Exchange Logon

External Password Spraying

Lay of the Land

---

1. Objective (အဓိကရည်ရွယ်ချက်)

- External password spraying technique ၄ မျိုးကို **ခွဲခြားနားလည်ခြင်း**
- OWA - Outlook Web Access
- MAPI - Messaging Application Programming Interface
- EAS - Exchange ActiveSync
- EWS - Exchange Web Services

> 👉 အဓိကရည်ရွယ်ချက်က **Exchange Server ကို ဘယ်သူတွေ ဘယ်လို HTTP request တွေနဲ့ လာရောက်ထိတွေ့ထားလဲ** ဆိုတာကို **IIS web server logs** ကိုအသုံးပြုပြီး နားလည်အောင် စိစစ်သွားခြင်းပါ။ Exchange ကို တိုက်ခိုက်ထားနိုင်တဲ့ attacker ရဲ့ လှုပ်ရှားမှုတွေကို “အစပိုင်းမြေပုံဆွဲကြည့်ခြင်း (Lay of the Land)” လိုပဲ စုစည်းကြည့်နေတယ်လို့ ယူဆလို့ရပါတယ်။

---

2. Data Source Overview

IIS Logs

Exchange Server မှာ web-based service တွေ (OWA, EWS, MAPI, ActiveSync) အားလုံးဟာ **IIS ပေါ်ကနေ HTTP/HTTPS request** တွေကို လက်ခံလုပ်ဆောင်တာဖြစ်လို့ IIS logs ကိုကြည့်ရင် **ဘယ် IP က ဘယ် endpoint ကို ဘယ်အချိန်မှာ လာခေါက်ခဲ့လဲ** ဆိုတာကို တိတိကျကျ သိနိုင်ပါတယ်။ ဒါကြောင့် forensic perspective မှာ IIS logs ဟာ Exchange incident investigation အတွက် အရေးကြီးဆုံး data source တစ်ခုပါ။

- Exchange web services အားလုံး (OWA, MAPI, EAS, EWS) → **IIS ပေါ်က HTTP/HTTPS**
- Physical path

  ```
  %SystemDrive%\inetpub\logs\LogFiles
  ```

- SIEM ထဲမှာ → `event.code:6200`

> ဒီ IIS HTTP transaction တွေဟာ **event.code = 6200** နဲ့ မှတ်တမ်းတင်ထားပါတယ်။ ဒါကြောင့် SIEM (Kibana) မှာ event.code 6200 ကို filter လုပ်လိုက်ရင် **Exchange web traffic အားလုံးနီးပါးကို တစ်နေရာတည်းမှာမြင်နိုင်ပါတယ်**။

- **Exchange forensic အတွက် အရေးကြီးဆုံး log source**

Key Fields (Must-Know)

- `winlog.event_data.c-ip` → **Client IP** ဖြစ်ပြီး ဘယ် external/internal IP က request လာပို့တာလဲဆိုတာကို ပြပါတယ်
- `winlog.event_data.cs-uri-stem` → Endpoint (/owa, /mapi, /EWS, /ActiveSync)
- `winlog.event_data.cs-username` → Authenticated user (anonymous ဖြစ်ရင် empty ဖြစ်နိုင်)

---

3. Four External Exchange Password Spraying Techniques

(1) OWA – Outlook Web Access

OWA (Outlook Web Access) က browser ကနေ email ဝင်ကြည့်ဖို့ သုံးတဲ့ web interface ဖြစ်ပါတယ်။ User တွေ web browser ကနေ mail ဝင်ကြည့်တဲ့အဓိကဝင်ပေါက် ဖြစ်လို့ attacker အများစုက ဒီ endpoint ကို ပထမဆုံးစမ်းတတ်ကြပါတယ်။ ဒါပေမယ့် organization မှာ Two-Factor Authentication (2FA) ထားထားရင် password မှန်တောင် login မဝင်နိုင်တဲ့အတွက် attacker အတွက် အောင်မြင်ဖို့ မလွယ်ပါဘူး။

Purpose

- Browser-based interactive login
- Endpoint

  ```
  /owa/auth/logon.aspx
  ```

Characteristics

- Human-driven login
- MFA enabled environments → attacker success probability နည်း

Failure Detection

သုံးတဲ့ query—

```
agent.hostname:exchange and event.code:4625 and
winlog.event_data.ProcessName:*w3wp.exe
```

