NIMI Issue Tracking

Tracking Network Device Issues with NIMI

Introduction

The purpose of this document is to detail the requirements for tracking network device issues in NIMI.

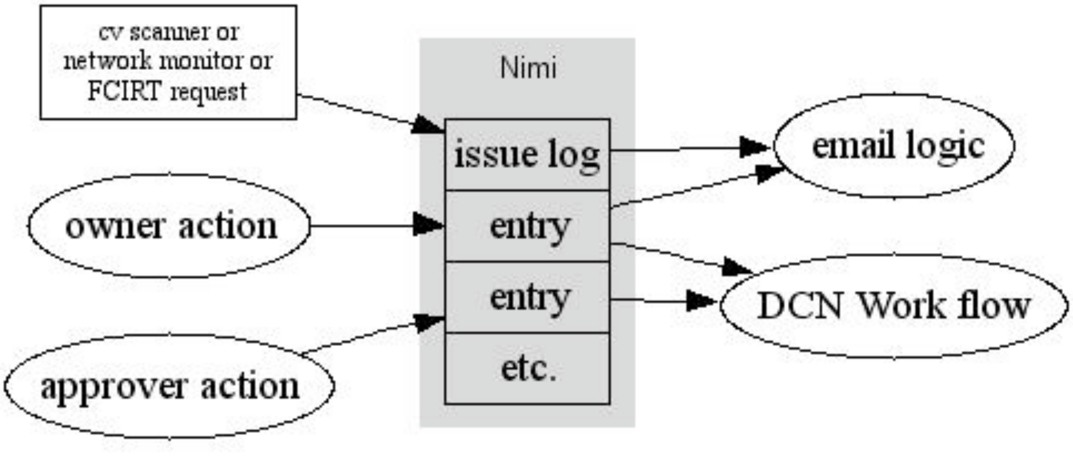
Computer system vulnerabilities are software flaws that can be exploited over a network. Computer systems that have been compromised may try to infect other systems or provide resources to unauthorized users. This document proposes a structure for tracking computer system vulnerabilities and compromises. Computer system vulnerabilities and compromises are called issues in this document. An important part of managing computer issues is notification. Individual system administrators are notified of issues found for the systems they manage. They are informed when network blocks affect their systems. Network block notification is made when network blocks are installed and lifted. The Data Communication group is notified when network blocks are needed, and when existing blocks can be removed.

Notification Requirements

The current notification technology is via email. Email may be replaced by other notification techniques in the future. To emphasize this, this document uses the terms ‘notification’ or ‘email’ where appropriate. The NIMI project is exploring techniques to organize and control workflow. The requirements to block/unblock network devices due to issues will be a driver for the workflow analysis.

Collecting Network Device Issues in NIMI

One feature of NIMI will be to act as a repository for tracking critical network device vulnerabilities. This diagram is a high level view of how NIMI can be used.



High Level NIMI view

The box on the top left of the diagram represents multiple inputs to the NIMI repository. A Nessus-based scanner that runs external to NIMI is named ‘cv scanner’. This scanner runs continuously using Nessus and a set of selected Nessus plugins that detect vulnerabilities. Whenever this scanner finds a network device which tests positive, an issue for this device is prepared and entered into NIMI. NIMI contains logic that uniquely identifies the network device and enters the new issue into a log the this device. NIMI then invokes email logic (which may be either internal or external to NIMI) that will notify the registered owner or administrator of the device that an issue has been found. NIMI will also invoke logic to determine if the network device should be blocked from network access. I a network block is indicated, work flow logic to request a block from Data Communication and Networking group is used.

Other inputs to the NIMI issue repository are network monitors such as AutoBlocker. The AutoBlocker monitors outgoing network traffic looking for internal hosts that exhibit scanning activity. This detection is automatic and the AutoBlocker can block the suspicious device from the network. An issues entry into NIMI will allow this activity to be tracked. Finally, the FCIRT (Fermilab Critical Incident Response Team) can request that a network device that is under investigation be entered into the NIMI repository for tracking.

