
TESTBED NetWare

SekChek for Netware Security Report

System: [Root].SEKNETWARE65

8 December 2011

Contents

| | |
|--|----|
| SekChek Options | 3 |
| System Details | 4 |
| 1 . Report Summaries | 5 |
| 1.1 Comparisons Against Industry Average and Best Practice | 6 |
| 1.2 Summary of Changes since the Previous Analysis | 10 |
| 2 . Directory Tree Structure | 11 |
| 3 . Intruder Detection Values | 12 |
| 4 . Alias Names | 14 |
| 5 . User Accounts | 15 |
| 6 . Objects with Supervisory Rights | 17 |
| 7 . Security Equivalences | 19 |
| 8 . Groups and Roles | 21 |
| 9 . Redundant Groups | 22 |
| 10 . Users Not Allowed to Change Their Passwords | 23 |
| 11 . Minimum Password Lengths Less than 6 | 24 |
| 12 . Password Change Intervals Greater than 30 Days | 26 |
| 13 . Users Not Requiring a Unique Password | 28 |
| 14 . Expired Passwords | 30 |
| 15 . Grace Logins | 31 |
| 16 . Disabled Accounts | 32 |
| 17 . Accounts with Expiry Dates | 33 |
| 18 . Invalid Logon Attempts Greater than 3 | 34 |
| 19 . Accounts Allowed Simultaneous Device Sessions | 35 |
| 20 . Last Logons, 30 Days and Older | 37 |
| 21 . Servers | 39 |
| 22 . Computers | 40 |
| 23 . Volumes | 41 |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| SekChek Options | |
|---|---------------------|
| Reference Number | 1009090004 |
| Requester | Richard Burns |
| Telephone Number | +44 (881) 846 8971 |
| City | London |
| Client Country | UK |
| Charge Code | SekChek100903 |
| Client Code | SEK001 |
| Client Industry Type | Communications |
| Host Country | UK |
| Security Standards Template | 0 - SekChek Default |
| Evaluate Against Industry Type | Communications |
| Compare Against Previous Analysis | Not Selected |
| Report Format | Word 2007 |
| Paper Size | A4 (21 x 29.7 cms) |
| Spelling | English UK |
| Large Report Format | MS-Access database |
| Large Report (Max Lines in Word Tables) | 10000 |
| Summary Document Requested | Yes |
| Scan Software Version Used | Version 5.0.4 |
| Scan Software Release Date | 14-May-2010 |

Your *SekChek* report was produced using the above options and parameters.

You can change these settings for all files you send to us for processing via the *Options* menu in the *SekChek* Client software on your PC. You can also tailor them (i.e. temporarily override your default options) for a specific file via the *Enter Client Details* screen. This screen is displayed:

- For *SekChek* for NT and NetWare - during the Extract process on the target Host system;
- For *SekChek* for AS/400 and UNIX - during the file encryption process in the *SekChek* Client software.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| System Details | |
|----------------|-------------------------|
| Tree | SEKNETWARE65 |
| Context | [Root] |
| Scan Time | 03-Sep-2010 19:27 |
| Scanned By | CN=admin.O=ServerNetw65 |

Report Date: 8 December, 2011

Declaration.

The provided observations and recommendations are in response to a benchmarking analysis that compares the user's information security features against industry. The recommendations are organized to identify possible implications to the company based on the gathered information, to identify a leading practices risk rating of the implications and provide possible recommended actions. The benchmarking analysis and the related observations and recommendations should supplement management's analysis but should not be and cannot be solely relied upon in any instance to identify and/or remediate information security deficiencies. Further, the observations and recommendations herein do not identify the cause of a possible deficiency or the cause of any previously unidentified deficiencies. The causes of the deficiencies must be determined by management for the recommendations selected to be relevant.

© 1996-2011 SekChek IPS. All rights reserved.

SekChek is a registered trademark of SekChek IPS. All other trademarks are the property of their respective owners.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

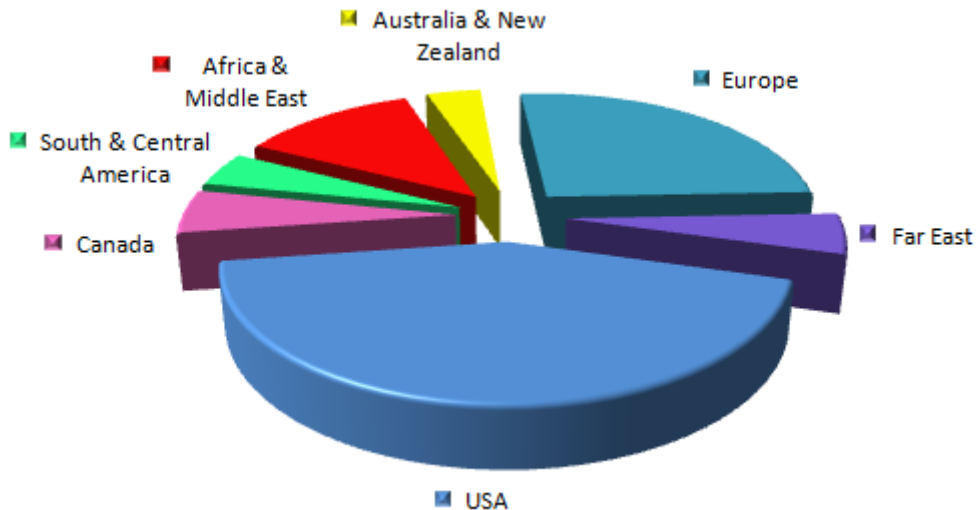
CONFIDENTIAL

1 . Report Summaries

The following two charts illustrate the diversity of regions and industries that make up the population of *Netware systems* in our statistics database. The remaining graphs in the *Report Summary* section evaluate security on your system against this broad base of real-life security averages.

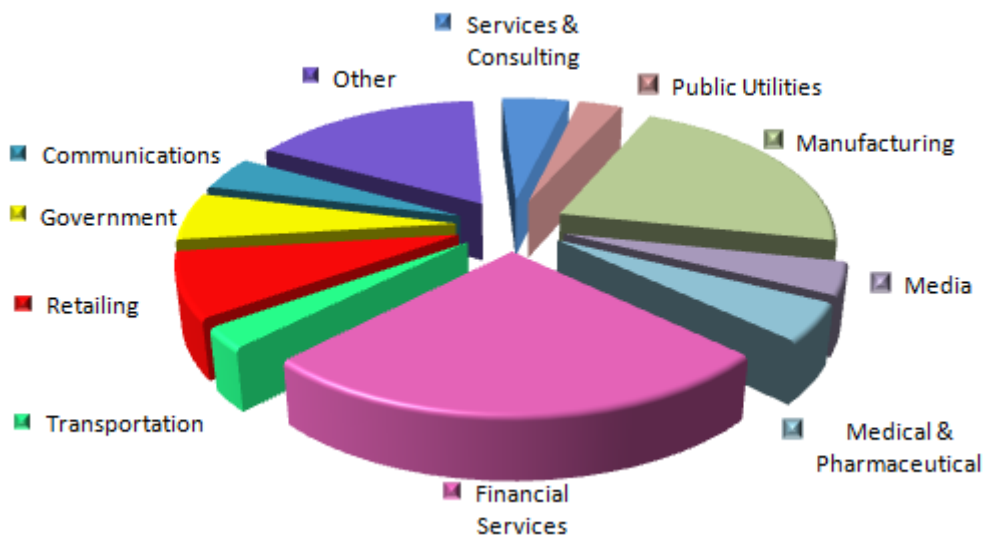
SekChek is used by the Big Four audit firms, IS professionals, internal auditors, security consultants & general management in more than 120 countries.

Statistics Population by Region



As new reviews are processed, summaries of the results (excluding client identification) are automatically added to a unique statistics database containing more than 60,000 assessments.

Statistics Population by Industry Type



Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

1.1 Comparisons Against Industry Average and Best Practice

Summary of Intruder Detection Values

This graph compares against the industry average using the following criteria:
Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = <All>
Your Intruder Detection settings are rated on a scale of 0 to 100, where '0' represents *Least Secure*, '50' represents *Industry Average* and '100' represents *Best Practice*.

