



PHYSICAL SCIENCES

ON PERFORMANCE OF SOME METHODS OF DETECTING NONLINEARITY IN STATIONARY AND NON-STATIONARY TIME SERIES DATA

¹Akeyede, I., and ²Oyeyemi, G.M

¹Department of Mathematics, Federal University Lafia, PMB 146, Lafia, Nigeria

²Department of Statistics, University of Ilorin, PMB. 1515, Ilorin, Nigeria

Corresponding Email : imamakeyede@gmail.com

Date Manuscript Received: 12/07/2016

Accepted: 23/12/2016

Published: December, 2016

ABSTRACT

There has been growing interest in exploiting potential forecast gains from the nonlinear structure of autoregressive time series. Several models are available to fit nonlinear time series data. However, before investigating specific nonlinear models for time series data, it is desirable to have a test of nonlinearity in the data. And since most of real life data collected are non-stationary, there is need to investigate which of these test is suitable for stationary and non-stationary data. Statistical tests have been proposed in the literature to help analysts to check for the presence of nonlinearities in observed time series, these tests include Keenan and Tsay tests, and they have been used under the assumption that data is stationary. However, in this paper, we investigated the performance of these two tests for the stationary and non-stationary data. The effect of the stationarity and non-stationarity were studied on simulated data based on general class of linear and nonlinear autoregressive structures using R-software. The powers of tests were compared at different sample sizes for the two cases. It was observed that the Tsay F-test performed better than Keenan's tests with little order of autoregressive and increase in sample size when data is non-stationary and vice-versa when data is stationary. Finally, we provided illustrative examples by applying the statistical tests to real life datasets and results obtained were desirable.

Key words: *Nonlinearity, Tsay's F Test, Keenan's Test, Stationarity and Non-Stationarity*

INTRODUCTION

Several techniques used in time series modeling assume linear relationships among variables. However, in some cases, variations in data do not show simple linearity and therefore, are difficult to analyse and predict accurately. Hence, for such data, it would not be practicable to expect a single, linear model to capture these distinct behaviours. Linear relationships and their combinations for describing the behaviour of such data are often found to be grossly inadequate. In general time series analysis, it is known that there are large numbers of nonlinear features such as cycles, thresholds, bursts, chaos, heteroscedasticity, asymmetries and combinations of one or more of these. Tong (1990), Franse, and van Dijk (2000) and Tsay (2010) have presented the various types of models that can be cast into these forms.

Nowadays, there are various applications of nonlinear time series models to different fields, such as meteorology, finance, engineering and econometrics. The nonlinear time series models have been used extensively in recent years for modeling time series data that cannot be adequately represented using linear models. Hipel and McLeod (1994) hypothesized that, although a linear model may be adequate to describe average annual river flows, the relationship between daily river flow and precipitation may be nonlinear. For examples, Tong (1990) provides an introduction to different types of nonlinear time series modeling primarily in the univariate setting. Chen and Tsay (1993, 1996) and Lewis and Ray (1997) investigated techniques for obtaining bivariate nonlinear models. Terasvirta (1993) mentioned vector nonlinear autoregressive processes, vector nonlinear average processes and multiple bilinear time series models in passing but concentrated on statistical inference for nonlinear models using parametric procedure.

Before fitting a nonlinear time series model to a given set of data, it is good if the nonlinearity characteristics of the data can be detected. There are various tests that have been suggested over the past years to distinguish linear from the nonlinear data sets. For example, Hunnich (1982) used the bispectrum test. They used the fact that the square modulus of normalized bispectrum is constant when the time series is linear. The hypothesis is based on the non-centrality of parameters of the marginal distribution of the square moduli, where n is the sample size. Yuan (2000) modified the Hunnich's test in such a way that the parameter being tested under the null hypothesis is the location parameters, such as the mean or variance.

The problem of nonlinear time series identification and modelling has attracted considerable attention for years in diverse fields such as biometrics,

socioeconomics, transportation, electric power systems, and finance which exhibit nonlinear process. A good nonlinear model should be able to capture some of the nonlinear phenomena in the data. Once a model is selected, sufficiently strong evidence need to be found in the data to abandon the linear model. Therefore, good statistical and diagnostic tests are needed to determine the nonlinearity in time series data.

This work examined the performance of two nonlinearity tests in time series analysis; these are Kennan's test and F-test of nonlinearity. The power efficiency of each test was studied on different sample size, models and under the violation of assumption of stationarity based on simulated data and real data collected.

Stationarity

In Statistics, a stationary process is a stochastic process whose joint probability distribution does not change when shifted in time. Consequently, parameters such as the mean and variance, if they are present, also do not change over time. The most important assumption made about time series data is that of stationarity.

The basic idea of stationarity is that the probability laws that govern the behavior of the process do not change over time. In indeed, the process is statistically equilibrium. Specifically, a process $\{Y_t\}$ is said to be strictly stationary if the joint distribution of Y_t is the same as that of Y_{t-k} for all t and k ; $t = 1, 2, \dots, k$. In other words, the Y 's are (marginally) identically distributed (see Jonathan and Kung-Sik, 2008). It then follows that $E(Y_t) = E(Y_{t-k})$ for all t and k so that the mean function is constant for all time. Additionally, $\text{Var}(Y_t) = \text{Var}(Y_{t-k})$ for all t and k so that the variance is also constant over time.

Linear Time Series Model

A relationship of direct proportionality that, when plotted on a graph, traces a straight line. In linear relationships, any given change in an independent variable will always produce a corresponding change in the dependent variable. For example, a linear relationship between production hours and output in a factory determines percentage of increase or decrease of the output. The concept of linear relationship suggests that two quantities are proportional to each other: doubling one causes the other to double as well.

Linear relationships are often the first approximation used to describe any relationship, even though there is no unique way to explain what a linear relationship is in terms of the underlying nature of the quantities. For example, a linear relationship between the height and weight of an object is different from a linear relationship between the volume and weight of an object. The second relationship makes more

sense, but both are linear relationships, and they are, of course, incompatible with each other. Medications, especially for children, are often prescribed in proportion to weight. This is an example of a linear relationship. The linear time series modeling depends on the type of system that generates the data. Time series analysis may be Autoregressive Models, Moving Average Model or Autoregressive Moving Average Model (ARMA). However For the purpose of this research work we considered only general classes of second order autoregressive models.