The network device's registered administrator or owner will receive in the email notification, a URL that will access NIMI to display a web page with the details of the issue found. Any history of previous issues will also be available. The registered administrator or owner can use this web page to request the following actions:

I. The issue is a false positive, meaning the network device is not vulnerable to the exploit.
II. The issue is real, but this network device should be exempt from network blocks for the reason entered.
III. The issue has been fixed using one of the listed remediations.

The 'owner action' using the NIMI web interface will cause subsequent notification or actions. The action may require approval. If approval is required, the 'approver action' may trigger the subsequent notifications. If the network device has been blocked from network access, work flow logic is invoked to request a unblock action from DCN.

Finally, reports and statistics can be generated using the NIMI repository.

NIMI Email Notification Requirements

When a vulnerability scanner or some other detection technique (e.g. network monitoring) finds a network device with an issue, the need is to remove the issue either by applying a software patch to the network device or, if the issue found is serious, removing the network device from the network until it is serviced. The first step is to determine the registered administrator or owner and send email notification. Other steps might require requesting that the device be blocked from the network. If a network block is requested and the device is subsequently repaired, then a network unblock request is needed. The network block/unblock requests can be done via email if no other work flow technique is available. The discussion below assumes that all notification will be done via email.

NIMI Email Logic Pseudo Code

The following definitions are used in the pseudo code.

Issue Block Type	Description
`Immediate`	Request network block immediately when issue is entered in NIMI.
`Regular`	Request network block after 'block delay' hours have expired.
`None`	Do not request a network block for this issue.

Issues entered into the NIMI repository must have an issues code defined in NIMI. Each issue code is assigned a severity, block delay value and FCIRT flag when the issue code is created. The following talbe shows how the block type is selected based on the issue's severity, block delay value and FCIRT flag.

Issue Block Type	Issue Severity	Issue Block Delay value	FCIRT flag
`Immediate`	Critical – 'C'	=0	Don't care
`Immediate`	Critical – 'C'	Don't care	'Y'
`Regular`	Not Critical	>0	'N'
`None`	Not Critical	=0	'N'

The following terms are used in the pseudo code below:

`issue`	The vulnerability or compromise (issue code) found for a system

`system`	The MISCOMP system ID
`administrator`	The system’s registered primary administrator or owner.
`restricted`	A DCN block is (or has been) requested for system.
`blkdelay`	The value of this issue’s ‘block delay’ in hours.
`email_date`	date email notification sent to administrator – User Notified
`email_DCN`	date system block requested from DCN

The following pseudo code describes the email notification required for each function.

Add_issue():

This function is used to add an issue to the NIMI repository.

```
For each issue:
      find system and administrator
      if issue is block_none
            format email type I.
      if issue is block_regular
            format email type II
            set system restricted=’Y’
      if issue is block_immediate
            format email type III - blocked
            format email type V
            set system restricted=’Y’
      set email_date = now
```

DCN_daily():

This function is used to notify DCN of block/unblock requests. It is anticipated that this function will be run periodically (e.g. once per day).

```
Sweep NIMI repository for restricted=’Y’ systems,
For each system:
      find administrator for system,
      For each issue:
            if issue is remediated
                  format email type IV – unblocked
                  format email type III - unblocked
                  set restricted=’N’
            else if issue is block_regular AND
               (email_date + bldelay) > now AND
                email_DCN is NULL
                  format email type IV – blocked
                  format email type III – blocked
                  set email_DCN = now
```