This, and the following [summary report](#), are of most value when they are used to compare 'snapshots' of your security measures at different points in time. Used in this way they provide a fairly clear picture of whether your security measures are improving or becoming weaker.

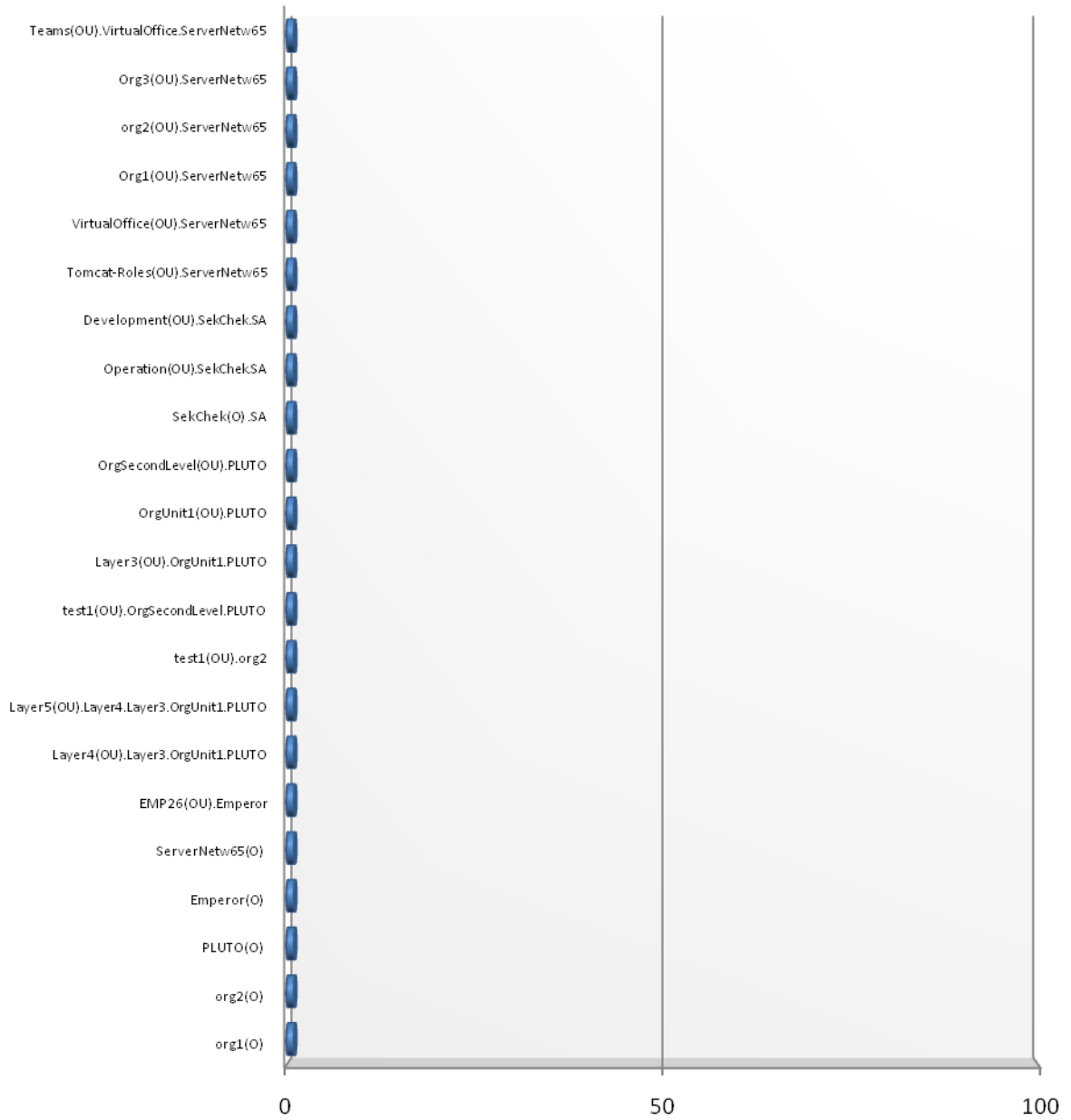
Industry Average (50) is a dynamic, calculated average for *all* NetWare systems processed by *SekChek* for NetWare. It indicates how your security measures compare with those of other organisations using NetWare systems.

Best Practice (100) represents the generally accepted international standard for Intruder Detection values; the standard to strive for.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL



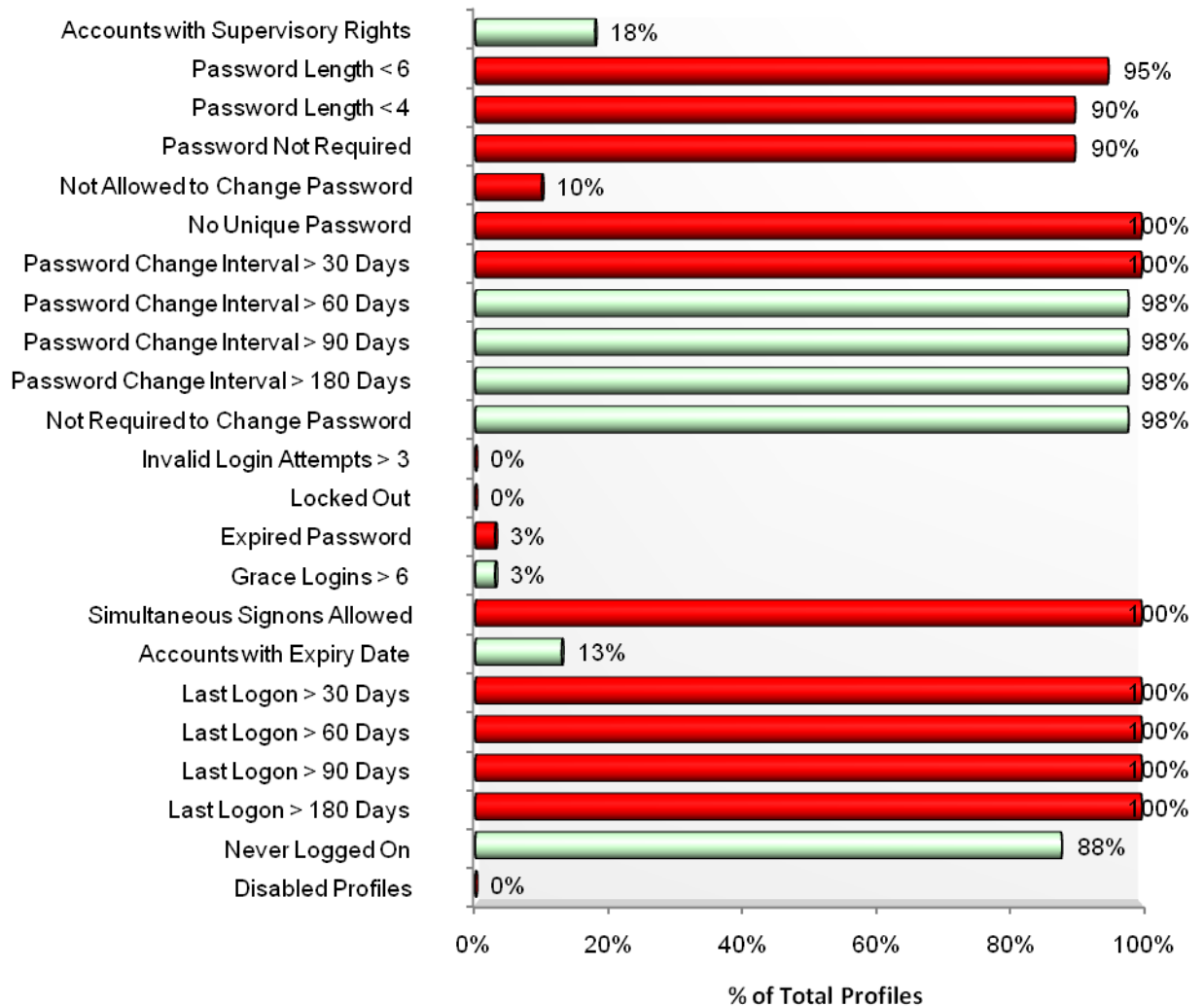
Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Comparisons Against Industry Average and Best Practice (continued)

Summary of User Accounts



This graph compares against the industry average using the following criteria:
Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small
■ Better than the industry average; ■ Worse than the industry average

Total number of user accounts defined to your system: 40.