Nonlinear Time series Model

Practitioners in many fields are increasingly faced with real data possessing nonlinear attributes. It is known that stationary Gaussian autoregressive models are structurally determined by their first two moments. Consequently, linear autoregressive models must be time reversible. Many real datasets are time irreversible, suggesting that the underlying process is nonlinear. Indeed, in Tong's seminal paper on threshold models, he would argue that no linear Gaussian model could explain the cyclical dynamics observed in sections of the lynx data (Tong and Lim, 1980). Furthermore, he argued that characteristics of nonlinear models, such as time irreversibility and limit cycles, mandated the development of practical nonlinear models to help resolve ongoing difficulties in real data. Tong's explanation and application of locally linear threshold models introduced striking opportunities for model building strategies.

The pioneering work in time series modeling is due to Wiener who had produced a very general class of nonlinear model, called Volterra series expansion and is generally given as follows;

$$X_t = \mu + \sum_{i=-\infty}^{\infty} \alpha_i X_{t-i} + \sum_{i,j=-\infty}^{\infty} \alpha_{ij} X_{t-i} X_{t-j} + \sum_{i,j,k=-\infty}^{\infty} \alpha_{ijk} X_{t-i} X_{t-j} X_{t-k} + \dots \quad 1$$

$$X_t = \mu + \sum_{i=-\infty}^{\infty} \beta_i e_{t-i} + \sum_{i,j=-\infty}^{\infty} \beta_{ij} e_{t-i} e_{t-j} + \sum_{i,j,k=-\infty}^{\infty} \beta_{ijk} e_{t-i} e_{t-j} e_{t-k} + \dots \quad 2$$

Where μ is the mean level of X_t , e_t , ($-\infty < t < \infty$) is a strictly stationary process of independent and identically distributed random variables. Obviously, X_t is nonlinear if one of the higher order coefficients α_{ij} , α_{ijk} , β_{ij} or β_{ijk} is non zero (Ibrahim *et al*, 2005).

For instance, the model 1 and 2 above can be illustrated with simple structures ($i, j = 1, 2, k = 0$) as follows;

$$X_t = \mu + \sum_{i=1}^2 \alpha_i X_{t-i} + \sum_{i=1}^2 \sum_{j=1}^2 \alpha_{ij} X_{t-i} X_{t-j}$$

$$\Rightarrow X_t = \mu + \alpha_1 X_{t-1} + \alpha_2 X_{t-2} + \alpha_{11} X_{t-1}^2 + \alpha_{12} X_{t-1} X_{t-2} + \alpha_{22} X_{t-2}^2 \quad \dots\dots\dots 3$$

$$X_t = \mu + \sum_{i=1}^2 \alpha_i e_{t-i} + \sum_{i=1}^2 \sum_{j=1}^2 \alpha_{ij} e_{t-i} e_{t-j}$$

$$\Rightarrow X_t = \mu + \alpha_1 e_{t-1} + \alpha_2 e_{t-2} + \alpha_{11} e_{t-1}^2 + \alpha_{12} e_{t-1} e_{t-2} + \alpha_{22} e_{t-2}^2 \quad \dots\dots\dots 4$$

Most linear models can be expressed into Volterra expansion form which includes the autoregressive model of order p , [AR (p)], the moving average model of order q [MA (q)] and the autoregressive moving average model of order p and q [ARMA (p, q)].

MATERIALS AND METHODS

Several authors such as Chan and Tong (1986) and Tsay (1986) raised the issue that one nonlinearity test is not enough to detect nonlinearity in a data set. Nonetheless, it is expected that the nonlinearity test will suggest whether a data set is linear or otherwise. Thus, if any test does suggest that the data is nonlinear, we expect that a nonlinear model will improve the modeling of the data set.

Indeed, in this work, a set of data were generated from model 1-4, under the assumption of stationarity stated earlier and the two tests, Keenan and F-tests of nonlinearity were applied to see the behavior of their acceptance of nonlinearity. Thereafter, another set of data were generated under the violation of the stationarity and white noise assumptions. Each test is subjected to 500 replication simulation at different sample sizes for stationarity and Non-Stationarity data structures. Both tests are based on time domain approach and suitably

applied on data generated from selected linear and nonlinear autoregressive models. Power efficiency of the tests was compared on the simulated data.

Keenan's Test

Keenan adopted the idea of Turkey one degree of freedom test for non-additivity to derive a time domain statistic. The test is motivated by similarity of Volterra expansions to polynomials, and is extremely simple, both conceptually and computationally. Assume that a time series Y_t , $t = 1, 2, \dots, n$, can be adequately approximated by order of Volterra expansion in 1 and 2

The approximation will be linear if the second and other higher terms on the right hand side are zero. The Keenan's test procedure is as follows;

(i) Regress Y_t on $(1, Y_{t-1}, \dots, Y_{t-m})$ and calculate the fitted values $(\hat{Y}_t)$, and the residuals, $(\hat{e}_t)$, for $t = m+1, \dots, n$, and the residual sum of squares $\sum e_s^2$

(ii) Regress Y_t^2 on $(1, Y_{t-1}, \dots, Y_{t-m})$ and calculate the residual (e_t) for $t = m, \dots, n$,

(iii) Regress $on \hat{e} = e_{m+1}, \dots, e_n$ on $\hat{\xi}_{m+1}, \dots, \hat{\xi}_n$

and obtain $\hat{\eta}$ and $\hat{F}$ from

$$\hat{\eta} = \hat{\eta}_0 \left(\sum_{t=m+1}^n \hat{\xi}_t^2 \right)$$

Where $\hat{\eta}_0$ is the regression coefficient, and

$$F_k = \frac{\hat{\eta}(n - 2m - 2)}{\sum_{t=m+1}^n \hat{\xi}_t^2 - \hat{\eta}^2}$$

Follows approximately $F_{1, n-2M-2}$, where the

degrees of freedom of associated with $\sum_{t=m+1}^n \hat{\xi}_t^2$ is $(n-M)-M-1$.

Keenan's test is based on the argument that if any of c_{ij} and other higher coefficients in 1 and 2 are non-zero, e.g c_{12} , then this nonlinearity will be distributionally reflected in the diagnostics of the fitted linear model, if the residuals of the linear model are correlated with $Y_t - IY_t - 2$. As in Turkey non additive test, Keenan's test used the aggregated quantity Y^2_t , the square of the fitted value of Y_t based on the fitted linear model, to obtain the quadratic terms upon which the residual can be correlated. The idea is extremely valuable when the sample size is small because it only requires one degree of freedom.