ဒီ query ကို ချိတ်ကြည့်ရင် အဓိပ္ပါယ်က
exchange server ပေါ်မှာဖြစ်တဲ့ event
logon failure (4625)
IIS worker process (w3wp.exe) ကနေ ဖြစ်လာတဲ့ authentication failure
ဆိုလိုတာက “local console login မဟုတ်ဘဲ web-based authentication ကနေ login မအောင်မြင်ခဲ့တဲ့ OWA attempt” ကို တိတိကျကျ ဖမ်းတာပါ။

- Security log:
  - `4625` (Logon failed)
  - `ProcessName: w3wp.exe`
  - `LogonType: 8`
  - Kerberos-based (often 4771)

KQL အနေနဲ့ပြောင်းရေးမယ် ဆိုရင်တော့

```
let ts = date("2023-01-13T11:44:40.000Z");
let ds = date("2023-01-13T12:12:12.000Z");
external_table('Winlog')
| where HostHostname=="exchange" and EventCode==4625 and ProcessName
endswith "w3wp.exe" and Timestamp between (ts .. ds)
| project Timestamp, TargetUserName, IpAddress, LogonType, ProcessName
| sort by Timestamp asc
```

Success Flow

- `4768` → `4769` → `4648` → `4624` → `4627` → `6200`

event.code	Description
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested.
4648	A logon was attempted using explicit credentials.
4624	An account was successfully logged on.
4627	Group membership information.
6200	IIS HTTP transaction.

HTTP Behavior

- Success → `200`
- Failure → `200`
  👉 OWA သည် error ကို HTML layer မှာပြ

---

(2) MAPI – Messaging Application Programming Interface

Purpose

MAPI ဆိုတာ Messaging Application Programming Interface ဖြစ်ပြီး

- Exchange Server ကို mail client (အထူးသဖြင့် Microsoft Outlook) ကနေ တိုက်ရိုက် ဆက်သွယ်ဖို့ သုံးတဲ့ protocol ဖြစ်ပါတယ်။
- OWA က browser ကနေ web login ဝင်တာဆိုရင် MAPI ကတော့ application-level access ဖြစ်ပါတယ်။
- Outlook ကို ဖွင့်လိုက်တာနဲ့ inbox, calendar, contacts တွေ အားလုံး auto-load ဖြစ်လာတာဟာ MAPI ကို သုံးလို့ပါ။

Key Differences from OWA

OWA က human interactive login ဖြစ်ပြီး browser-based
MAPI က client automation friendly ဖြစ်ပြီး Outlook / script / tool တွေကနေ ဆက်သွယ်လို့ရပါတယ်။

- `LogonType: 3` (Network)
- NTLM authentication (Kerberos fallback)
- Domain Controller:
  - `4776` (NTLM credential validation)

> Event Code 4625 နောက်တစ်ချက်မှာ 4776 event ကို domain controller ပေါ်မှာ တွေ့ရတက်တယ်။ 4776 ဆိုတာက “ဒီ computer (Exchange) က **user credential ကို NTLM နဲ့ validate လုပ်ဖို့ ကြိုးစားတယ်**” ဆိုတဲ့ event ပါ။ OWA မှာလို `4771 (Kerberos pre-auth fail)` မဟုတ်တော့ဘဲ NTLM validation flow ကို ပြောင်းသွားပြီဆိုတာကို ဒီနေရာမှာ တိတိကျကျ မြင်ရပါတယ်။

Important Forensic Notes

- `6200` event တွင် **username မပါတာ ပုံမှန်**
- **User-Agent** သည် key indicator
  - Outlook version mismatch
  - Tool-based UA (non-human)

> IIS 6200 events တွေကတော့ မရှိမဖြစ်ပါပဲ၊ ဒါပေမယ့် ဒီတစ်ခါမှာ username မပါတော့ပါဘူး။ MAPI authentication flow မှာ IIS က HTTP transaction ကို log လုပ်တဲ့အချိန် user context မ bind ဖြစ်သေးတဲ့အတွက် username field ပျောက်သွားနိုင်ပါတယ်။ ဒါကြောင့် forensic မှာ “6200 မှာ username မပါတာ = benign” လို့ မယူဆရပါဘူး။

ဒီနေရာမှာ အရေးပါတဲ့ field က User-Agent ဖြစ်လာပါတယ်။ Outlook version, OS info တွေ ပါတတ်ပြီး

- GitHub tool name
- abnormal agent string
- environment နဲ့ မကိုက်တဲ့ Outlook version
  တွေ့ရင် quick win indicator ဖြစ်နိုင်ပါတယ်။ Tool-based attacker အများစုက user-agent ကို spoof မလုပ်ဘဲ default ထားတတ်လို့ပါ။