This summary report presents the number of user accounts, with the listed characteristics, as a percentage of the total number of user accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant section in the [main body](#) of the report.

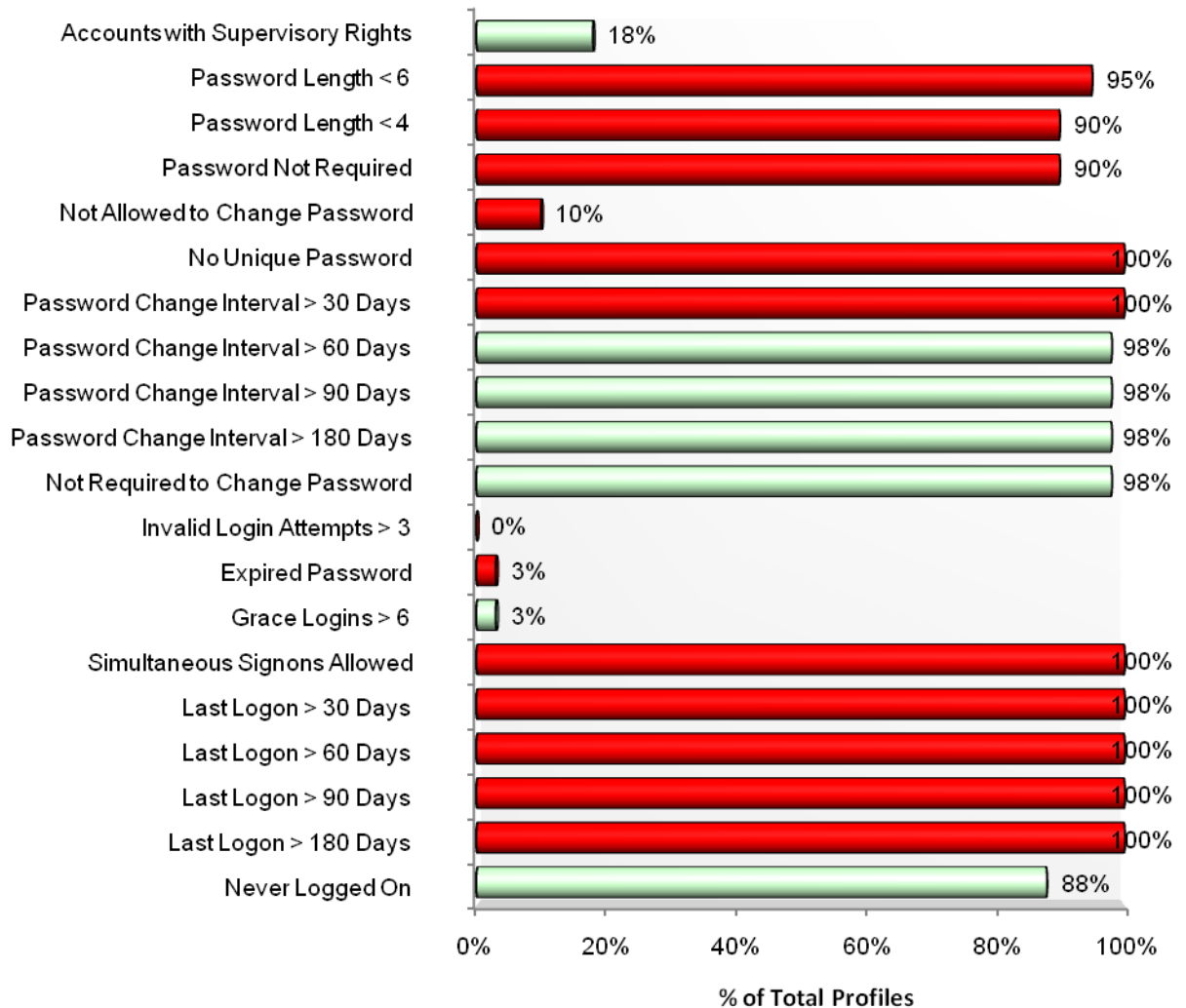
Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Comparisons Against Industry Average and Best Practice (continued)

Summary of User Accounts (excluding disabled accounts)



This graph compares against the industry average using the following criteria:
Country = <All>; Industry Type = Communications; Machine Size (Nbr of Accounts) = Very Small
■ Better than the industry average; ■ Worse than the industry average

Total number of user accounts defined to your system: 40.

This summary report presents the number of *enabled* accounts (i.e. excluding those with a status of disabled, accounts that are locked, and accounts that have expired), with the listed characteristics, as a percentage of the total number of user accounts defined to your system. In general, longer bars highlight potential weaknesses in your security measures and should be investigated. For more details, refer to the relevant section in the [main body](#) of the report.

Security Analysis: TESTBED NetWare

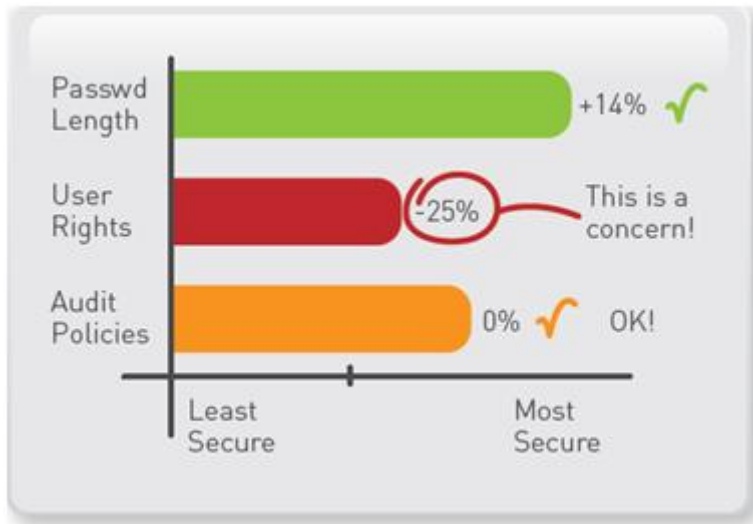
System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

1.2 Summary of Changes since the Previous Analysis

Need to quickly highlight changes in security controls since your previous review?

SekChek's latest time-comparison graphs are just the solution!



Note: The above graph is provided for illustrative purposes only.

A collection of easy-to-read reports in a very familiar format provides you with visual indicators of:

- Whether security has improved, weakened, or remained about the same since your previous analysis
- The effectiveness of your measures to strengthen controls
- Whether risk is increasing or decreasing
- The degree of change, both positive and negative

The applications are endless. Some of the practical benefits are:

- Time savings. Reduced time spent poring over volumes of unconnected information
- Objectivity. The results are guaranteed to be the same regardless of who performs the review
- Compliance with legislation. Easier monitoring for compliance with statutory requirements imposed by SOX, HIPAA and other legislative changes relating to corporate governance
- More powerful justifications. The ability to present more convincing arguments to senior, non-technical management who do not have the time, or the inclination, to understand masses of technical detail

Interested?

Contact us at inbox@sekchek.com to find out how to get started!

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

2 . Directory Tree Structure

This report lists all Container objects and summarises the Directory tree structure for your system.

| L2 | L3 | L4 | L5 | L6 |
|-----------------|----------------|-------------|--------|--------|
| Emperor(O) | | | | |
| | EMP26 | | | |
| org1(O) | | | | |
| org2(O) | | | | |
| | test1 | | | |
| PLUTO(O) | | | | |
| | OrgSecondLevel | | | |
| | | test1 | | |
| | OrgUnit1 | | | |
| | | Layer3 | | |
| | | | Layer4 | |
| | | | | Layer5 |
| SA(C) | | | | |
| | SekChek(O) | | | |
| | | Development | | |
| | | Operation | | |
| ServerNetw65(O) | | | | |
| | Org1(O) | | | |
| | org2(O) | | | |
| | Org3 | | | |
| | Tomcat-Roles | | | |
| | VirtualOffice | | | |
| | | Teams | | |

Although all report sections list an object's context, this report may help you to understand the *overall* structure of the Directory tree, especially in cases where it is particularly large or complex. Levels in the Directory tree are shown left (highest level) to right (lowest level).