F-Test

Tsay (1986) modifies Keenan's test by replacing the aggregated quantity Y^2_t by the disaggregated variable $Y_t - iY_t - j$, $i, j = 1, \dots, M$, where M is defined in Keenan's test. The F-test procedure is as follows:

(i) Regress Y_t on $(1, Y_{t-1}, \dots, Y_{t-m})$ and calculate the fitted values $(\hat{Y}_t)$, and the residuals, $(\hat{e}_t)$, for $t = M+1, \dots, n$. the regression model is denoted by

$$Y_t = W_t \theta + e_t, \text{ where,}$$

$$W_t = (1, Y_{t-1}, \dots, Y_{t-m}) \text{ and } \theta = (\theta_0, \theta_1, \dots, \theta_m)T.$$

(ii) Regress vector Z_t on $(1, Y_{t-1}, \dots, Y_{t-m})$ and calculate the residuals (X_t) , for $t = M+1, \dots, n$. In this step, the multivariate regression model is $Z_t = W_t H + X_t$, where Z_t is an $m =$ dimensional vector defined by $Z_t = \text{Vech}(UT_t U_t)$ with $U_t = (Y_{t-1}, \dots, Y_{t-m})$, and Vech denoting the half stacking vector

$$(iii) F_j^+ = \hat{X}_t \beta + \epsilon_t, t = M + 1, \dots, n \quad \text{And define } \hat{F} = \frac{\frac{\sum \hat{X}_t^T \hat{e}_t (\sum \hat{X}_t^T \hat{X}_t)^{-1} \sum \hat{X}_t^T \hat{e}_t}{m}}{\frac{\sum \hat{e}_t^2}{n - M - m - 1}}$$

Where the summation is over t from $M+1$ to n . Here, $\hat{F}$ is asymptotically distributed as $F_{m, n-m-M-1}$

MODELS SELECTED FOR SIMULATION

Data is generated from several linear and nonlinear second orders of general classes of autoregressive models given below:

$$\text{Model 1. AR(2): } Y_{ti} = 0.3Y_{ti-1} - 0.6Y_{ti-2} + e_t$$

$$\text{Model 2. TR(2): } Y_{ti} = 0.3\sin(Y_{ti-1}) - 0.6\cos(Y_{ti-2}) + e_t$$

$$\text{Model 3. EX(2): } Y_{ti} = 0.3Y_{ti-2} + \exp(-0.6Y_{ti-2}) + e_t$$

$$\text{Model 4. PL(2): } Y_t = 0.3Y_{t-1}^2 - 0.6Y_{t-2} + e_t$$

$Y_{ti} \sim N(0,1)$ and $e_{ti} \sim N(0,1)$ for stationary series and $Y_{ti} \sim N(2000,20)$ and $e_{ti} \sim N(1000,10)$,

$t = 1, 2, \dots, 50, 150$ and 300 $i = 1, 2, \dots, 3000$

The model 1, 2, 3 and 4 are linear, trigonometry, exponential and polynomial autoregressive models respectively with coefficients of Y_{t-1} being 0.3 and Y_{t-2} being -0.6. Simulation studies were conducted to investigate the performance of **Keenan's** and **F-test**. The hypothesis test were null hypothesis of nonlinearity against the alternative hypothesis of linearity of data. Thus, if the data is linear with $\alpha = 0.05$, more than 95% of the replicates are expected to have the test statistic less than the critical values. Power of the two tests is compared for the different models, sample size and distributions to know which of the two tests is acceptably good for detecting nonlinearity for time series data generated from the given model.

Note that in autoregressive modeling, the innovation (error), e_t process is often specified as independent and identically normally distributed. The normal error assumption implies that the stationary time series is also a normal process; that is, any finite set of time series observations are jointly normal. For example, the pair (Y_1, Y_2) has a bivariate normal distribution and so does any pair of Y 's; the triple (Y_1, Y_2, Y_3) has a trivariate normal distribution and so does any triple of Y 's, and so forth. Indeed, this is one of the basic assumptions of stationary data. However, in this study, the data will be generated under white noise assumption of stationarity and when the stationarity assumption is violated for order of past responses and random error terms to see behavior of the models in each case. 3000 replications were used to stabilize models estimations at different combinations of n and models.

Selection Rule

The average acceptance of linearity by each test was recorded as in table 1-4, at $n=50, 150$ and 300 representing small, mild and large samples respectively for each case (stationarity and Non-Stationarity) and model. The test with highest proportion of acceptance in a category is the best for that category. Note that only second order autoregressive models were considered in each case and situation

RESULTS AND DISCUSSIONS

Relative Performance of Keenan- and F-Tests on General Class of Stationary Autoregressive Cases at Different Sample Sizes

The performance of the following Keenan- and F-tests in detecting general classes of linear and nonlinear autoregressive cases were examined at sample size of 50, 150, and 300 which represent small, mild and large sample sizes respectively. The data were simulated using R statistical software following the assumption of stationarity earlier stated to fix the parameters. The parameters were fixed for each model as shown in model 1-4 to observe how the tests would accept the null hypothesis of linearity of stationary data. The white noise assumption of the error term was also observed to make the data simulated be stationary. Each created data were replicated 1000 times using TSA Package in R software.

Table 1: Empirical frequencies of rejection of the null hypothesis of linearity;

$n=50$ and 1000 replications. Nominal significance level, 0.05 (Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.8505	0.6198
Model 2	0.6449	0.5046
Model 3	0.6756	0.0283
Model 4	0.0033	0.0005

Table 2: Empirical frequencies of rejection of the null hypothesis of linearity;

$n=150$ and 1000 replications. Nominal significance level, 0.05 (Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.4731	0.9280
Model 2	0.0514	0.0414
Model 3	0.0088	0.0062
Model 4	0.0012	0.0000

Table 3: Empirical frequencies of rejection of the null hypothesis of linearity;
n =300 and 1000 replications. Nominal significance level, 0.05(Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.5179	0.8706
Model 2	0.0735	0.0179
Model 3	0.0169	0.0061
Model4	0.0000	0.0000

Table 4: Effect of Sample size on the Power of the Tests for model 1-4
Nominal significance level, 0.05 (Stationary Data)

Model	Sample Size	Model 1	Model 2	Model 3	Model 4
Keenan	50	0.6198	0.6449	0.6756	0.0033
	150	0.4731	0.0514	0.0088	0.0012
	300	0.5179	0.0735	0.0169	0.0000
F-test	50	0.8505	0.5046	0.0283	0.0005
	150	0.9280	0.0414	0.0062	0.0000
	300	0.8706	0.0179	0.0061	0.0000

Relative Performance of Keenan- And F-Tests on General Class of Non-Stationary Autoregressive Cases at Different Sample Sizes

One of the objectives of this study is to find out the performance of Keenan and F-test of nonlinearity on general classes of linear and nonlinear autoregressive, simulated with violation of assumption of non-stationarity. Since most of real life data collected are non-stationary, there is need to investigate which of these tests is suitable for non-stationary data. One major assumption of stationarity is validity of white noise assumption of error term; the error term is independently distributed with zero mean and positive variance.

