelist Alert
- FTP, TFTP, SSH, etc

8

hotel-wp-lite.1.3.10.zip school-manageme...zip



- Blacklist Alert
- AKA Naked IP

Newly Observed File Transfer Protocol Use

- Rolling Whitelist Alert
- FTP, TFTP, SSH, etc

Unauthorized ~~X-Forwarded-For~~ Address

9

- X-Forwarded-For specifies the proxy forwarding
- Blacklist

4. Web Server Use Cases

Aggregate Count

- HTTP GET Method Counts
- HTTP POST Method Counts
- User Agent String Counts
- Allow/Block Ratio per System/User
- GET/POST Ratio per System/User

posterity.2.3.zip

hotel-wp-lite.1.3.10.zip

school-manageme

40 minutes ago

B I U A                 

- X-Forwarded-For specifies the proxy forwarding
- Blacklist

4. Web Server Use Cases

Aggregate Count

- HTTP GET Method Counts
- HTTP POST Method Counts
- User Agent String Counts
- Allow Block Ratio per System/User
- GET/POST Ratio per System/User
- Up/Down Bytes Ratio per System/User

Blacklist Alert

- URL containing "/etc/"
- URL containing "/system32/"
- URL containing "cmd.exe"
- URL containing "command.exe"
- URL containing "powershell.exe"
- URL containing an IP Address
- HTTPS request with 3 or more / (when no break-and-inspect is deployed, this signifies HTTP over port 443)
- Known-bad User Agents
- Suspicious User Agents
 - Contains "curl"
 - Contains "python"
 - Contains "Go-http-client"
 - Contains "wget"
- User Agent string containing 'Nmap'
- Known-bad Domains
- A privileged account generates any web traffic
- A service account generates any web traffic

10

erity.2.3.zip

hotel-wp-lite 1.3.10.zip

school-manageme...zip



4. Web Server Use Cases

Aggregate Count

- HTTP GET Method Counts
- HTTP POST Method Counts
- User Agent String Counts
- Allow Block Ratio per System/User
- GET/POST Ratio per System/User
- Up Down Bytes Ratio per System/User

Blacklist Alert

- URL containing "/etc/"
- URL containing "/system32/"
- URL containing "cmd.exe"
- URL containing "command.exe"
- URL containing "powershell.exe"
- URL containing an IP Address
- HTTPS request with 3 or more / (when no break-and-inspect is deployed, this signifies HTTP over port 443)
- Known-bad User Agents
- Suspicious User Agents
 - Contains "curl"
 - Contains "python"
 - Contains "Go-http-client"
 - Contains "wget"
- User Agent string containing 'Nmap'
- Known-bad Domains
- A privileged account generates any web traffic
- A service account generates any web traffic
- A system account generates any web traffic
- User Agent string containing 'Nmap'

11

Whitelist Alert

I

t 2

was 2 days ago



- Known-bad Domains
- A privileged account generates any web traffic
- A service account generates any web traffic
- A system account generates any web traffic
- User Agent string containing 'Nmap'

Whitelist Alert

12

- Newly Observed Domains
- Web Traffic to Domains not in "Top Million" Lists

Levenshtein Score Alert

- Typosquatting company and trusted domains

Rolling Whitelist Alert

- Newly Observed User Agent

Shannon Entropy Score Alert

- High Entropy Domain Name

Threshold Alert

- User Name, Request URL Host, Bytes Out Total where Bytes Out Total out exceeds threshold
- User Name, Allow Count, Block Count, Allow/Block Ratio where Allow/Block Ratio exceeds threshold



Part 2

edit was 2 days ago

- A system account generates any web traffic
- User Agent string containing 'Nmap'

Whitelist Alert

13

- Newly Observed Domains
- Web Traffic to Domains not in "Top Million" Lists

Levenshtein Score Alert

- Typosquatting company and trusted domains

Rolling Whitelist Alert

- Newly Observed User Agent

Shannon Entropy Score Alert

- High Entropy Domain Name

Threshold Alert

- User Name, Request URL Host, Bytes Out Total where Bytes Out Total out exceeds threshold
- User Name, Allow Count, Block Count, Allow/Block Ratio where Allow/Block Ratio exceeds threshold
- User Name, GET Total, Post+Put Total, GET POST/Put Ratio where GET POST/Put Ratio exceeds threshold
- User Name, Bytes In Total, Bytes Out Total, Bytes In/Out Ratio Where Bytes

- Newly Observed User Agent

Shannon Entropy Score Alert

- High Entropy Domain Name

Threshold Alert

- User Name, Request URL Host, Bytes Out Total where Bytes Out Total out exceeds threshold
- User Name, Allow Count, Block Count, Allow/Block Ratio where Allow/Block Ratio exceeds threshold
- User Name, GET Total, Post+Put Total, GET/POST/Put Ratio where GET/POST/Put Ratio exceeds threshold
- User Name, Bytes In Total, Bytes Out Total, Bytes In/Out Ratio Where Bytes In/Out Ratio exceeds threshold

14

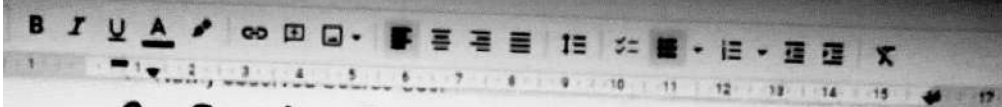
5. Service Modification Use Cases

Service modification can be used by an adversary to achieve persistence

Rolling Whitelist Alert

2

2 days ago



6. Service Creation Use Cases

Service creation can be used by an adversary to achieve persistence.