Values in brackets () indicate the class of the Container object:

- (C) is a Country object. Although not mandatory, Countries are the highest possible level in the Directory tree and belong to [Root]. Country objects can only contain Organisation objects.
- (O) is an Organisation object. Organisation objects can (optionally) contain Organisational Unit objects and leaf objects.

All other objects listed are Organisational Units.

All NDS objects (e.g. Users, Groups, Servers) belong to either an Organisation or to an Organisational Unit Container object.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

3 . Intruder Detection Values

This report lists Intruder Detection values for all Organisation (O) and Organisational Unit (OU) objects defined on your system.

SekChek's Recommended Intruder Detection Values.

| <u>Detect Intruder</u> | <u>Incorrect Login Count</u> | <u>Lock Account After Detection</u> | <u>Intruder Lockout Reset Interval</u> | <u>Intruder Attempt Reset Interval</u> |
|------------------------|------------------------------|-------------------------------------|--|--|
| Yes | 3 | Yes | 40:00:00 | 1:00:00 |

Actual Intruder Detection Values.

| Context | Container | Detect Intruder | Incorrect Login Count | Lock Account After Detection | Intruder Lockout Reset Interval | Intruder Attempt Reset Interval |
|------------------------------|--------------------|-----------------|-----------------------|------------------------------|---------------------------------|---------------------------------|
| [Root] | Emperor(O) | No | 6 | No | | |
| | org1(O) | Yes | 7 | Yes | 10:0:0 | |
| | org2(O) | Yes | 18 | Yes | | 5:0:0 |
| | PLUTO(O) | No | 6 | No | | |
| | ServerNetw65(O) | No | 6 | No | | |
| Emperor | EMP26(OU) | No | 6 | No | | |
| Layer3.OrgUnit1.PLUTO | Layer4(OU) | No | 6 | No | | |
| Layer4.Layer3.OrgUnit1.PLUTO | Layer5(OU) | No | 6 | No | | |
| org2 | test1(OU) | No | 6 | No | | |
| OrgSecondLevel.PLUTO | test1(OU) | No | 6 | No | | |
| OrgUnit1.PLUTO | Layer3(OU) | No | 6 | No | | |
| PLUTO | OrgSecondLevel(OU) | No | 6 | No | | |
| | OrgUnit1(OU) | No | 6 | No | | |
| SA | SekChek(O) | Yes | 20 | Yes | | |
| SekChek.SA | Development(OU) | No | 6 | No | | |
| | Operation(OU) | No | 6 | No | | |
| ServerNetw65 | Org1(OU) | No | 6 | No | | |
| | org2(OU) | No | 6 | No | | |
| | Org3(OU) | No | 6 | No | | |
| | Tomcat-Roles(OU) | No | 6 | No | | |
| | VirtualOffice(OU) | No | 6 | No | | |
| VirtualOffice.ServerNetw65 | Teams(OU) | No | 6 | No | | |

Implications

Intruder Detection features play an important role in controlling the risk of unauthorised access to your system via repeated password guessing attempts.

Context. The location of the Container object in the Directory tree.

Container. The name of the Organisation (O) or Organisational Unit (OU) object. Intruder Detection values can be defined for Organisation and Organisational Unit objects and apply to all user accounts within their scope.

Detect Intruder. Determines whether *Intruder Detection* features for the Container are active ('Yes') or inactive ('No').

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

Incorrect Login Count. Defines the number of consecutive, incorrect login attempts (i.e. incorrect password guessing attempts) allowed before offending user accounts are automatically locked by the system. Refer also *Lock Account After Detection*.

The Incorrect Login Count for a user account is automatically reset to zero after the period defined in *Intruder Attempt Reset Interval* has expired or after a successful login.

Lock Account After Detection. Determines whether the system automatically locks offending user accounts when the threshold defined in *Incorrect Login Count* is exceeded.

Intruder Lockout Reset Interval. The length of time that user accounts are locked by the system if the threshold for *Incorrect Login Attempts* is exceeded. Expressed as *Days:Hours:Minutes*.

Intruder Attempt Reset Interval. Defines the time after which the number of *Incorrect Login Attempts* for offending user accounts is automatically reset to zero. Expressed as *Days:Hours:Minutes*.

Risk Rating

Medium to High. (High if *Intruder Detection* features are not used; Medium/High if they are set to inappropriate values)

Recommended Action

You should review *Intruder Detection* values and ensure they are set to the following recommended values for all Organisations and Organisational Units defined on your system:

- Detect Intruder: Yes
- Incorrect Login Count: 3
- Lock Account After Detection: Yes
- Intruder Lockout Reset Interval: 40 (days)
- Intruder Attempt Reset Interval: 1 (day) or greater

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

4 . Alias Names

Section Summary

There are a total of 2 alias names defined on your system.

Section Detail

| Alias Context | Alias Name | Aliased Object Context | Aliased Object |
|---------------|-------------|------------------------|----------------|
| SekChek.SA | Alias Admin | ServerNetw65 | admin(U) |
| ServerNetw65 | Alias1 | ServerNetw65 | admin(U) |

Implications

An Alias object points to another object in the Directory tree. It makes it appear that the object that it references actually exists in the part of the Directory tree where the Alias is created. Although an Alias is a Leaf object, it can point to a Container object, so an Alias can appear to contain other objects.

The purpose of an Alias is to allow users to work with the object the Alias points to without having to change to the object's context.

Although an object appears both where it was first created and where an Alias object referring to it was created, only one copy of the object really exists. Changes made to either object affect what appears in both locations. Note that Rights to the Aliased object are always inherited from an object's true parent container, and not from the parent container of an Alias that points to it.

Risk Rating

None. (information only)

Recommended Action

None. Information only.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

5 . User Accounts

Section Summary

There are a total of 40 user accounts defined on your system.

Section Detail

| Context | User | Full Name |
|-------------------------------------|-----------------------|-----------|
| Development.SekChek.SA | James | |
| | Janice | |
| | June | |
| | Kirk | |
| EMP26.Emperor | User1 | |
| | User2 | |
| | User3 | |
| | User4 | |
| | User5 | |
| | User6 | |
| Layer3.OrgUnit1.PLUTO | jonesl | |
| Layer4.Layer3.OrgUnit1.PLUTO | jimmy | |
| Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | |
| | sublieutenant | |
| Operation.SekChek.SA | Jeffrey | |
| | Jerry | |
| org1 | jopes | |
| | jophnny | |
| | m | |
| Org1.ServerNetw65 | test1 | |
| org2.ServerNetw65 | test2 | |
| Org3.ServerNetw65 | test3 | |
| OrgSecondLevel.PLUTO | jenna | |
| | johnny | |
| | Jose | |
| | Sally | |
| OrgUnit1.PLUTO | *& | |
| | 2132 | |
| PLUTO | hidden1 | |
| SekChek.SA | O'neil | |
| | superadmin | |
| | Tom | |
| ServerNetw65 | admin | |
| | BackupAdmin | |
| | eGuidePublicUser32312 | |
| | NFAUUser | |
| test1.org2 | TestUser | |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Context | User | Full Name |
|----------------------------|------------|-----------|
| | TestUser1 | |
| Tomcat-Roles.ServerNetw65 | test | |
| VirtualOffice.ServerNetw65 | publicUser | |

Implications

In general, user accounts should be assigned to specific individuals and owners should be responsible for ensuring the confidentiality of their private login passwords. If user accounts are assigned to job functions, and shared by several people, it will be difficult to ensure accountability for actions performed by them.

Accounts that are no longer in use, such as those belonging to personnel who have left the organisation, should be promptly deleted from the system. Redundant accounts present intruders with unnecessary opportunities to gain access to your system with little risk of detection.

