THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Running a RADIUS IP Intercept

OpenLI Training: Chapter Sixteen

Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

Current Status

- Last lesson, we configured a RADIUS IP intercept
  - Target user was `b4CPidYn7u8Vesbo`

- OpenLI will now monitor RADIUS sessions for that user
  - Intercept any traffic for the user's assigned IP
  - Derive IRIs from RADIUS messages

Replaying RADIUS Traffic

- On the collector container, run:

```
tracereplay -X 5 /home/openli-coll/pcaps/radiuswithip.pcap ring:eth2
```

- Pcap contains:
  - RADIUS messages for our target user
  - IP packets sent to and by the target user

Examining HI2 Output

- This time, we're going to start with the HI2 output
  - Again, this output is going to be on the openli-agency container

- Start with the **first** IRI displayed once you replay the pcap
  - After the HI1-Operation record for "RADIUS003"

Examining HI2 Output

```
Mon Oct 11 09:48:56 2021
 Capture: Packet Length: 184/184 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: RADIUS003
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 383980
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 0
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633945736
 ETSILI:       microSeconds: 750751
 ETSILI:     timeStampQualifier: timeOfInterception
```

Examining HI2 Output

```
Mon Oct 11 09:48:56 2021
 Capture: Packet Length: 184/184 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: RADIUS003
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 383980
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 0
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633945736
 ETSILI:       microSeconds: 750751
 ETSILI:     timeStampQualifier: timeOfInterception
```

Examining HI2 Output

```
Mon Oct 11 09:48:56 2021
 Capture: Packet Length: 184/184 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: RADIUS003
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 383980
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 0
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633945736
 ETSILI:       microSeconds: 750751
 ETSILI:     timeStampQualifier: timeOfInterception
```

Examining HI2 Output

- PS Header
  - Nothing we haven't seen before

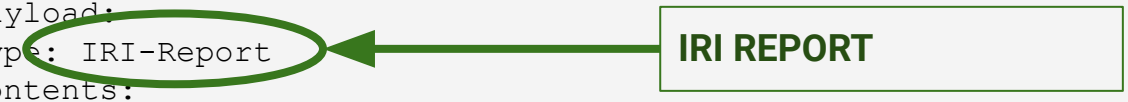
- Moving on to the IRI Payload
  - This is a bit more interesting...

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```



Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```

EVENT TYPE

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```

USERNAME

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```

ACCESS TYPE

Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAttempt
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             pOPPortNumber: 608168733
ETSILI:             pOPIdentifier:
ETSILI:               printableIDType: ktpauEQnsFYzpGei8O
ETSILI:             pOPIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 55.42.134.93
ETSILI:               iP-assignment: Not Known
ETSILI:               iPv4SubnetMask: 255.255.255.255
```

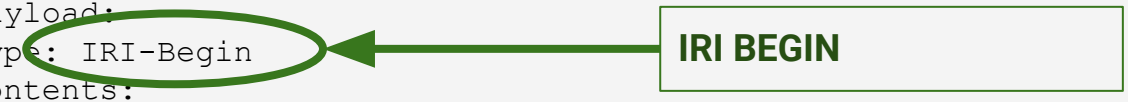
RADIUS NAS

Examining HI2 Output

- Let’s look at the next IRI
  - Sequence Number: 1
  - Ignore the PS Header, skip straight to the IRI payload...

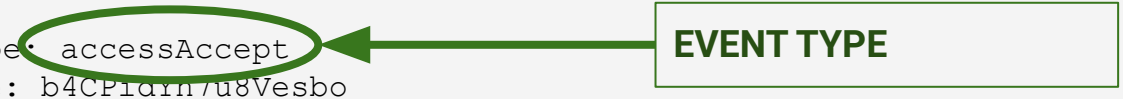
Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Begin
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAccept
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             iPVersion: IPv4
ETSILI:             targetIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 80.180.114.112
ETSILI:               iP-assignment: Dynamic
ETSILI:               iPv4SubnetMask: 255.255.255.255
ETSILI:             startTime: 211011094856.687Z
```



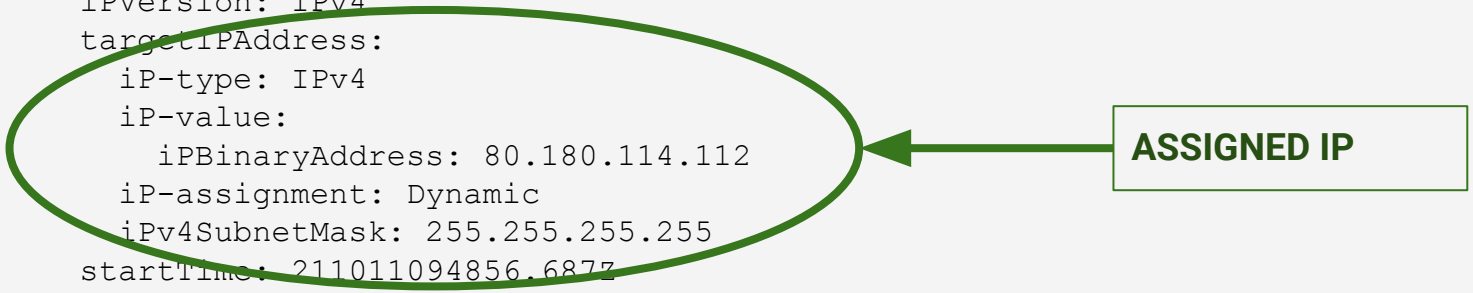
Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Begin
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAccept
ETSILI:             targetUsername: b4CPidrh7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             iPVersion: IPv4
ETSILI:             targetIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 80.180.114.112
ETSILI:               iP-assignment: Dynamic
ETSILI:               iPv4SubnetMask: 255.255.255.255
ETSILI:             startTime: 211011094856.687Z
```



Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Begin
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAccept
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             iPVersion: IPv4
ETSILI:             targetIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 80.180.114.112
ETSILI:               iP-assignment: Dynamic
ETSILI:               iPv4SubnetMask: 255.255.255.255
ETSILI:             startTime: 211011094856.687Z
```



Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Begin
ETSILI:       iRIContents:
ETSILI:         iPIRI:
ETSILI:           iPIRIObjId: .5.3.10.1
ETSILI:           iPIRIContents:
ETSILI:             accessEventType: accessAccept
ETSILI:             targetUsername: b4CPidYn7u8Vesbo
ETSILI:             internetAccessType: xDSL
ETSILI:             iPVersion: IPv4
ETSILI:             targetIPAddress:
ETSILI:               iP-type: IPv4
ETSILI:               iP-value:
ETSILI:                 iPBinaryAddress: 80.180.114.112
ETSILI:               iP-assignment: Dynamic
ETSILI:               iPv4SubnetMask: 255.255.255.255
ETSILI:             startTime: 211011094856.687Z
```

SESSION START TIME

Examining HI2 Output

- IRI Sequence Number 2
  - IRI Type: IRI-Continue
  - Access Event Type: interimUpdate

- Union of the fields from the previous IRIs
  - Assigned IP address
  - NAS information
  - Session start time

Examining HI2 Output

- IRI Sequence Number 3
  - Another interim update

- Two new fields

```
ETSILI:            startTime: 211011094856.687Z
ETSILI:            octetsReceived: 84
ETSILI:            octetsTransmitted: 30
ETSILI:            pOPIdentifier:
ETSILI:              printableIDType: ktpauEQnsFYzpGei8O
```

Examining HI2 Output

- IRI Sequence Number 3
  - Another interim update

- Two new fields

```
ETSILI:            startTime: 211011094856.687Z
ETSILI:            octetsReceived: 84
ETSILI:            octetsTransmitted: 30
ETSILI:            pOPIdentifier:
ETSILI:              printableIDType: ktpauEQnsFYzpGei8O
```

Examining HI2 Output

- IRI Sequence Number 4
  - Session has ended
  - IRI Type: IRI-End
  - Access Event Type: accessEnd

- Two more new fields

```
ETSILI:            startTime: 211011094856.687Z
ETSILI:            endTime: 211011094947.177Z
ETSILI:            endReason: undefined
ETSILI:            octetsReceived: 1298
ETSILI:            octetsTransmitted: 1982
```

Examining HI2 Output

- IRI Sequence Number 4
  - Session has ended
  - IRI Type: IRI-End
  - Access Event Type: accessEnd

- Two more new fields

```
ETSILI:            startTime: 211011094856.687Z
ETSILI:            endTime: 211011094947.177Z
ETSILI:            endReason: undefined
ETSILI:            octetsReceived: 1298
ETSILI:            octetsTransmitted: 1982
```

Examining HI2 Output

- IRI Sequence Number 4
  - Session has ended
  - IRI Type: IRI-End
  - Access Event Type: accessEnd

- Two more new fields

```
ETSILI:            startTime: 211011094856.687Z
ETSILI:            endTime: 211011094947.177Z
ETSILI:            endReason: undefined
ETSILI:            octetsReceived: 1298
ETSILI:            octetsTransmitted: 1982
```

Examining HI2 Output

- Continue to scroll and you will see the session re-establish
  - Nothing new in these IRIs
  - CIN is different, of course
  - Session lasts longer, more interim updates
  - Session does not end -- pcap completes before then

Examining HI3 Output

- What about HI3?
  - PS Header and CC Payload sections are the same as before

- Note the effects of the session re-establishment
  - CIN should change to match the concurrent IRIs
  - Sequence numbering will restart from zero

Examining HI3 Output

```
 ETSILI:   Payload:
 ETSILI:     cCPayloadSequence:
 ETSILI:       CCPayload:
 ETSILI:       payloadDirection: toTarget
 ETSILI:       cCContents:
 ETSILI:         iPCC:
 ETSILI:           iPCCObjId: .5.3.10.2
 ETSILI:           iPCCContents:
 ETSILI:             iPPackets: ...
 IP: Header Len 20 Ver 4 DSCP 00 ECN 0 Total Length 40
 IP: Id 29854 Fragoff 0
 IP: TTL 46 Proto 6 Checksum 61732
 IP: Source 74.125.25.108 Destination 80.180.114.112
 TCP: Source 25 Dest 52228
 TCP: Seq 1966847238
 TCP: Ack 0
 TCP: DOFF 5 Flags: RST Window 0
 TCP: Checksum 37491 Urgent 0
unknown protocol tcp/25
 Unknown Protocol: 25
  00 00 00 00 00 00                                    ......
```

ASSIGNED IP!

Examining HI3 Output

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:       payloadDirection: toTarget
ETSILI:       cCContents:
ETSILI:         iPCC:
ETSILI:           iPCCObjId: .5.3.10.2
ETSILI:           iPCCContents:
ETSILI:             iPPackets: ...
IP: Header Len 20 Ver 4 DSCP 00 ECN 0 Total Length 40
IP: Id 29854 Fragoff 0
IP: TTL 46 Proto 6 Checksum 61732
IP: Source 74.125.25.108 Destination 80.180.114.112
TCP: Source 25 Dest 52228
TCP: Seq 1966847238
TCP: Ack 0
TCP: DOFF 5 Flags: RST Window 0
TCP: Checksum 37491 Urgent 0
```

Next Time

- Integration with vendor-specific traffic mirroring
  - Juniper Jmirror