Indeed, in this work non-stationarity was injected in our simulated data from different models used for the simulation by violating the independence and normality assumption of error term in the following way to know the effect of non-stationarity on each model at different sample sizes: the results are displayed in table 5-8

$$Y_t \sim N(2000, 20) \text{ and } e_t \sim N(1000, 10)$$

The value of mean and variance were specified based on the history of nature of real life data considered, Data on Nigeria Gross Domestic Products (GDP)

Table 5: Empirical frequencies of rejection of the null hypothesis of linearity;
n =50 and 1000 replications. Nominal significance level, 0.05 (Non-Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.3697	0.4607
Model 2	0.000	0.3072
Model 3	0.0000	0.3123
Model 4	0.0000	0.0034

Table 6: Empirical frequencies of rejection of the null hypothesis of linearity;
n =150 and 1000 replications. Nominal significance level, 0.05 (Non-Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.3840	0.2088
Model 2	0.0000	0.7596
Model 3	0.0000	0.3953
Model 4	0.0000	0.0017

Table 7: Empirical frequencies of rejection of the null hypothesis of linearity;
n =300 and 1000 replications. Nominal significance level, 0.05 (Non-Stationary Data)

Model	Keenan's Test	F-Test
Model 1	0.9811	0.0819
Model 2	0.0000	0.2931
Model 3	0.0169	0.0061
Model 4	0.0000	0.0000

Table 8: Effect of Sample size on the Power of the Tests for model 1-4

Nominal significance level, 0.05 (Non-Stationary Data)

Model	Sample Size	Model 1	Model 2	Model 3	Model 4
Keenan	50	0.3697	0.0000	0.0000	0.0000
	150	0.3840	0.0000	0.0000	0.0000
	300	0.9811	0.0000	0.0000	0.0000
F-test	50	0.4607	0.3072	0.3123	0.0034
	150	0.2088	0.7596	0.3953	0.0017
	300	0.0819	0.2931	0.7670	0.0000

Table 9: Results of Nonlinearity Tests on Nigeria GDP

Test	Test Statistic	Critical value	Conclusion
Keenan's Test	10.982	0.0052	Nonlinear
F-Test	8.0797	0.0293	Nonlinear

Table 1-8 show the results of analyses of performance of Keenan's test and F-test with respect to the model 1-4 at small, mild and large sample sizes taken to be 50, 150 and 300 respectively under the assumption of stationarity and violation of the assumption of stationarity. The two tests were compared at the 5% level of significance for two tailed test in each case. The average powers of the tests for both tests were computed for easy comparison.

CONCLUSION

We noticed that both test do not reject the linearity of the Model 1, linear autoregressive at different sample sizes. However, F-test has higher power of acceptance than Keenan test when data is stationary while Keenan's test performs better for non-stationary data especially at large sample size. In model 2-4, trigonometric, exponential and polynomial autoregressive models respectively, most of the average p-value are less than the 5% level of significance and as the sample size increases the p-value decreases indicating the significant of linearity of the models by

the two tests. Meanwhile, the F-test perform better as its average p-values are less than Keenan's test at the three sample sizes for stationary data and vice versa for non-stationary data as shown in the summary Table 4 and 8.

More so, both tests wrongly accept the null hypothesis of linearity for model 2, 3, and 4 with their average p-values greater than 5% level of significance at sample size 50 for stationary data. When the Non-Stationarity was introduced in data generated F-test's p-value were greater than 5% and therefore wrongly accept the null hypothesis of linearity of nonlinear autoregressive model except that of polynomial model which its linearity was rightly rejected and more powerful when the sample size increases. While Keenan's test has the p-value close to zero which show the significant of linearity of the three nonlinear models at the three sample sizes and therefore considered as the most powerful test for non-stationary data

Finally, we provided illustrative examples by applying the statistical tests to real life datasets and results obtained are desirable.

REFERENCES

- Chan, W. S., and Tong, H. (1986), On Tests for Non-linearity in Time Series Analysis. *Journal of Forecasting*, 5: 217-228.
- Chen R. and Tsay, R.S. (1993), Nonlinear additive ARX models. *J. Amer. Statist. Assoc.* 88, 995-967.
- Chen R. and Tsay, R.S. (1996). Nonlinear transfer functions. *Journal of Nonparametric Statistics*, 6:193-204.
- Franse, P.H. and van Dijk, D. (2000). Nonlinear error-correction models for interest rates in the Netherlands, in W.A.
- Hunnich, M. J. (1982), Testing for Gaussianity and Linearity of a Stationary Time Series. *Journal of Time Series Analysis*. 3(3): 169-176.
- Hipel, K. W. and McLeod, A.I. (1994). Time Series Modeling of Water Resources and Environmental Systems. Amsterdam: Elsevier.
- Ibrahim M., Azami Z. and Mohd., S.Y. (2005), *Jurnal Teknologi*, 42(C), 1-10 Universiti Teknologi Malaysia
- Jonathan D. C. and Kung-Sik C. (2008), Time Series Analysis with Applications in R Second Edition, Springer Science+Business Media, LLC
- Keenan, D.M. (1985). A Tukey non-additivity-type test for time series nonlinearity. *Biometrika* 72, 39-44.
- Lewis, P., and B. Ray (1997): "Modeling nonlinearity, long-range dependence, and periodic phenomena in sea surface temperatures using TSMARS," *Journal of the American Statistical Association*, 92: 881-893.
- Terasvirta, T. (1993): Testing linearity against smooth transition autoregressive models. *Biometrika* 74, 491-499.
- Tong, H. (1990): Nonlinear Time Series: A Dynamical System Approach, Oxford: Clarendon.
- Tong H. and Lim, K. S. (1980). Threshold Autoregression, Limit Cycles and Cyclical Data. *Journal of Royal Statist. Soc.*, B 42:245-292.
- Tsay, R.S. (1986). Nonlinearity tests for time series. *Biometrika* 73, 461-466.
- Tsay, R.S. (1998). Testing and modeling multivariate threshold models. *J. Amer. Statist. Assoc.*, 93, 1188- 1202.
- Tsay, R. S. (2010): Analysis of Financial Time Series; 3rd Edition, Published by John Wiley & Sons, Inc., Hoboken, New Jersey. Published simultaneously in Canada
- Yuan, J. (2000): Testing Linearity for Stationary Time series using the Sample Inter-quartile Range. *Journal of Time series Analysis* 21(6) 714-722
- Yule, G. U. (1926). "Why do we sometimes get nonsense-correlations between time-series? — A study in sampling and the nature of time-series." *Journal of the Royal Statistical Society*, 89:1, 1-63.