Risk Rating

Medium. (If user accounts are not assigned to specific individuals)

Recommended Action

You should check that:

- User accounts are still current and that their owners still require access to the system; and
- User accounts are assigned to specific individuals and not to job functions.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

6 . Objects with Supervisory Rights

Section Summary

A total of 13 objects on your system have one or more Supervisory rights:

- 18% (7) of user accounts have one or more Supervisory rights

Section Detail

| Subject Context | Subject | Object Context | Object | Property |
|----------------------------|------------------|----------------|------------------|-------------------------|
| [Root] | [This] | [Root] | [Root] | nsimHint |
| | | | | nsimPasswordReminder |
| | ServerNetw65(O) | [Root] | ServerNetw65(O) | CN |
| | | | | Full Name |
| | | | | Given Name |
| | | | | Internet EMail Address |
| | | | | Surname |
| SekChek.SA | NetworkAdmin(R) | [Root] | [Root] | [All Properties Rights] |
| | | | | [Object Rights] |
| | O'neil(U) | SekChek.SA | Login Profile(P) | [All Properties Rights] |
| | | | | [Object Rights] |
| | superadmin(U) | [Root] | [Root] | [All Properties Rights] |
| | | | | [Object Rights] |
| | | SekChek.SA | Login Profile(P) | [All Properties Rights] |
| | | | | [Object Rights] |
| | Tom(U) | SekChek.SA | Login Profile(P) | [All Properties Rights] |
| | | | | [Object Rights] |
| ServerNetw65 | admin(U) | [Root] | [Root] | [Object Rights] |
| | DNSDHCP-GROUP(G) | ServerNetw65 | DNSDHCP-GROUP(G) | [All Properties Rights] |
| | NFAUUser(U) | ServerNetw65 | NFAUUser(U) | [All Properties Rights] |
| | SEKSQL65(S) | [Root] | ServerNetw65(O) | [All Properties Rights] |
| | | | | [Object Rights] |
| | | ServerNetw65 | SEKSQL65(S) | [Object Rights] |
| test1.org2 | TestUser(U) | [Root] | Emperor(O) | [All Properties Rights] |
| | | | | [Object Rights] |
| VirtualOffice.ServerNetw65 | pco | [Root] | ServerNetw65(O) | ACL |
| | | | | bhCmAcceptList |
| | | | | bhCmApprovedList |
| | | | | bhCmAssignList |
| | | | | bhCmDeniedList |
| | | | | bhCmInviteList |
| | | | | bhObjectGUID |
| | | | | Object Class |
| | publicUser(U) | [Root] | ServerNetw65(O) | CN |

Key:

Subject: The account with the supervisory right.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

- Object:** The object over which the account has the supervisory right.
(CM) = Computer; (G) = Group; (O) = Organisation; (OU) = Organisational Unit; (P) = Profile; (R) = Role; (S) = Server; (U) = User; (V) = Volume.
- Property:** The property of the object for which the account has the supervisory right. Some of the more important properties are:
- All Property Rights
 - Object Rights
 - Account Disabled
 - Account Locked
 - Allow User To Change Password
 - Days Between Forced (password) Changes
 - Default Server
 - Group Membership
 - Incorrect Login Count
 - Intruder Attempt Reset Interval
 - Intruder Lockout Reset Interval
 - Login Script
 - Minimum Password Length
 - Require a Password

Implications

The Supervisory right is the most powerful right that can be granted to a user.

Risk Rating

High. (If users are assigned powerful Supervisory rights that are not in line with their job functions)

Recommended Action

You should check that the listed Supervisory rights over objects are appropriate and in line with users' job functions. See report [Security Equivalences](#) also.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

7. Security Equivalences

Section Summary

There are a total of 20 'security equivalent' rules defined on your system.

Section Detail

| Security Equal To Context | Security Equal To | Object Context | Object | M/O | |
|-------------------------------------|---------------------------|-------------------------------------|--------------------------|----------------|-----|
| Development.SekChek.SA | DEV(G) | Development.SekChek.SA | James(U) | Yes | |
| | | | Janice(U) | Yes | |
| | TSG(G) | Development.SekChek.SA | June(U) | Yes | |
| | | | Kirk(U) | Yes | |
| Layer5.Layer4.Layer3.OrgUnit1.PLUTO | manage\.\.*group(G) | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin(U) | Yes | |
| | | | sublieutenant(U) | Yes | |
| Operation.SekChek.SA | Shift leader(R) | Operation.SekChek.SA | Jeffrey(U) | Yes | |
| OrgSecondLevel.PLUTO | group\manager(G) | OrgSecondLevel.PLUTO | jenna(U) | Yes | |
| | | | johnny(U) | Yes | |
| | | | Jose(U) | Yes | |
| | | | Sally(U) | Yes | |
| SekChek.SA | NetworkAdmin(R) | SekChek.SA | O'neil(U) | Yes | |
| ServerNetw65 | admin(U) | SekChek.SA | superadmin(U) | | |
| | | | ServerNetw65 | BackupAdmin(U) | |
| | | | | NFAUUser(U) | |
| | apchadm-Administrators(G) | ServerNetw65 | admin(U) | Yes | |
| | | | BackupAdmin(U) | admin(U) | |
| | | | sshadm-Administrators(G) | admin(U) | Yes |
| Tomcat-Roles.ServerNetw65 | admin(G) | ServerNetw65 | admin(U) | Yes | |
| | manager(G) | ServerNetw65 | admin(U) | Yes | |

Note.

A value of 'Yes' in the M/O column indicates that the object acquired security equivalence via a Group membership or Role occupancy.

Implications

A User object that is security equivalent to other objects automatically inherits the Rights of those objects. These inherited Rights are added to those Rights that are directly assigned to the User object.

E.g. if User JOE is security equivalent to User ADMIN, JOE also has the same Supervisory Rights as ADMIN. If a User object is a member of a Group or Organisational Role object, the user is automatically made security equivalent to that Group or Organisational Role. This is the recommended way of granting the same set of Rights to a large number of Users.

Note that every object is *automatically* security equivalent to all of the objects in its complete name. E.g. user JOE in ACCOUNTS.SEKCHEK_ORG is security equivalent to the 2 containers above him. This means that if the container ACCOUNTS has the Supervisory object right to MARKETING, so does JOE. *Note that these higher-level container objects are not listed in the report.*

Only User objects can be security equivalent to other objects. By implication, this means that Groups cannot have other Groups as members.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

The implications are fairly obvious. If Users are made security equivalent to too many objects with powerful Rights, these accumulated Rights could be used accidentally, or deliberately, to exploit security on your system.

Risk Rating

Medium to High. (if users are granted excessive security equivalences to other objects).

Recommended Action

You should check that security equivalences assigned to users do not result in them being given Rights that are inconsistent with their job functions. In particular, you should ensure that the number of security equivalences to user Admin (and to other user objects that are security equivalent to Admin) are kept to a minimum.

See report [Objects with Supervisory Rights](#) also.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

8 . Groups and Roles

Section Summary

There are a total of 19 Group and Role objects defined on your system:

- 47% (9) of these do not have any members and may be redundant

Section Detail

| Context | Group/Role | Description |
|-------------------------------------|----------------------------|--|
| Development.SekChek.SA | DEV(G) | Members of the development team: |
| | TSG(G) | This is the technical support |
| EMP26.Emperor | Group1(G) | |
| | Group2(G) | |
| | Group3(G) | |
| | Group4(G) | |
| | Group5(G) | |
| Layer5.Layer4.Layer3.OrgUnit1.PLUTO | manage\.\.*group(G) | |
| Operation.SekChek.SA | Shift leader(R) | Operation leader regarding: |
| Org1.ServerNetw65 | 123654(G) | |
| OrgSecondLevel.PLUTO | group\.manager(G) | |
| SekChek.SA | NetworkAdmin(R) | Administering: |
| ServerNetw65 | apchadmn-Administrators(G) | |
| | DNSDHCP-GROUP(G) | |
| | NFAUWorld(G) | NFAU World Group Object |
| | SMS SMDR Group(G) | Group of Backup/Restore entities user by SMS |
| Tomcat-Roles.ServerNetw65 | sshadmn-Administrators(G) | |
| | admin(G) | |
| | manager(G) | |

Implications

Groups and Roles are leaf objects. They provide a convenient way to give several users the same set of Rights and privileges. Access rights assigned to Group and Role objects are added to rights that are directly assigned to Users via their user accounts.

Refer also report [Redundant Groups](#).

Risk Rating

Low. Information only.