Username မပါတဲ့ 6200 event ကို 4625 နဲ့ ဆက်စပ်ချင်ရင် IP address ကို bridge အဖြစ် သုံး လို့ရပါတယ်။

Correlation Technique

- Bridge field = IP address
  - IIS: `c-ip`
  - Security: `IpAddress`

> ဒီနှစ်ခုကို တူညီတဲ့ IP (100.27.56.5) နဲ့ ချိတ်လိုက်ရင် MAPI authentication attempt တစ်ခုတည်းကနေ ဆက်တိုက်ဖြစ်လာတဲ့ event chain ကို ပြန်တည်ဆောက်နိုင်ပါတယ်။

Successful MAPI Flow

- `4776` → `4624` → `4627` → `4634` → `6200`

EventCode	Description
4776	NTLM credential validation attempt
4624	login success
4627	group membership information (login context build)
4634	logoff
6200	IIS HTTP transaction (ဒီအချိန်မှာ username ပါလာပြီ)

---

(3) EAS – Exchange ActiveSync

Purpose

- mobile device တွေအတွက် email sync လုပ်ဖို့ သုံးတဲ့ protocol ဖြစ်ပြီး Outlook mobile, iOS Mail, Android Mail တွေက သုံးပါတယ်။
- Continuous sync ဖြစ်လို့ low-and-slow traffic ဖြစ်တတ်ပြီး
- brute-force မဟုတ်ဘဲ credential validation အတွက် attacker တွေ သုံးတတ်ပါတယ်။

Endpoint

```
/Microsoft-Server-ActiveSync/default.eas
```

Authentication Flow

- Similar to OWA (Kerberos-based)

> (OWA မှာ သုံးခဲ့တဲ့ workflow) ကိုပဲ ထပ်သုံးလိုက်တဲ့အခါ logon success / failure sequence က OWA နဲ့ နီးပါးတူတယ် ဆိုတာကို တွေ့ရပါတယ်။ အကြောင်းက EAS လည်း Kerberos

> authentication ကို အသုံးပြုပြီး IIS ပေါ်က HTTP endpoint ဖြစ်လို့ပါ။

Failure

- `4771` → `4625` → `6200`
- 4771 – Kerberos pre-authentication fail
- 4625 – logon failure
- 6200 – IIS HTTP transaction

Success

- `4768` → `4769` → `4648` → `4624` → `4627` → `6200`
- 4768 / 4769 – Kerberos ticket request (TGT + service ticket)
- 4648 – explicit credentials အသုံးပြုပြီး logon attempt
- 4624 – login success
- 4627 – group membership context
- 6200 – IIS HTTP transaction

ဒီအဆင့်ထိဆိုရင် OWA နဲ့ ခွဲရခက်ပါတယ်။ ဒါပေမယ့် အဓိကကွာခြားချက်က IIS 6200 event ထဲက HTTP status code ဖြစ်ပါတယ်။

OWA မှာဆိုရင် **login success ဖြစ်ဖြစ် login fail ဖြစ်ဖြစ်**HTTP status 200 (OK) ကို ပြန်ပါတယ်။ OWA က login page ကိုပြပြီး error message ကို HTML ထဲမှာ ပြတာဖြစ်လို့ HTTP layer မှာ success လို့ပဲမြင်ရတာ ပါ။

ဒါပေမယ့် EAS မှာတော့

- success ဖြစ်ရင် client (mobile device) က sync ဆက်လုပ်လို့ရအောင် protocol-specific response ပြန်ပြီး
- failure ဖြစ်ရင် HTTP 401 (Unauthorized) ကို တိတိကျကျ ပြန်ပါတယ်။
  ဒါကြောင့် 6200 event ထဲမှာ sc-status:401 ကို မြင်ရင် EAS credential failure လို့ ခွဲနိုင်ပါတယ်။

Key Differentiator (HTTP Layer)

- Success → protocol-specific response
- Failure → `401 Unauthorized`

👉 `sc-status:401` = **EAS credential failure**

---

(4) EWS – Exchange Web Services

Purpose

- programmatic access အတွက် API ဖြစ်ပြီး scripts, backup tools, admin tools တွေက သုံးပါတယ်။

- attacker တွေအတွက်တော့ mailbox dump, rule creation, persistence လုပ်ဖို့ အကောင်းဆုံး လမ်းကြောင်းပါ။
- **High risk – low noise** (နည်းနည်းနဲ့ အစိတ်ပြင်း)

Endpoint

```
/EWS/Exchange.asmx
```

Critical Facts

- ❌ **No Two-Factor Authentication**
- ❌ Authentication artifacts နည်း
- ✔ Ideal target for password spraying