PHYSICAL SCIENCES

OPERATING SYSTEM SECURITY AND PENETRATION TESTING

Adoga, H. U., Ezugwu, E. A. and Umar, M. B.

Department of Computer Science, Faculty of Science, Federal University Lafia, Nasarawa State, Nigeria

Corresponding Email: haruna.adoga@fulafia.edu.ng

Date Manuscript Received: 30/11/2016

Accepted: 30/12/2016

Published: December, 2016

ABSTRACT

Penetration testing is an integral part of any organization or individual that employs the use of Information Technology services. This ensures that their computing infrastructures are checked for vulnerabilities in a routine manner. This paper explains the processes and phases involved in ethical hacking. In addition, major penetration testing types available are also discussed. A Local Area Network (LAN) was designed in a virtual environment running Linux and Windows Operating Systems. We carried out a white box penetration test on the systems. Kali Linux; an open source Debian-based Linux distribution designed for penetration testing and digital forensics was used for the experiment. Several built-in tools in Kali Linux were used, while going through the main phases of penetration testing. Starting from the reconnaissance phase of the process, information about computers was gathered, the network was scanned for vulnerabilities in the scanning phase, and identified vulnerabilities were exploited in the third phase of the penetration test, which is gaining access. Backdoors to exploited system(s) were created to maintain access and event logs were deleted to prevent detection in the final phase of the process.

Keywords: *Malware, operating system security, work station virtualization, penetration testing, network security.*

INTRODUCTION

With the rapid growth of Information Technology (IT) and increased accessibility in recent years, we produce more data now than ever before. Therefore, this calls for an urgent need to protect information and information systems from all sorts of manipulation and unauthorized access. Ensuring the protection of network infrastructure and computer systems, and the services they provide is paramount to the success of any business. Sensitive data, such as financial records, medical records and e-commerce services amongst other sensitive information, need to be protected by ensuring the Confidentiality, Integrity and availability (CIA) of such information. Host and server based operating systems faces an increasingly high level of security threats by the day. Penetration testing provides a way for organizations to check their computer infrastructure for vulnerabilities that could be exploited by an adversary.

There are some very important objectives that we set aim to achieve by carrying out this research; these objectives are listed below. They include, using Kali Linux, which is an open source Linux distribution designed for digital forensics and penetration testing, in determining the possible vulnerabilities that exist in a typical Local Area Network environment, design of a typical Local Area Network, in a virtual environment, consisting of both open source and proprietary Operating Systems as obtainable in most network environments, the implementation of each phase of ethical hacking and penetration testing using the digital forensics tool (Kali Linux) and exploiting any vulnerability found with the aim of providing useful recommendations, which can help organizations harden their network infrastructure even better.

Kali Linux is the most advanced Debian-based Linux distribution for penetration testing available at the time of this research. This distribution provides applications and tools that can be used in each of the five main phases of penetration testing. An empirical approach was adopted in reviewing ethical hacking and penetration-testing procedures with focus on commonly used operating systems in today's network infrastructures.

Ethical hacking can be described as a process of testing the computer infrastructure of an organization or individual by professional certified hacker(s) with the aim of assessing the infrastructure for possible vulnerabilities and making them known to the management of the organization for appropriate security measures. Unlike black hat hackers who gain unauthorized access to computer systems (networks) without the authorization of the owner, ethical hacking is usually done with the consent of the organization or owner of the computer system or network. A certified ethical hacker will normally use the same

tools that a black hat hacker will use to achieve their aim. According to Whitaker and Newman (2006), a penetration tester is an ethical hacker who is hired to attempt to compromise the network of a company for the purpose of assessing its data security.

There are basically five phases of ethical hacking, as reported by Engebretson (2013).

Reconnaissance is basically the process of gathering information about the target infrastructure and systems. This is the first phase of the ethical hacking process as it allows the ethical hacker to have a good understanding of the organization's infrastructure and the underlying technology in use. At the end of this phase, the pen tester should have a good idea of information such as the facility information, phone numbers, employee information, Internet Protocol (IP) address ranges, and namespaces. Nidhra and Dondeti (2012).

Vulnerability Scanning is a phase that makes use of data gathered to find out the valuable resources the target has, presence of known vulnerabilities in infrastructure the target uses. According to Nidhra and Dondeti (2012), the pen tester gets information on hosts, ports on the hosts and services that may be running on the hosts. Scanning is predicated on the assumption that reconnaissance has been successfully completed.

Gaining access (Exploitation) is a phase of the penetration testing lifecycle where the hacker attempts to gain access to the target system(s) using the information gathered from previous phases of the process. Broad and Bindner (2014) reported that information such as usernames, permissions and passwords gotten from early phases are utilized to exploit any known vulnerabilities on the target systems.

Maintaining access to the target system after securing it is an important phase of a penetration test, as this will ensure that the pen tester stays connected long enough to carry out all the tests (attacks). The use of backdoors and key loggers are employed in this phase, backdoors will allow pen testers to connect to the same target at a later time even when a patch (update) has been implemented to fix the vulnerability. It is great to exploit a computer, networking device, or a firewall device, however the goal of penetration testers is to maintain access to the exploited system(s). Broad and Bindner (2014).

This is the final phase in the ethical hacking process, as known existing vulnerabilities have been exploited. Activities in this phase involves deleting event logs that might reveal that the hacker was there in the first place. Engebretson (2013) reported that an attacker who wishes to remain untraceable after successfully carrying out an attack, needs to erase all the tracks that may lead back to him/her.

MATERIALS AND METHODS

A Local Area Network (LAN) was designed with both Linux and Windows Operating Systems in a virtualized environment. According Cisco Systems (2016), the benefits of a centralized design include IP address management, simplified configuration and troubleshooting, and roaming at scale. Using Kali Linux, we went through the phases of penetration testing on the LAN. Information about the Operating Systems was gathered and the computers were scanned for vulnerabilities. Finally, some of the vulnerabilities were exploited and recommendations made. Figure 1 below depicts the phases involved in performing penetration testing.