Recommended Action

You should confirm that [group memberships/security equivalences](#) are appropriate. You should also check that Rights assigned to Group and Role objects are reasonable and intended. This can be done via the 'NetWare Administrator' utility.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

9 . Redundant Groups

Section Summary

The following 9 Group and Role objects do not have any members and may be redundant.

Section Detail

| Context | Group/Role |
|-------------------|-------------------|
| EMP26.Emperor | Group1(G) |
| | Group2(G) |
| | Group3(G) |
| | Group4(G) |
| | Group5(G) |
| Org1.ServerNetw65 | 123654(G) |
| ServerNetw65 | DNSDHCP-GROUP(G) |
| | NFAUWorld(G) |
| | SMS SMDR Group(G) |

Implications

A housekeeping issue only.

Risk Rating

None.

Recommended Action

You should determine the reason these empty Group and Role objects are defined to your system. If there is no valid reason, they should be deleted.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

10 . Users Not Allowed to Change Their Passwords

Section Summary

All Accounts

10% (4) of users are not allowed to change their passwords.

Excluding Disabled Accounts

10% (4) of users are not allowed to change their passwords.

Section Detail

| Context | User Name | Account Disabled |
|-------------------|-----------|------------------|
| Org1.ServerNetw65 | test1 | |
| org2.ServerNetw65 | test2 | |
| Org3.ServerNetw65 | test3 | |
| ServerNetw65 | NFAUUser | |

Implications

If users are not permitted to change their passwords on a frequent basis, their passwords are likely to become known to other employees and potential intruders. The user account could then be used to gain unauthorised access to systems and data until the password is changed to a new one.

Risk Rating

Medium to High. (Dependant on the strength of other password controls & the rights assigned to the account)

Recommended Action

In general, you should allow all users with access to your system to change their own passwords.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

11 . Minimum Password Lengths Less than 6

Section Summary

All Accounts

95% (38) of user accounts on your system are allowed to use passwords less than 6 characters in length:

- 90% (36) of user accounts are allowed to use passwords less than 4 characters in length
- 90% (36) of user accounts are allowed to use passwords less than 2 characters in length
- 90% (36) of user accounts are not required to use a password to sign-on to your system

Excluding Disabled Accounts

95% (38) of user accounts on your system are allowed to use passwords less than 6 characters in length:

- 90% (36) of user accounts are allowed to use passwords less than 4 characters in length
- 90% (36) of user accounts are allowed to use passwords less than 2 characters in length
- 90% (36) of user accounts are not required to use a password to sign-on to your system

Section Detail

| Minimum Password Length | Context | User Name | Account Disabled | Password Required |
|-------------------------|-------------------------------------|---------------|------------------|-------------------|
| | Development.SekChek.SA | James | | No |
| | Development.SekChek.SA | Janice | | No |
| | Development.SekChek.SA | June | | No |
| | EMP26.Emperor | User1 | | No |
| | EMP26.Emperor | User2 | | No |
| | EMP26.Emperor | User3 | | No |
| | EMP26.Emperor | User4 | | No |
| | EMP26.Emperor | User5 | | No |
| | EMP26.Emperor | User6 | | No |
| | Layer3.OrgUnit1.PLUTO | jonesl | | No |
| | Layer4.Layer3.OrgUnit1.PLUTO | jimmy | | No |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | | No |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | sublieutenant | | No |
| | Operation.SekChek.SA | Jeffrey | | No |
| | Operation.SekChek.SA | Jerry | | No |
| | org1 | jopes | | No |
| | org1 | jophnny | | No |
| | org1 | m | | No |
| | Org1.ServerNetw65 | test1 | | No |
| | org2.ServerNetw65 | test2 | | No |
| | OrgSecondLevel.PLUTO | jenna | | No |
| | OrgSecondLevel.PLUTO | johnny | | No |
| | OrgSecondLevel.PLUTO | Jose | | No |
| | OrgSecondLevel.PLUTO | Sally | | No |
| | OrgUnit1.PLUTO | *& | | No |
| | OrgUnit1.PLUTO | 2132 | | No |
| | PLUTO | hidden1 | | No |
| | SekChek.SA | O'neil | | No |
| | SekChek.SA | Tom | | No |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Minimum Password Length | Context | User Name | Account Disabled | Password Required |
|-------------------------|----------------------------|-----------------------|------------------|-------------------|
| | ServerNetw65 | admin | | No |
| | ServerNetw65 | eGuidePublicUser32312 | | No |
| | ServerNetw65 | NFAUUser | | No |
| | test1.org2 | TestUser | | No |
| | test1.org2 | TestUser1 | | No |
| | Tomcat-Roles.ServerNetw65 | test | | No |
| | VirtualOffice.ServerNetw65 | publicUser | | No |
| 4 | Org3.ServerNetw65 | test3 | | |
| 5 | SekChek.SA | superadmin | | |

Implications

A blank value for Minimum Password Length (or a value of 'No' in the 'Password Required' field) indicates that the user is not required to use a password to sign-on to your system.

Short passwords allow users to select trivial and easy-to-guess passwords, which increases the risk of unauthorised access to your system and information resources. The particular resources an intruder could gain access to depend on the access rights and privileges assigned to the user account.

Weak password controls also result in a loss of accountability for actions performed on your system.

Risk Rating

Medium to High. (If users are not required to use passwords to sign-on to your system or minimum password lengths are too short)

Recommended Action

You should ensure strong passwords are assigned to *all* user accounts defined to your system. A generally accepted standard for a minimum password length is 6 characters.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

12 . Password Change Intervals Greater than 30 Days

Section Summary

All Accounts

100% (40) of the user accounts on your system are not forced to change their password every 30 days (or less):

- 98% (39) are not forced to change their password every 60 days (or less)
- 98% (39) are not forced to change their password every 90 days (or less)
- 98% (39) are not forced to change their password every 120 days (or less)
- 98% (39) are not forced to change their password every 180 days (or less)
- 98% (39) are never required to change their password

Excluding Disabled Accounts

100% (40) of the user accounts on your system are not forced to change their password every 30 days (or less):

- 98% (39) are not forced to change their password every 60 days (or less)
- 98% (39) are not forced to change their password every 90 days (or less)
- 98% (39) are not forced to change their password every 120 days (or less)
- 98% (39) are not forced to change their password every 180 days (or less)
- 98% (39) are never required to change their password

Section Detail

| Password Change Interval | Context | User Name | Account Disabled |
|--------------------------|-------------------------------------|---------------|------------------|
| 40 | Development.SekChek.SA | Kirk | |
| | Development.SekChek.SA | James | |
| | Development.SekChek.SA | Janice | |
| | Development.SekChek.SA | June | |
| | EMP26.Emperor | User1 | |
| | EMP26.Emperor | User2 | |
| | EMP26.Emperor | User3 | |
| | EMP26.Emperor | User4 | |
| | EMP26.Emperor | User5 | |
| | EMP26.Emperor | User6 | |
| | Layer3.OrgUnit1.PLUTO | jonesl | |
| | Layer4.Layer3.OrgUnit1.PLUTO | jimmy | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | sublieutenant | |
| | Operation.SekChek.SA | Jeffrey | |
| | Operation.SekChek.SA | Jerry | |
| | org1 | jopes | |
| | org1 | jophnny | |
| | org1 | m | |
| | Org1.ServerNetw65 | test1 | |
| | org2.ServerNetw65 | test2 | |
| | Org3.ServerNetw65 | test3 | |
| | OrgSecondLevel.PLUTO | jenna | |
| | OrgSecondLevel.PLUTO | johnny | |
| | OrgSecondLevel.PLUTO | Jose | |
| | OrgSecondLevel.PLUTO | Sally | |
| | OrgUnit1.PLUTO | *& | |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Password Change Interval | Context | User Name | Account Disabled |
|--------------------------|----------------------------|-----------------------|------------------|
| | OrgUnit1.PLUTO | 2132 | |
| | PLUTO | hidden1 | |
| | SekChek.SA | O'neil | |
| | SekChek.SA | superadmin | |
| | SekChek.SA | Tom | |
| | ServerNetw65 | admin | |
| | ServerNetw65 | BackupAdmin | |
| | ServerNetw65 | eGuidePublicUser32312 | |
| | ServerNetw65 | NFAUUser | |
| | test1.org2 | TestUser | |
| | test1.org2 | TestUser1 | |
| | Tomcat-Roles.ServerNetw65 | test | |
| | VirtualOffice.ServerNetw65 | publicUser | |

Implications

Password Change Intervals are expressed in days. A blank entry indicates that the user is never required to change his password.