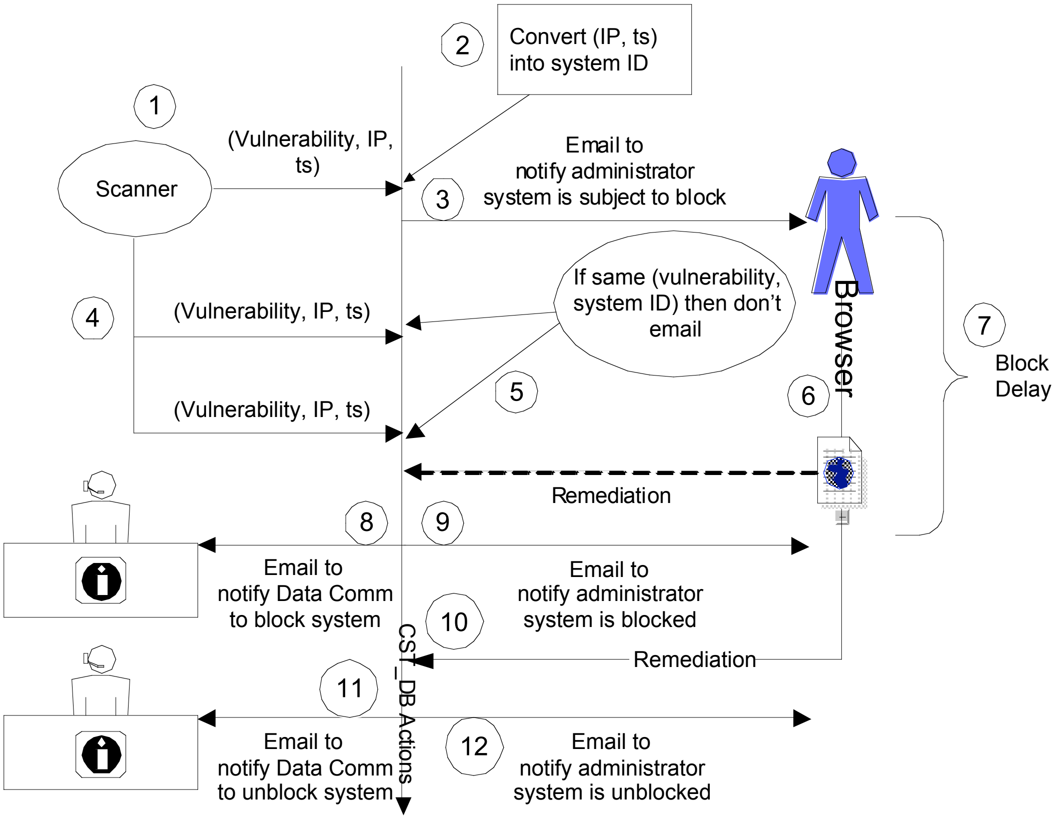
NIMI Email Logic Time Line Description

The email logic is diagramed in the figure below. The line in the center of the figure is a time line with increasing time moving down the line. The events numbered in circles are described here:

1. The vulnerability scanner or AutoBlocker source is running continuously. FCIRT can enter systems with critical vulnerabilities or compromises at any time. When a vulnerable system is found, the source uses `add_issue()` to add the issue to the NIMI repository.

2. The NIMI logic converts the system's IP address, DNS name and timestamp into a MISCOMP system ID. The NIMI logic uses the internal DHCP_leases table and the MISCOMP database to make this conversion. The system ID is important as it uniquely identifies the target system. The unique system ID combined with the specific issue are used together by the email logic to track what emails have been sent.
3. Shortly after `add_issue()` is called, the email logic determines what email (if any) is needed. The format of this email depends on the issue's block type value as follows:
   a. If any issue in the list of issues for this system is `'block_immediate'` an email is formatted using III - blocked. In addition, the network block is requested from DCN using an email formatted as V.
   b. If any issues in the list of issues for this system are `'block_regular'`, an email is formatted using II below.
   c. If all issues in the list of issues for this system are `'block_none'`, an email is formatted using I below.

   The email formatted for a system administrator gathers all affected systems into one email per email format. This is done to minimize the number of emails a system administrator will receive.
4. As the vulnerability scanner continues to run, it may find the same issue for the same system. The scanner will use `add_issue()` to add the issue to the NIMI repository.