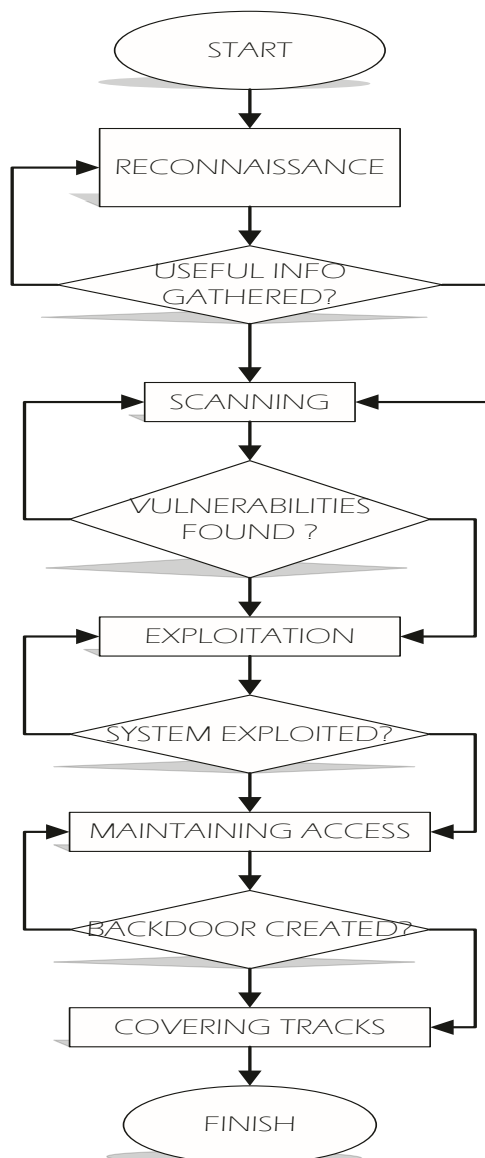


Figure 1. Penetration testing flowchart

Based on the information depicted in Figure 1 above, the flowchart starts with the reconnaissance phase of penetration testing, where information about live hosts were collected, upon completion, the network was scanned in order to reveal available ports and services. Vulnerabilities found in the scanning

phase were exploited in the exploitation phase of the penetration test. Backdoors were also created in order to maintain access to the exploited systems. The process completes by covering the tracks, to avoid detection by system administrators.

The experiment from the reconnaissance phase of ethical hacking and walked through subsequent phases of the process in the following sections. The different phases of penetration testing were performed using Kali Linux. The network infrastructure was simulated in a virtual environment using VMware workstation 11. A comprehensive network topology structure was designed based on the information collected from the reconnaissance phase of the penetration testing carried out (See Table 1 and Figure 2).

Reconnaissance

Identification of live hosts

Running the *ifconfig* command on the Kali Linux terminal reveals the local IP address on Kali (a static IP address was assigned), having this information can help you get an idea of the subnet mask of the network you are connected to. A ping sweep was done on the network as part of the information gathering reconnaissance phase. This reveals some important information about host IP addresses on the network and the output shows that 5 hosts are up with their respective IP and mac addresses displayed.

IP addressing scheme from ping sweep

Using ping sweep with nmap tool on Kali Linux, i.e running the `nmap -sP 192.168.1.0/24` command with `sP` option to specify ping sweep. The IP addresses on the network are as shown in Table 2 below.

Table 1. Ip addressing and MAC address discovered using nmap tool

Host MAC address	IP address	Subnet mask
00:0c:29:84:e3:39	192.168.1.1	255.255.255.0
00:0C:29:56:DA:E2	192.168.1.2	255.255.255.0
00:0C:29:A0:FF:18	192.168.1.3	255.255.255.0
00:0C:29:08:35:C1	192.168.1.4	255.255.255.0
00:0C:29:D0:EC:2F	192.168.1.5	255.255.255.0

After performing a ping sweep on the network, the IP addresses of hosts on the network were revealed.

Based on the information gathered from the reconnaissance activity above, it is now known to the pen tester that 4 more devices are connected on the same network and a network topology can be drawn in order to make the subsequent phases of the ethical hacking process more efficient and precise. The network topology used to model the experimental setup is illustrated in Figure 2.

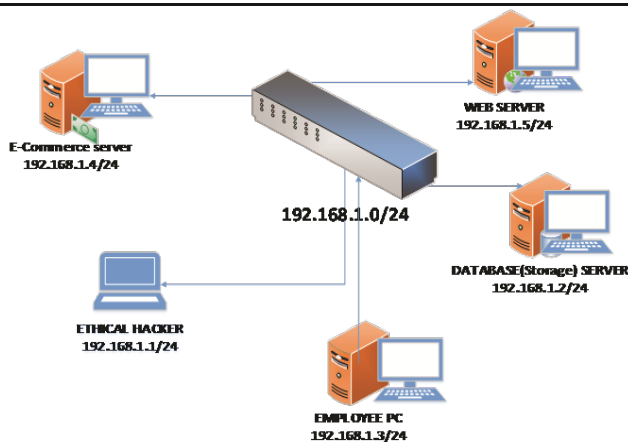


Figure 2. Network topology designed from reconnaissance.

Vulnerability scanning was performed on the e-commerce server, using the Nmap tool on Kali Linux. A list of open ports and services available on the server are shown in the table below.

Table 2: Msf console scan on the e-commerce server (192.168.1.4/24)

s/n	Port type	Port number	Status	Service
1	Tcp	135	open	Msrpc
2	Tcp	139	open	Netbios-ssn
3	Tcp	445	open	Microsoft-ds

Nmap scan on the web server (192.168.1.2) shows a

potential vulnerability, telnet port 23 is open. We will try to exploit this vulnerability in the exploitation phase. Nmap scan on the web server (192.168.1.5/24) shows potential vulnerabilities i.e. open ports and services that can be exploited using penetration testing. Figure 3 below depicts the data collected on the web server.