Passwords that are not changed on a frequent basis can be compromised over time. This would enable an intruder to gain authorised access to your system functions and data.

Risk Rating

Medium to High. (Dependant on the strength of other password controls, such as minimum password length)

Recommended Action

Password change intervals for these user accounts should be brought in line with installation standards.

A generally accepted standard is to force users to change their passwords every 30 to 60 days.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

13 . Users Not Requiring a Unique Password

Section Summary

All Accounts

100% (40) of user accounts on your system are not required to use unique passwords.

Excluding Disabled Accounts

100% (40) of user accounts on your system are not required to use unique passwords.

Section Detail

| Context | User Name | Disabled |
|-------------------------------------|-----------------------|----------|
| Development.SekChek.SA | James | |
| | Janice | |
| | June | |
| | Kirk | |
| EMP26.Emperor | User1 | |
| | User2 | |
| | User3 | |
| | User4 | |
| | User5 | |
| | User6 | |
| Layer3.OrgUnit1.PLUTO | jonesl | |
| Layer4.Layer3.OrgUnit1.PLUTO | jimmy | |
| Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | |
| | sublieutenant | |
| Operation.SekChek.SA | Jeffrey | |
| | Jerry | |
| org1 | jopes | |
| | jophnny | |
| | m | |
| Org1.ServerNetw65 | test1 | |
| org2.ServerNetw65 | test2 | |
| Org3.ServerNetw65 | test3 | |
| OrgSecondLevel.PLUTO | jenna | |
| | johnny | |
| | Jose | |
| | Sally | |
| OrgUnit1.PLUTO | *& | |
| | 2132 | |
| PLUTO | hidden1 | |
| SekChek.SA | O'neil | |
| | superadmin | |
| | Tom | |
| ServerNetw65 | admin | |
| | BackupAdmin | |
| | eGuidePublicUser32312 | |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Context | User Name | Disabled |
|----------------------------|------------|----------|
| | NFAUUser | |
| test1.org2 | TestUser | |
| | TestUser1 | |
| Tomcat-Roles.ServerNetw65 | test | |
| VirtualOffice.ServerNetw65 | publicUser | |

Implications

Determines whether any of the previous 8 passwords can be reused.

If users are allowed to reuse previous passwords it increases the risk of their passwords being compromised over time.

Risk Rating

Medium. (Dependant on the strength of other password controls, such as *minimum password length*)

Recommended Action

You should ensure that users are prevented from reusing previous passwords.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

14 . Expired Passwords

Section Summary

All Accounts

3% (1) of the user accounts on your system have expired passwords.

Excluding Disabled Accounts

3% (1) of the user accounts on your system have expired passwords.

Section Detail

| Password Expiry Date | Context | User Name | Grace Logins Remaining | Disabled |
|----------------------|------------------------|-----------|------------------------|----------|
| 16-Aug-2010 | Development.SekChek.SA | Kirk | 10 | |

Implications

The passwords for these accounts have expired and must be changed by their owners the next time they are used to logon to the system, unless the number of Grace Logins Remaining is greater than zero.

Grace Logins allow a user with an expired password to continue signing-on until his Grace Logins are consumed. The Grace Login count is decreased by 1 each time a user with an expired password logs on without changing his password. Refer also to report [Grace Logins](#).

It is also possible that a system administrator has set the passwords for these accounts to well-known, trivial values that users are required to change the first/next time they logon to the system. Examples would include new accounts and accounts for which the owners have forgotten the passwords.

Risk Rating

Low. (Unless an administrator has set passwords for these accounts to a well known default value)

Recommended Action

Initial passwords for new accounts, and accounts for which owners have forgotten the password, should always be set to random, non-trivial values.

Owners should be reminded to sign-on to their accounts promptly and change the password to a new, private value known only to themselves.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

15 . Grace Logins

Section Summary

All Accounts

3% (1) of the user accounts on your system have Grace Login counts greater than 6.

Excluding Disabled Accounts

3% (1) of the user accounts on your system have Grace Login counts greater than 6.

Section Detail

| Grace Logins | Context | User Name | Disabled |
|--------------|------------------------|-----------|----------|
| 10 | Development.SekChek.SA | Kirk | |

Implications

Grace Logins allow users with expired passwords to continue signing-on until their Grace Logins are consumed. The Grace Login count is decreased by 1 each time a user with an expired password logs on without changing his password.

If the Grace Login count is set to a very high value, it will have an effect similar to a *long period between password changes*. I.e. it increases the risk of passwords being compromised over time.

Risk Rating

Low to Medium. (Dependent on the strength of other password controls)

Recommended Action

Grace Login values should be set to a maximum of 6.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

16 . Disabled Accounts

Section Summary

0% (0) of usernames are disabled and cannot be used to sign-on to your system.

Section Detail

*** None were found ***

Implications

The listed user accounts cannot be used to login to the system for the following reasons:

- The account has been *disabled* by a system administrator; or
- The account has been *locked* by the system because it exceeded the system's Intruder detection threshold (see [Intruder Detection Values](#)); or
- The account has an *expiry date*, which has been reached.

Risk Rating

Low. A housekeeping issue only.

Recommended Action

You should determine the reason that accounts have been locked. It could indicate that an intruder is attempting to guess users' password in order to login to your system.

The other listed accounts should be checked and deleted if they will not be required again.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

17 . Accounts with Expiry Dates

Section Summary

13% (5) of user accounts are set to expire on a certain date.

Section Detail

| Account Expiration Date | Context | User Name | Full Name |
|-------------------------|------------------------|-----------|-----------|
| 01-Jan-2020 | Development.SekChek.SA | June | |
| 16-Aug-2020 | Development.SekChek.SA | Kirk | |
| 17-Aug-2020 | Development.SekChek.SA | James | |
| 01-Jan-2026 | Operation.SekChek.SA | Jerry | |
| 17-Aug-2028 | Operation.SekChek.SA | Jeffrey | |

Implications

The Account Expiration Date parameter allows you to ensure an account is automatically disabled on the assigned date. This feature may be used for example, to ensure accounts assigned to temporary personnel are automatically disabled when the person leaves the organisation.

Risk Rating

None. (Information only)

Recommended Action

It is good practice to set an expiration date for temporary accounts or accounts assigned to contractors and temporary staff.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

18 . Invalid Logon Attempts Greater than 3

Section Summary

0% (0) of user accounts have invalid logon attempts greater than 3:

- 0% (0) of user accounts have been locked out due to excessive invalid logon attempts

Section Detail

*** None were found ***

Implications

Incorrect Logon Attempts indicate the number of unsuccessful attempts at signing on to your system with the listed accounts. The value is reset to '0' after a successful sign-on to the system or when the *Intruder Attempt Reset Interval* (defined in the users' Container object) expires.

Accounts flagged as *Locked* have been locked out by the system because the number of invalid logon attempts via the account has exceeded the threshold allowed. These accounts can only be unlocked by an administrator unless the period defined in the *Intruder Lockout Reset Interval* expires, in which case the accounts are automatically unlocked by the system.

Consistently high values, or frequent account lockouts, could indicate that an intruder is attempting to guess user passwords to gain access to your system.

Risk Rating

Medium to High. (Dependent on the value of the Intruder Detection values in the users' Container objects and on the strength of password controls, such as minimum password length and password content)

Recommended Action

You should investigate the reason for high numbers of incorrect sign-on attempts and take appropriate action.