2
Convert (IP, ts) into system ID
1
Scanner
(Vulnerability, IP, ts)
3
Email to notify administrator system is subject to block
Browser
4
(Vulnerability, IP, ts)
If same (vulnerability, system ID) then don't email
(Vulnerability, IP, ts)
5
6
7
Block Delay
Remediation
8
9
Email to notify Data Comm to block system
Email to notify administrator system is blocked
10
Remediation
11
CST_DB Actions
12
Email to notify Data Comm to unblock system
Email to notify administrator system is unblocked

Figure 1

5. As before, the NIMI logic converts the system's IP address, DNS name and timestamp into a MISCOMP system ID and notices that the issue has already been found for this system. The '`last found`' date is changed and the '`issue_count`' is updated by generating log entries, but no new email is generated.

6. The system administrator can use the customized link in the notification email to enter a remediation into the NIMI web interface. Once the system administrator has used the link to enter a remediation, the NIMI logic is reset for this combination of system ID and issue. If the remediation is entered before the `bldelay` time, no block is requested from Data Communications. This means that steps 8 and 9 and beyond do not occur.
7. If the system's administrator does not use the customized link to enter a remediation before the issue's `bldelay` time (number of hours), the NIMI logic will cause a block request email to be prepared for systems that have '`block_regular`' issues.
8. The next time `DCN_daily()` is called, an email is formatted and sent to Data Communications notifying of the critical issue in the block list using format IV.
9. At the same time, an email is formatted and sent to the system's system administrator notifying that the system is now blocked from network access due to a critical issue. The format of this email is III below.
10. When the system administrator uses the customized link in the email to enter a remediation code, the NIMI logic is prepared to unblock the system. The format of this email is in Email Formats item IV.
11. The next time `DCN_daily()` is called, an email is formatted and sent to Data Communications notifying that this system in the unblock list using format IV.
12. At the same time, an email is formatted and sent to the system administrator notifying that the system is now unblocked and network access is restored. The format of this email is in Email Formats item III – unblock.

Instances of the issue found by the scanner after the Data Communication block has been requested simply update the '`last found`' date. The current value of the '`last found`' date is always available on the web page when using the customized link for this system. Once the system's system administrator has used the link to enter a remediation or an issue, the NIMI logic is reset for this combination or system ID and issue.

Email Formats:

Here are the email formats for the five types of email generated by the NIMI. In the email headers, the '`GCSC-xxx`' means the GCSC email list for the division/section/experiment named '`xxx`'. GCSC email lists exist for the following:

GCSC-BD	Accelerator Division GCSC and deputies mailing list
GCSC-BSS	BSS GCSC and deputies mailing list
GCSC-CD	Computing Division GCSC and deputies mailing list
GCSC-CDF	CDF GCSC and deputies mailing list
GCSC-D0	D0 GCSC and deputies mailing list
GCSC-DIR	Directorate GCSC and deputies mailing list
GCSC-ESH	ES&H GCSC and deputies mailing list
GCSC-FESS	FESS GCSC and deputies mailing list
GCSC-LSS	Lab Services GCSC and deputies mailing list
GCSC-PPD	Particle Physics Division GCSC and deputies mailing list
GCSC-SOUDAN	SA Compliance Screen scanner results
GCSC-TD	Technical Division GCSC and deputies mailing list

I. Non-critical Vulnerability:

Email Headers:

Subject: `Latest List of Machines with Vulnerabilities`

To: <system administrator> if known, else To: computer_security?

From: cst@fnal.gov

Cc:

Body:

```
Dear <First Name> <Last Name>


The system(s) listed below are registered to you as a sysadmin and test
positive for one or more vulnerabilities.


IP Address    MAC Address        Node Name  Last Found

A.B.C.D       XX-XX-XX-XX-XX-XX  name       MM/DD/YY HH:MM

Issue: <sname from issue_codes table>


Please visit:

<URL to NIMI web interface for this administrator>
to view more details about the vulnerabilities found and to enter
the remediation taken.

Matt Crawford

Fermilab Computer Security Coordinator
```

II. Critical Vulnerabilities

Email Headers:

Subject: Latest List of Machines with Critical Vulnerabilities

To: <system administrator> if known, else To: computer_security?