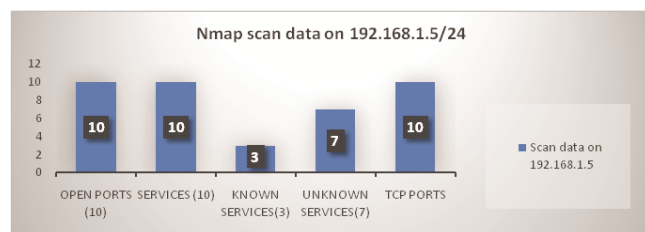


Figure 3. Open ports and services on web server 192.168.1.5/24

Gaining access (Exploitation)

On 192.168.1.4/24, we exploited the ms08_067_netapi vulnerability identified during the scan. Figure 4 shows the screenshot of the ms08_067 attack carried out on the e-commerce server on the network infrastructure, which gives access to the command prompt of the server, data can be modified and system settings can be tampered with.

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse handler on 192.168.1.1:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - Lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.1.4
[*] Meterpreter session 1 opened (192.168.1.1:4444 -> 192.168.1.4:2089) at 2015-04-12 16:38:09 -0400

meterpreter > shell
Process 1312 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
C:\WINDOWS\system32>cd ..
C:\WINDOWS>dir
```

Figure 4: Ms08_067 vulnerability exploit on e-commerce server 192.168.1.4/24.

The figure below depicts the vulnerability levels, their indications, which followed by a brief summary of each vulnerability level.

L	Low
M	Medium
H	High
C	Critical

Figure 5: Vulnerability level color codes.

From the image shown above, L depicts low and this means a particular vulnerability would not cause serious harm to the system even though it exists, it can be fixed by updating the Operating to get latest patches and fixes.

M depicts medium level of vulnerability, which implies that, the threat level has a mild effect on the Operating System. A more specific patch, which is peculiar to the vulnerability need to be used.

H depicts high level of vulnerability, it basically means that, it can cause damage to the Operating System when exploited.

C depicts critical level of vulnerability, if exploited, this can bring the system to a complete halt, and an attacker can take over the system remotely.

Multi/handler can be used with a payload of 'windows/metsvc_bind_tcp' to connect to the remote system, as shown in Figure 6 below.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp
PAYLOAD => windows/metsvc_bind_tcp
msf exploit(handler) > set LPORT 31337
LPORT => 31337
msf exploit(handler) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf exploit(handler) > exploit

[*] Started bind handler
[*] Starting the payload handler...
```

Figure 6. Multi-handler to exploit metasploit backdoor on e-commerce server.

RESULTS AND DISCUSSION

The outcome of the penetration test carried out on the network created in the experiment phase shows that using the nmap tool on Kali Linux, we were able to discover the number of computers on the network, which comprises of both client and server operating systems. We were able to discover both the Media Access Control addresses of the devices and their respective ip addresses. Using this information, a network topology was drawn, which

assigns valid IP addresses to both client and server operating systems found on the network. The network topology presented depicts all the devices that are on the network, including the Kali Linux PC used for carrying out the pen test on the network. Although the structure of the penetration testing process requires that results are presented after each phase, we have also presented the important results in table 3 below, followed by a detailed analysis of some results in subsequent subsections.

Table 3. Results and description

Device name	Device Internet Protocol address	Vulnerabilities and open ports found	Vulnerabilities exploited	Description	Proposed solution
E-commerce server.	192.168.1.4/24	TCP port 135, TCP port 139, TCP port 445 (Msrpc, Netbios-ssn, Microsoft-ds)	Ms08_067_netapi vulnerability.	This attack carried out on the E-commerce server gives full access to the command prompt, where changes can be made to the exploited Operating System.	The Ms08_067_netapi vulnerability patch should be implemented on the server, including other supported patches. Open ports on the server should be closed, allowing only ports that are in use by the server.
Web server.	192.168.1.5/24	Telnet port 23, 3 known services, 10 open ports, 7 unknown services.	Using the telnet protocol on port 23 sends data in clear text form.	This gives access to remote data using a packet sniffing tool.	The telnet protocol which uses port 23 for remote access should be replaced with SSH, which is more secured and operating on port 22. Telnet port 23 should always be closed and the protocol deactivated.
E-commerce server.	192.168.1.4/24	metsvc_bind_tcp	The multi-handler tool was used for exploiting the metasploit bind_tcp vulnerability found on the server.	This vulnerability was exploited by maintaining access to the server.	The local port number 31337 on the server should be closed at all times.
E-commerce server.	192.168.1.4/24	metsvc payload	Backdoor exploit using meterpreter	Using the metasploit payload gave us the ability to create a backdoor on the e-commerce server.	A patch should be selected and installed from updates that are made available by the Operating System vendor.
E-commerce server.	192.168.1.4/24	Covering tracks	425 system data were wiped, and 236 app data were also wiped on the server to cover the tracks upon completion, as shown in figure 7.	This phase of the ethical hacking process is important since it helps in clearing all the activities of the ethical hacker.	Suggested solutions from subsequent phases of the pen test process should be implemented to prevent the hacker from getting to this final stage of covering tracks.

The Ms08_067 Vulnerability Analysis

The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows Server systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. The MS08_067 vulnerability can also be used to shut down the server remotely, which can have a catastrophic effect on the company's business.

Threat level: Critical

Vulnerability level: Critical

Denial of Service attack on webserver 192.168.1.5/24

The Table below depicts the screenshot of the Denial of Service (DoS) attack carried out on the web server.

Table 4. Denial of service attack on webserver 192.168.1.5/24 using port 80 (SYN flood)

S/N	Parameter	Value
1	LHOST (local host)	192.168.1.1
2	RHOST (remote host)	192.168.1.5
3	RPORT (remote port)	80
4	SNAPLEN (LENGTH)	65535
5	TIMEOUT	500

Denial of Service analysis

A Denial of service (DoS) attack on port 80 of the webserver results when the web server is continuously flooded with packets until it makes it unavailable or unable to reply legitimate requests from clients. Denial of service overloads the target's resources and other system resources affected are: CPU usage, network bandwidth, Hard disk space, database pool, and server memory.

Threat level: Critical

Vulnerability level: Critical

Backdoor exploit analysis

metasploit payload will give access back to the exploited server at later time using meterpreter shell. Having such backdoor access has a catastrophic effect on the server. Using the `clearev` command on the meterpreter prompt will clear the event log on the victim's computer and thus make it difficult for the victim to notice any changes or even know their system has been hacked. Figure 7 below shows the data that was wiped from the e-commerce server to prevent detection by the organization after completing the exploit.