15

Whitelist Alert

- Anomalous Services

Rolling Whitelist Alert

- Newly observed Service File Name: Service Account

Log Source Examples

- Windows Security Event ID 4697

7. Scheduled Task Creation Use Cases

Whitelist Alert

- Anomalous Scheduled Task Creator

Rolling Whitelist Alert



- Newly observed Service File Name, Service Account

Log Source Examples

- Windows Security Event ID 4697

7. Scheduled Task Creation Use Cases

Whitelist Alert

- Anomalous Scheduled Task Creator

Rolling Whitelist Alert

- Newly observed Scheduled Task Name

Log Source Examples

- Windows Security Event ID 4698

8. Resource Consumption Use Cases

Threshold Alert

- High CPU/Memory Usage over X Minutes

16

8.Resource Consumption Use Cases

Threshold Alert

- High CPU/Memory Usage over X Minutes

17

8.Resource Consumption Use Cases

Threshold Alert

- High CPU/Memory Usage over X Minutes

18

9. Registry Modification Use Cases

Blacklist Alert

- "HKU(SID)\Software\Microsoft\Windows\CurrentVersion\Run"
- "HKU(SID)\Software\Microsoft\Windows\CurrentVersion\RunOnce"
- "HKU(SID)\Software\Microsoft\Windows\CurrentVersion\RunOnceEx"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx"
- "HKU(SID)\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
- "HKU(SID)\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders"
- "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders"
- "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"

9. Registry Modification Use Cases

Blacklist Alert

- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\Run"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\RunOnce"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\RunOnceEx"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\Run"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders"
- "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders"
- "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\RunServices"
- "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run"
- "HKU{SID}\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run"
- "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit"
- "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell"
- "HKU{SID}\Software\Microsoft\Windows NT\CurrentVersion\Windows"

10. Network Activity by Full Packet Capture Use Cases

Blacklist Alert

19



- "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit"
- "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell"
- "HKU{SID}\Software\Microsoft\Windows NT\CurrentVersion\Windows"

10. Network Activity by Full Packet Capture Use Cases

Blacklist Alert

- Certificate Expired
- Certificate is Self-Signed
- Certificate Algorithm is Weak

I 20

- Certificate Validity Exceeds 3 Years
- Certificate Common Name Has no Periods
- Certificate With Blank Fields

Whitelist Alert

- Certificate with Invalid Country Code/State

Log Source Examples

- Network IDS Logs



- Certificate Validity Exceeds 3 Years
- Certificate Common Name Has no Periods
- Certificate With Blank Fields

Whitelist Alert

- Certificate with Invalid Country Code/State

Log Source Examples

- Network IDS Logs
- Layer 7 Firewall Logs

21 I

11. Network Activity by Process Use





Log Source Examples

- Network IDS Logs
- Layer 7 Firewall Logs

11. Network Activity by Process Use Cases

Blacklist Alert

- mistsc.exe from an unexpected source user
- wscript.exe
- cscript.exe
- bitsadmin.exe


Whitelist Alert

- Unexpected Process Names with network activity

Rolling Whitelist Alert

- Newly observed Process
- Newly observed Port
- Newly observed Source Port
- Newly observed Source Port Name
- Newly observed Destination Port
- Newly observed Destination Port Name

22

- 
- cscript.exe
 - bitsadmin.exe

Whitelist Alert


- Unexpected Process Names with network activity

Rolling Whitelist Alert

- Newly observed Process
- Newly observed Port
- Newly observed Source Port
- Newly observed Source Port Name
- Newly observed Destination Port
- Newly observed Destination Port Name

I 23

Threshold Alert

- Source System, Destination System, Protocol=UDP where Source System Count exceeds threshold
 - Source System, Destination System, Protocol=UDP where Destination System Count exceeds threshold
 - Source System, Protocol=TCP where Count exceeds threshold
 - Destination System, Protocol=TCP where Count exceeds threshold
 - Bytes In Total, Bytes Out Total, Bytes In/Out Ratio where Bytes In/Out Ratio exceeds threshold
 - Connection Length where Connection Length exceeds threshold
- 

Threshold Alert

- Source System, Destination System, Protocol=UDP where Source System Count exceeds threshold
- Source System, Destination System, Protocol=UDP where Destination System Count exceeds threshold
- Source System, Protocol=TCP where Count exceeds threshold
- Destination System, Protocol=TCP where Count exceeds threshold
- Bytes In Total, Bytes Out Total, Bytes In/Out Ratio where Bytes In/Out Ratio exceeds threshold
- Connection Length where Connection Length exceeds threshold