You should also ensure that *Intruder Detection* values for users' Container objects are set to appropriate values.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

19 . Accounts Allowed Simultaneous Device Sessions

Section Summary

All Accounts

100% (40) of user accounts on your system can sign-on to more than one work-station at the same time:

- 100% (40) of user accounts can sign-on to an unlimited number of work-stations at the same time

Excluding Disabled Accounts

100% (40) of user accounts on your system can sign-on to more than one work-station at the same time:

- 100% (40) of user accounts can sign-on to an unlimited number of work-stations at the same time

Section Detail

| Maximum Connections | Context | User Name | Disabled |
|---------------------|-------------------------------------|---------------|----------|
| | Development.SekChek.SA | James | |
| | Development.SekChek.SA | Janice | |
| | Development.SekChek.SA | June | |
| | Development.SekChek.SA | Kirk | |
| | EMP26.Emperor | User1 | |
| | EMP26.Emperor | User2 | |
| | EMP26.Emperor | User3 | |
| | EMP26.Emperor | User4 | |
| | EMP26.Emperor | User5 | |
| | EMP26.Emperor | User6 | |
| | Layer3.OrgUnit1.PLUTO | jonesl | |
| | Layer4.Layer3.OrgUnit1.PLUTO | jimmy | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | sublieutenant | |
| | Operation.SekChek.SA | Jeffrey | |
| | Operation.SekChek.SA | Jerry | |
| | org1 | jopes | |
| | org1 | jophnny | |
| | org1 | m | |
| | Org1.ServerNetw65 | test1 | |
| | org2.ServerNetw65 | test2 | |
| | Org3.ServerNetw65 | test3 | |
| | OrgSecondLevel.PLUTO | jenna | |
| | OrgSecondLevel.PLUTO | johnny | |
| | OrgSecondLevel.PLUTO | Jose | |
| | OrgSecondLevel.PLUTO | Sally | |
| | OrgUnit1.PLUTO | *& | |
| | OrgUnit1.PLUTO | 2132 | |
| | PLUTO | hidden1 | |
| | SekChek.SA | O'neil | |
| | SekChek.SA | superadmin | |
| | SekChek.SA | Tom | |
| | ServerNetw65 | admin | |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Maximum Connections | Context | User Name | Disabled |
|---------------------|----------------------------|-----------------------|----------|
| | ServerNetw65 | BackupAdmin | |
| | ServerNetw65 | eGuidePublicUser32312 | |
| | ServerNetw65 | NFAUUser | |
| | test1.org2 | TestUser | |
| | test1.org2 | TestUser1 | |
| | Tomcat-Roles.ServerNetw65 | test | |
| | VirtualOffice.ServerNetw65 | publicUser | |

* A blank in the *Maximum Connections* column indicates that an unlimited number of simultaneous sessions are permitted for the account.

Implications

These accounts can be signed on to multiple workstations at the same time. This increases the risk of unauthorised access to the system because:

- An intruder could access the system via these user accounts without detection, even if the account is currently being used;
- If the owner has more than one active session, it is likely that the other sessions are unattended and could be used to gain unauthorised access to the system.

Risk Rating

Low to Medium. (Unless password controls, such as *minimum password length* and change frequency, are weak)

Recommended Action

These accounts should be checked to ensure that there is a valid need for them to have the capability of signing-on to multiple workstations at the same time. If there is no real need, they should be restricted to signing on to only one device at a time.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

20 . Last Logons, 30 Days and Older

Section Summary

All Accounts

100% (40) of users have not logged on to your system in the last 30 days:

- 100% (40) of users have not logged on in the last 60 days
- 100% (40) of users have not logged on in the last 90 days
- 100% (40) of users have not logged on in the last 180 days
- 88% (35) of users have never logged on

Excluding Disabled Accounts

100% (40) of users have not logged on to your system in the last 30 days:

- 100% (40) of users have not logged on in the last 60 days
- 100% (40) of users have not logged on in the last 90 days
- 100% (40) of users have not logged on in the last 180 days
- 88% (35) of users have never logged on

Note:

This is an exception report, so only lists accounts that have not logged on in the last 30 days. I.e. if an account logged in 29 days ago (or more recently) it will not be listed in the report section.

Section Detail

| Last Login | Context | User Name | Disabled |
|------------|-------------------------------------|---------------|----------|
| | Development.SekChek.SA | James | |
| | Development.SekChek.SA | Janice | |
| | Development.SekChek.SA | June | |
| | Development.SekChek.SA | Kirk | |
| | EMP26.Emperor | User1 | |
| | EMP26.Emperor | User2 | |
| | EMP26.Emperor | User3 | |
| | EMP26.Emperor | User4 | |
| | EMP26.Emperor | User5 | |
| | EMP26.Emperor | User6 | |
| | Layer3.OrgUnit1.PLUTO | jonesl | |
| | Layer4.Layer3.OrgUnit1.PLUTO | jimmy | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | SubAdmin | |
| | Layer5.Layer4.Layer3.OrgUnit1.PLUTO | sublieutenant | |
| | Operation.SekChek.SA | Jeffrey | |
| | Operation.SekChek.SA | Jerry | |
| | org1 | jopes | |
| | org1 | jophnny | |
| | org1 | m | |
| | Org1.ServerNetw65 | test1 | |
| | org2.ServerNetw65 | test2 | |
| | Org3.ServerNetw65 | test3 | |
| | OrgSecondLevel.PLUTO | jenna | |
| | OrgSecondLevel.PLUTO | johnny | |
| | OrgSecondLevel.PLUTO | Jose | |

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

| Last Login | Context | User Name | Disabled |
|-------------|----------------------------|-----------------------|----------|
| | OrgSecondLevel.PLUTO | Sally | |
| | OrgUnit1.PLUTO | *& | |
| | OrgUnit1.PLUTO | 2132 | |
| | PLUTO | hidden1 | |
| | SekChek.SA | O'neil | |
| | SekChek.SA | Tom | |
| | ServerNetw65 | eGuidePublicUser32312 | |
| | test1.org2 | TestUser1 | |
| | Tomcat-Roles.ServerNetw65 | test | |
| | VirtualOffice.ServerNetw65 | publicUser | |
| 31-Dec-1989 | ServerNetw65 | admin | |
| 31-Dec-1989 | ServerNetw65 | NFAUUser | |
| 01-Jan-1990 | test1.org2 | TestUser | |
| 18-Aug-2007 | ServerNetw65 | BackupAdmin | |
| 20-Aug-2007 | SekChek.SA | superadmin | |

* A blank date indicates that the account has never logged on or that the last logon date is unavailable.

Implications

Some of these user accounts may no longer be required. Inactive user accounts are a prime target for intruders. If their passwords are compromised, they can be used with little fear of detection.

Risk Rating

Low. (Unless password controls, such as *minimum password length*, are weak)

Recommended Action

The list of accounts should be reviewed and redundant ones should be deleted.

Accounts that will be required at some future time should be *disabled* until required.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

21 . Servers

Section Summary

There are 1 servers defined in your Directory tree.

Section Detail

| Context | Server | Version | Department |
|--------------|----------|----------------------------|------------|
| ServerNetw65 | SEKSQL65 | Novell NetWare 5.70.06[DS] | |

Implications

Every server and workstation represents a potential entry point and threat to your network and the computer and information resources attached to it.

Risk Rating

Low to Medium. (Dependant on the security settings on the Server)

Recommended Action

You should ensure that:

- Configurations and security settings are set to appropriate standards.
- Services and resources are appropriately restricted on servers and workstations.
- The rights and privileges assigned to user accounts and groups are effectively controlled.
- Effective virus detection and prevention software is installed and started automatically at system start-up time.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

22 . Computers

Section Summary

There are 5 computers defined in your Directory tree.

Section Detail

| Context | Computer |
|------------------------|-------------|
| Development.SekChek.SA | venustest |
| | winxpnovell |
| EMP26.Emperor | Computer1 |
| | Computer2 |
| | Computer3 |

Implications

Every workstation represents a potential entry point and threat to your network and the computer and information resources attached to it.

Risk Rating

Low to Medium. (If unnecessary devices are connected to your network)

Recommended Action

You should confirm that unintended workstations are not connected to your network.

Security Analysis: TESTBED NetWare

System: [Root].SEKNETWARE65
Analysis Date: 03-Sep-2010

CONFIDENTIAL

23 . Volumes

Section Summary

There are 2 volumes defined in your Directory tree.

Section Detail

| Context | Volume | Server | Host Resource |
|--------------|----------------|----------|---------------|
| ServerNetw65 | ADMIN_SEKSQL65 | SEKSQL65 | _ADMIN |
| | SEKSQL65_SYS | SEKSQL65 | SYS |

Implications

None. Information only.

Risk Rating

None.

Recommended Action

None.