From: cst@fnal.gov

Cc: computer_security@fnal.gov, GCSC-xxx@fnal.gov

Body:

```
Dear <First Name> <Last Name>


The system(s) listed below are registered to you as a sysadmin and test
positive for one or more of the currently declared critical
vulnerabilities.  Please patch these systems immediately. If you cannot
patch the system or believe this test to be in error, contact your GCSC
or nightwatch@fnal.gov.


NOTE: These systems are now subject to being blocked from the network.


IP Address    MAC Address        Node Name  Last Found

A.B.C.D       XX-XX-XX-XX-XX-XX  name       MM/DD/YY HH:MM

Issue: <sname from issue_codes table>
```

Please visit:

<URL to NIMI web interface for this administrator>
to view more details about the vulnerabilities found and to enter
the remediation taken.

Matt Crawford

Fermilab Computer Security Coordinator

III. Critical Vulnerabilities – DCN Block/Unblock Requested

Email Headers:

Subject:
<if blocking>
List of Machines with Vulnerabilities - Network Block Requested
<else unblocking>
List of Machines with Vulnerabilities - Network UnBlock Requested
<endif>

From: cst@fnal.gov

Cc: computer_security@fnal.gov

Body:

Dear <First Name> <Last Name>

<if blocking>

The system(s) listed below are registered to you as a sysadmin and test positive for one or more of the currently declared critical vulnerabilities. Please patch these systems immediately. If you cannot patch the system or believe this test to be in error, contact your GCSC or nightwatch@fnal.gov.

NOTE: These systems are now blocked from the network.

<else unblocking>

The system listed below are registered to you are now unblocked.

<endif>

IP Address	MAC Address	Node Name	Last Found
A.B.C.D	XX-XX-XX-XX-XX-XX	name	MM/DD/YY HH:MM

Issue: <sname from issue_codes table>

<if blocking>

Please visit:

<URL to NIMI web interface for this administrator>
to view more details about the vulnerabilities found and to enter
the remediation taken.

```
<endif>

Matt Crawford

Fermilab Computer Security Coordinator
```

IV. DCN – Block/Unblock list

Email Headers:

Subject: Requested Network Block/Unblock

NOTE: Current implementation uses the Subject: Network Restrictions

To: netadmin@fnal.gov

From: cst@fnal.gov

Cc: computer_security@fnal.gov, helpdesk@fnal.gov

Body:

```
BLOCK Static IP (system in MISCOMP):

IP Address     MAC Address         Node Name   Last Found   User Notified

A.B.C.D        XX-XX-XX-XX-XX-XX   name        MM/DD HH:MM MM/DD HH:MM

Issue: <sname from issue_codes table>



BLOCK DHCP (system not in MISCOMP):

IP Address     MAC Address         Node Name   Last Found   User Notified

A.B.C.D        XX-XX-XX-XX-XX-XX   name        MM/DD HH:MM MM/DD HH:MM

Issue: <sname from issue_codes table>



UNBLOCK Static IP

IP Address     MAC Address         Node Name   Last Found   User Notified

A.B.C.D        XX-XX-XX-XX-XX-XX   name        MM/DD HH:MM MM/DD HH:MM

Issue: <sname from issue_codes table>


UNBLOCK DHCP

IP Address     MAC Address         Node Name   Last Found   User Notified

A.B.C.D        XX-XX-XX-XX-XX-XX   name        MM/DD HH:MM MM/DD HH:MM

Issue: <sname from issue_codes table>
```

V. DCN – URGENT Block list

Email Headers:

Subject: Urgent Network Block

To: netadmin@fnal.gov

From: cst@fnal.gov

Cc: computer_security@fnal.gov, helpdesk@fnal.gov

Body:

```
BLOCK Static IP (system in MISCOMP):
IP Address    MAC Address        Node Name  Last Found  User Notified
A.B.C.D       XX-XX-XX-XX-XX-XX  name       MM/DD HH:MM MM/DD HH:MM
Issue: <sname from issue_codes table>



BLOCK DHCP (system not in MISCOMP):
IP Address    MAC Address        Node Name  Last Found  User Notified
A.B.C.D       XX-XX-XX-XX-XX-XX  name       MM/DD HH:MM MM/DD HH:MM
Issue: <sname from issue_codes table>
```