Log Source Examples

- Sysmon Event ID 3

12. Network Activity by IP Use Cases

Blacklist Alert

- Egress Traffic to Known-Bad Port
- Egress Traffic to Known Bad IP
- Egress Traffic to Known Sinkhole IP

Whitelist Alert

- Anomalous Destination Port Use

Rolling Whitelist Alert

- Newly observed Source System, Protocol
- Newly Observed Source System, HourOfDay

24

1 edit was 3 minutes ago



Log Source Examples

- Sysmon **Event ID 3**

12. Network Activity by IP Use Cases

Blacklist Alert

- Egress Traffic to Known-Bad Port
- Egress Traffic to Known Bad IP
- Egress Traffic to Known Sinkhole IP

Whitelist Alert

- Anomalous Destination Port Use

Rolling Whitelist Alert

- Newly observed Source System, Protocol
- Newly Observed Source System, HourOfDay

Threshold Alert

- Source System, Destination System, Protocol=UDP where Source System Count exceeds threshold

25





- Egress Traffic to Known Sinkhole IP

Whitelist Alert

- Anomalous Destination Port Use

Rolling Whitelist Alert

- Newly observed Source System, Protocol
- Newly Observed Source System, HourOfDay

Threshold Alert

- Source System, Destination System, Protocol=UDP where Source System Count exceeds threshold

26

- Source System, Destination System, Protocol=UDP where Destination System Count exceeds threshold
- Source System, Protocol=TCP where Count exceeds threshold
- Destination System, Protocol=TCP where Count exceeds threshold

Log Source Examples

- Layer 3 or 7 Firewall Logs

13. Network Activity by Flow Use Cases



- Source System, Destination System, Protocol=UDP where Destination System Count exceeds threshold
- Source System, Protocol=TCP where Count exceeds threshold
- Destination System, Protocol=TCP where Count exceeds threshold

Log Source Examples

- Layer 3 or 7 Firewall Logs

13. Network Activity by Flow Use Cases

Blacklist Alert

- Known-Bad Destination Port Use

Whitelist Alert

- Anomalous Destination Port Use

Rolling Whitelist Alert

- Newly observed Source System, Protocol
- Newly Observed Source System, HourOfDay

Threshold Alert

- Source System, Destination System, Protocol=UDP where Count exceeds threshold
- Source System, Destination System, Protocol=UDP where Count exceeds threshold
- Source/Destination System, Protocol=TCP where Count exceeds threshold
- Source/Destination System, Protocol=TCP where Count exceeds threshold
- Source/Destination System, Bytes In Total, where Bytes In Total exceeds threshold

27

3 minutes ago



13. Network Activity by Flow Use Cases

Blacklist Alert

- Known-Bad Destination Port Use

Whitelist Alert

- Anomalous Destination Port Use

Rolling Whitelist Alert

- Newly observed Source System, Protocol
- Newly Observed Source System, HourOfDay

Threshold Alert

- Source System, Destination System, Protocol=UDP where Count exceeds threshold
- Source System, Destination System, Protocol=UDP where Count exceeds threshold
- Source/Destination System, Protocol=TCP where Count exceeds threshold
- Source/Destination System, Protocol=TCP where Count exceeds threshold
- Source/Destination System, Bytes In Total, where Bytes In Total exceeds threshold
- Source/Destination System, Bytes Out Total, where Bytes Out Total exceeds threshold
- Source/Destination System, Bytes In Total, Bytes Out Total, Bytes In/Out Ratio where Bytes In/Out Ratio exceeds threshold

I

28



29

- Source/Destination System, Connection Length where Connection Length exceeds threshold

Log Source Examples

- Netflow Logs
- IPFIX Logs
- SFLOW Logs
- VPC Flow Logs

14. Next-Generation Antivirus Use Cases

Aggregate Count

- Count of Alarms per Source User
- Count of Alarms per Source System

Blacklist Alert

- Any Server Firing Alarms



Log Source Examples

- Netflow Logs
- IPFIX Logs
- SFLOW Logs
- VPC Flow Logs

14. Next-Generation Antivirus Use Cases

Aggregate Count

- Count of Alarms per Source User
- Count of Alarms per Source System

Blacklist Alert

- Any Server Firing Alarms

Rolling Whitelist Alert

- Newly Observed Virus Scan Signature
- Newly Observed Virus Scan Signature per System/User

30

15. Log Clearing Use Cases

- Clearing event logs is a way for adversaries to clear their tracks. With proper event collection, this should occur seldom, making it a relatively easy detection method. Event logs set to "fill" rather than roll or that allow a large enough rolling file size that it causes system administrators to want to clear the logs should be avoided.

Aggregate Count

t 2

Event Viewer



detection method. Event logs set to "fill" rather than roll or that allow a large enough rolling file size that it causes system administrators to want to clear the logs should be avoided.

Aggregate Count

31

Blacklist Alert

- Event log cleared

Rolling Whitelist Alert

- Newly Observed Source User

Threshold Alert

- EventId=1104 where Count exceeds threshold

LogSource Examples

- Windows Security Event ID 1102: The audit log was cleared
- Windows Security Event ID 1104: The security Log is now full

