

Mapping Targets - Instructions for n-ORM Monitoring System

Contents

1 Introduction	
2 File Format	
3 Updating the file	
3.1 Automatic Updating	
3.2 Determining the Target	2
3.3 Determining the Category	2
3.4 Editing Clashes	2

1 Introduction

This document describes the use of the mappings file in the system. An example is given in figure 1. The mappings file is used to map between the snort classification of a threat and the requirements for the nORM XML file.

2 File Format

The file is a simple CSV file with one line per threat. Each line has five values:

SID - The unique identification number assigned to this threat by the external IDS/IPS system

Alert - This is the name of the threat also provided by the external IDS/IPS system, but can be changed by the Administrator.

Target - The Target as needed by nORM's Threat tag and is provided manually by the administrator. The default value is "Unknown".

Category - Is the Category field as required by nORM's Threat tag, again provided by the administrator. The default value is "Indiscriminate".

Severity - Is the SeverityScore field as required by nORM's Threat tag. The default value automatically calculated from the the external IDS/IPS system priority value.

The mapping from the external IDS/IPS system to nORM is:

1 → 10; 2 → 7; 3 →! 4; 4 → 1.

3 Updating the file

3.1 Automatic Updating

When the system detects a new threat that is not already in the mappings file,

a new line is automatically added with the default values specified above. The intention is the System Administrator will periodically check for missing values and fill these in. This should be defined as part of the System Administrator's workow.

3.2 Determining the Target

In order to determine the Target of a threat a manual examination of the the external IDS/IPS system rules in use must be undertaken. It is therefore important to start with a set of well-documented rules.

Such sets are available from <http://www.snort.org/vrt/> e.g. Source_re VRT certi_ed rules.

This document will use the "Rules for Snort v2.4" as exemplars. The file of rules is called snortrules-pr-2.4.tar.gz.

When unpacked this contains two directories; rules and doc. The doc directory contains a further directory-signatures. In here is a file corresponding to each SID. The doc file 2924.txt is shown in figure 2. In this case the relevant section is "Affected Systems", although the "Summary" section will give sufficient information in most cases. As in this case "All systems sharing resources using SMB" are affected, then a value of SMB. Exact values need be agreed between the capture system and n-ORM.

3.3 Determining the Category

Most threats will be indiscriminate. The difference is that a discriminate (directed) attack will at some point be directed by a Human targeting a specific machine, rather than a self-propagating virus or worm. It is difficult to determine this simply from the threat ID.

3.4 Editing Clashes

By default, the mappings file is only consulted and updated by the system once per week at midnight on Monday morning. Any updates will be completed in fractions of a second. However, a System Administrator should not edit the file at this time, or more significantly leave an editing session open over this time.

```
# SID,Alert,Target,Category,Severity
2050,MS-SQL version overflow attempt,SQLServer,Indiscriminate,1
2003,MS-SQL Worm propagation attempt,Unknown,Indiscriminate,7
2466,NETBIOS SMB-DS IPC$ unicode share access,Unknown,Indiscriminate,4
2924,NETBIOS SMB-DS repeated logon failure,Unknown,Indiscriminate,10
2404,NETBIOS SMB-DS Session Setup AndX request unicode username overflow
attempt
,Unknown,Indiscriminate,10
1113,WEB-MISC http directory traversal,Unknown,Indiscriminate,7
2570,WEB-MISC Invalid HTTP Version String,Unknown,Indiscriminate,7
1852,WEB-MISC robots.txt access,Unknown,Indiscriminate,7
```

```
1002,WEB-IIS cmd.exe access,Unknown,Indiscriminate,10
1408,DOS MSDTC attempt,Unknown,Indiscriminate,7
472,ICMP redirect host,Unknown,Indiscriminate,7
1918,SCAN SolarWinds IP scan attempt,Unknown,Indiscriminate,4
2417,FTP format string attempt,Unknown,Indiscriminate,4
579,RPC portmap mountd request UDP,Unknown,Indiscriminate,7
```

Figure 1: Example mappings file

```
Rule:
--
Sid:
2924
--
Summary:
This event is generated when repeated failed attempts are made to access
an SMB share.
--
Impact:
Unknown. Possible information disclosure and loss of data.
--
Detailed Information:
This event indicates that multiple failed attempts have been made to
access an SMB network share. This may indicate a determined effort by an
unauthorized user to access information and data on a network share.
--
Affected Systems:
All systems sharing resources using SMB
--
Attack Scenarios:
An attacker can make repeated attempts to access network shares in an
attempt to gain information.
--
Ease of Attack:
Simple. No exploit software required.
--
False Positives:
None known
--
False Negatives:
None known
--
Corrective Action:
Apply strict access control to all networked resources.
--
```

Figure 2: SNORT documentation for rule 2924 from snort rules for SNORT 2.4