SOAP Services

The following SOAP services are hosted by NIMI to implement the issue tracking functionality:

```
add_issue_code(
        icode integer,                 issue code from Nessus scanner,
        sname varchar2,                short name for vulnerability,
        lname varchar2,                long name for vulnerability,
        descr varchar2,                vulnerability description,
        scode varchar2,                source code,
        acode varchar2,                action code,
        cve varchar2,                  vulnerability CVE number,
        bugtraq varchar2,              vulnerability BugTraq number,
        severity varchar2,             severity code,
        fcirt varchar2,                FCIRT flag,
        bldelay integer default 24)    block delay
```

The add_issue_code() service prepares the NIMI repository to receive issues. Each issue has an 'icode' that either the Nessus scanner assigns or is assigned manually for example with FCIRT issues. The 'sname' and 'lname' are used for easy identification of the issue. The 'descr' contains text that provides more information about the issue. In the case of FCIRT initiatiated issues, the 'descr' can be updated to contain a history log. The 'scode' indicates the source detector that will find the issue. Source codes are maintained using the add_source_code() service. Examples of source codes are 'O' for Outbound Autoblocker and 'V' for Vulnerability Scanner. The 'acode' is the action required to remediate the issue. Action codes are maintained using the add_action_code() service. Examples of actions codes are 'PS' for Patch and Scan. The 'cvs' and 'bugtraq' numbers refer to services that keep track of software vulnerabilities. Not all issues will have values for these fields. The 'severity' indicates the email actions that the NIMI email logic will take with respect to this issue. Severity codes are maintained using the add_severity_code() service. Examples of severity codes are 'C' for critical, 'V' for vulnerable, 'I' for informational and 'W' for warning. The 'fcirt' flag is 'Y' if this issue requires FCIRT approval for remediation. Finally, the 'bldelay' is the number of hours to delay between notifying the user or administrator that a critical issue exists and requesting a network block of the system by the Data Communications Group (DCN).

```
add_issue(
        ip varchar2,                   IP address of system with vulnerability,
        icode varchar2,                  issue code from Nessus scanner,
        ts varchar2 default null,        time of scan,
        msgtxt varchar2 default null,    additional text message from scan,
        email_data_comm varchar2 default 'Y')  invoke DCN email logic
```

The `add_issue()` service enters an issue into the NIMI repository. A network monitor device such as the OutBound Autoblocker or a vulnerability scanner will use this function when a vulnerability or compromise is found. The 'ip' is the IP address of the affected system. The 'icode' is the number assigned to the issue found. The 'ts' is the time stamp when the issue was found. The 'msgtxt' is additional information about the issue. Finally, the 'email_data_comm' is a flag that will either invoke the DCN email logic if 'Y' or suppress the logic if 'N'.

```
email_immediate(
        email_addr varchar2)             used for debugging, email To: address
```

The `email_immediate()` service is used to invoke the NIMI email logic for debugging. This function sweeps through NIMI looking for combinations of systems and issues for which the responsible system administrator has not been notified. This function also uses the DCN notification logic by looking for systems with `block_immediate` issues. `Block_immediate` issues trigger an email with the subject 'Urgent Network Restrictions'. When the '`email_addr`' parameter is non-null, the email address specified is used for the To: header for all email generated. The '`email_addr`' parameter facilities debugging the email without disturbing any real administrators.

```
DCN_daily(
        email_addr varchar2 default null)        used for debugging, To: address
```

The `DCN_daily()` service is used to invoke the NIMI email logic to request network block/unblock actions from DCN and to notify system administrators of network blocks and unblocks.. This function sweeps through NIMI looking for combinations of systems with type '`block_regular`' for which a network block or unblock action should be requested from DCN. For '`block_regular`' systems this function requires that the 'bldelay' non-zero value hours has elapsed since notifying the system administrator that the issue exists before requesting a block action by DCN. Unblock actions do not use the 'bldelay' and occur after a system with an active network block has had all issues remediated.