> ပထမဆုံး သိထားရမယ့် အချက်က EWS (Exchange Web Services) မှာ Two-Factor Authentication ကို မထောက်ပံ့ဘူး ဆိုတာပါ။ အဲဒါကြောင့် credential တစ်ခုရသွားပြီဆိုရင် attacker အတွက် API-level access ကို တိုက်ရိုက်ရနိုင်တဲ့ လမ်းကြောင်း ဖြစ်သွားပါတယ်။ ထို့အပြင် EWS က authentication artifact (log footprint) နည်းပါတယ်။ ဒါကြောင့် forensic လုပ်ရင် အခြား endpoint တွေထက် ပိုပြီး ခက်ခဲပါတယ်။

Why Hard to Detect

- No `4625` on failure
- Exchange server logs alone → blind spot

Required Logs

- Domain Controller: *ဒီနှစ်ခုက EWS authentication attempt ဖြစ်နေတယ်ဆိုတာကို ပြပေးပါတယ်။*
  - `4771` (Kerberos pre-auth fail)
  - `4768` (TGT request)

  > ဒါပေမယ့် အရေးကြီးတဲ့ ပြဿနာတစ်ခုရှိပါတယ်။ ဒီ event တွေက Exchange ကနေ လာတယ်ဆိုတာကို တိုက်ရိုက် မပြဘူး။ Domain Controller perspective ကနေကြည့်ရင် "IP တစ်ခုက user credential စမ်းတယ်" ဆိုတာပဲ မြင်ရပါတယ်။ Exchange involvement ကို အတည်ပြုချင်ရင် IIS logs ကို မဖြစ်မနေ လိုပါတယ်။

- IIS:
  - `6200` with `/EWS/Exchange.asmx`

> ဒီလိုနဲ့ username ကို search လုပ်လိုက်ရင် အခြား event မတွေ့ရပါဘူး။ ဒါကြောင့် source IP ကို key အဖြစ် သုံးပြီး IIS 6200 event ကို လိုက်ရှာရပါတယ်။ /EWS/Exchange.asmx hit ဖြစ်တဲ့ 6200 event နဲ့ DC ပေါ်က 4768/4771 ကို IP + time proximity နဲ့ grouping လုပ်မှသာ "ဒီ credential attempt က Exchange EWS ကို target လုပ်တာ" ဆိုတာကို အတည်ပြုနိုင်ပါတယ်။

Hunting Method

- Grouping by:
  - Source IP
  - Time proximity
- DC events + IIS events **must be correlated**

> EWS abuse ကို hunt / investigate လုပ်ချင်ရင် IIS logs (EWS endpoint) + Domain Controller Security logs ကို မဖြစ်မနေ တွဲသုံးရပါမယ်။ SIEM capacity မလောက်ရင်တော့ /EWS/Exchange.asmx request တွေကိုပဲ filter လုပ်ပြီး သိမ်းထားရပါမယ်။ မဟုတ်ရင် EWS attack တွေကို လုံးဝမမြင်နိုင်ပါဘူး။

ဒီလို event တွေကို အပိုင်းအစလိုက် ခွဲမကြည့်ဘဲ အတူတကွ စုစည်းပြီး အဓိပ္ပါယ်ထုတ်ခြင်းကို **"Grouping"** လို့ ခေါ်ပါတယ်။ Grouping ဆိုတာ threat hunting မှာ log correlation ထက်တောင် အရေးကြီးတဲ့ reasoning technique ဖြစ်ပါတယ်။

IP Rotation

- High unique IP count
- Cloud infrastructure abuse
- Single-IP outlier မပေါ်

---

4. HTTP Status Code Fingerprints (Quick Reference)

Technique	Success	Failure
OWA	200	200
MAPI	500	401
EAS	505	401
EWS	200	401

👉 **OWA မဟုတ်ရင် failure = 401 (almost always)**

---

5. Core Hunting Concepts

Grouping (Most Important Takeaway)

- Log တစ်မျိုးတည်း မကြည့်
- IIS + DC + Exchange Security logs ကို **စုစည်း reasoning**
- Artifact တစ်ခုချင်းစီက puzzle piece

Password Spraying Reality

- IP rotation → detection ခက်
- Visibility > Prevention
- Detection itself = success

---

6. Final Takeaways (Exam / Revision Style)

- IIS logs (6200) = Exchange forensic backbone
- Endpoint + HTTP status = technique fingerprint
- EWS = MFA bypass + minimal artifacts
- DC logs မပါရင် EWS abuse မမြင်နိုင်
- Username မပါတဲ့ 6200 ≠ benign
- Unique IP count spike = spraying indicator