Threat level: Critical

Vulnerability level: Critical

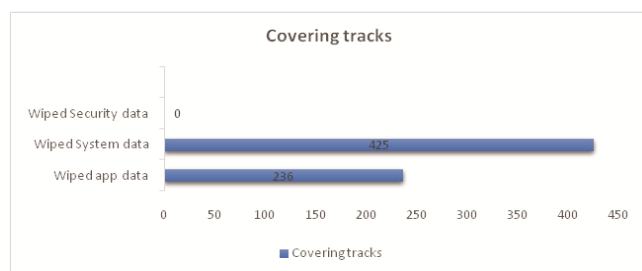


Figure 7: covering tracks using `clearev` on e-commerce server.

CONCLUSION

Ethical hacking unlike black hat hacking or hacking with malicious intent is an integral part of any organization or business that employs the use of Information Technology (IT). This ensures that computer systems and infrastructure are tested in a routine manner to prevent against hackers; this paper has shed light on the procedures by going through the five phases of penetration testing. Organizations need to employ pen testers to routinely test their server and host operating systems for vulnerabilities and make recommendations that will strengthen security of such systems. Kali Linux, an open source toolkit can be used to perform these tests as it provides all the tools

needed to go through all the phases of penetration testing. The future direction of our work is to have this same technique of penetration testing, using Kali Linux, implemented in a datacenter environment, where more servers with different kinds of Operating Systems are available, and with connections to Wide Area Networks.

We conclude the experiment section by presenting the following recommendations:

1. The MS08_067 vulnerability found on the e-commerce server is a huge security risk as it allows a hacker access to sensitive information. Latest patches should be applied to the server to remedy this vulnerability.
2. The use of telnet service for remote access should be discouraged and replaced with SSH on port 22, as it is more secure sending encrypted traffic.
3. Hosts and network devices should be configured to block ICMP echo requests from unknown source addresses (broadcasts) by default. This is a suspicious behavior which hackers use for information gathering about the IP and mac addresses on the network using ping sweeps.
4. Organizations making use of various types of Operating Systems as emulated in the virtual network designed in this work should always have the Operating Systems updated to versions that include latest patches with built-in Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
5. Patches to Operating Systems should be managed using patch management systems, as this is a more effective and efficient way of applying patches. This will ensure a centralized control of updates to all systems, which reduces the burden of manual updates by system administrators thus enhancing overall system security.
6. Penetration testing should be conducted at least twice a year and vulnerability assessment be conducted at least three times a year, this will help fix security challenges when major changes are carried out in the organization's computer infrastructure.

REFERENCES

- Broad, J. and Bindner, A. (2014). Hacking with Kali. Massachusetts: Elsevier. Pp167-172.
- Cisco Systems Inc. (2016). *Campus Wireless LAN Design Fundamentals*, San Francisco, Cisco Publishing, Pp7-24.
- Engebretson, P., 2013. *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.
- Global Knowledge. (2011). *The 5 Phases of Hacking: Covering Your Tracks*. Available: <http://blog.globalknowledge.com/technology/security/hacking-cybercrime/the-5-phases-of-hacking-covering-your-tracks/>. Last accessed 16th April 2015.
- Naik, A., Kurundkar, D., Khamitkar, D. and Kalyankar, V. (2009). Penetration Testing: A Roadmap to Network Security. *Journal of Computing*. 1 (1):187-190.
- Nelson, W.B.V., Laizerovich, D., Bunker, E.E. and Van Schuyver, J.D., Achilles Guard Inc., 2008. *Network security testing*. U.S. Patent 7,325,252.

- Nidhra, S and Dondeti, J. (2012). Black Box and White Box Testing Techniques- A literature Review. *International Journal of Embedded Systems and Applications (IJESA)*. 2 (2):29-50.
- Oriyano, S (2014). Certified Ethical Hacker Study Guide. 8th ed. Indiana: John Wiley & Sons, Inc. Pp444-473.
- Simpson, T., Backman, K. and Corley J. (2011). Ethical Hacking Overview. In: Helba, S. and Bellegarde, Marah HANDS-ON ETHICAL HACKING AND NETWORK DEFENSE. Boston: Cengage Learning. Pp4-5.
- Stallings, W (2012). *Operating Systems: Internals and Design Principles*. 7th ed. New Jersey, Prentice Hall. Pp620-700.
- Sulagna. (2009). Introduction to API Testing. Available: <http://www.scribd.com/doc/9808382/Introduction-to-API-Testing#scribd>. Last accessed 20th April 2015.
- Tang, A. (2014) A guide to penetration testing. Network Security, Pp8-11.
- Whitaker, A & Newman, D. (2006). Understanding Penetration Testing. In: John Kane and Brett Bartow *Penetration Testing and Network Defense*. Indianapolis: Cisco Press. Pp5-6
- Yeo, J. (2013) *Using penetration testing to enhance your company's security*. *Computer Fraud & Security* 2013.4 (2013), Pp17-20.

EDITORIAL POLICY

The FULafia Journal of Science and Technology (FJST) specifically adopts and strives to adhere to the **COPE** - Committee on Publication Ethics.

The FJST is a biannual publication of the Faculty of Science, Federal University Lafia. It is published in March and December.

Authorship: An author is an individual who has significantly contributed to the development of a manuscript.

Acknowledgement: Individuals who participated in the development of a manuscript but do not qualify as an author should be acknowledged. Organizations that provided support in terms of funding and/or other resources should also be acknowledged.

Changes in Authorship: Whenever there is a need to make changes in the authorship of a manuscript or a published article, the changes will be implemented according to COPE specification. Only corresponding authors can make request for a change in authorship.

Submission of Manuscript: Authors should read the “Instruction for Authors” on the journal’s Webpage before making a submission. Manuscript should be prepared according to the style and specifications prescribed in Guidelines to Authors. Authors listed on the manuscript should have met the requirements for Authorship specified above. All authors should approve the final version of the manuscript prior to submission. Once a manuscript is submitted, it is therefore assumed that all authors have read and given their approval for the submission of the manuscript.

Declaration of Conflicts of Interest should be stated in the manuscript: Submission should be made online <http://www.fulafiajst.com> using the Journal submission form.

Conflict of interest: Conflict of interest (COI) exists when there is a divergence between an individual’s private interests (competing interests) and his or her responsibilities to scientific and publishing activities such that a reasonable observer might wonder if the individual’s behavior or judgment was motivated by considerations of his or her competing interests”.

Reviewers should disclose any conflict of interest and if necessary, decline the review of any manuscript they perceive to have a conflict of interest. Editors should also decline from considering any manuscript that may have conflict of interest. Such manuscripts will be re-assigned to other editors.

Confidentiality: A submitted manuscript is a confidential material. FJST will not disclose submitted manuscript to anyone except individuals who partake in the processing and preparation of the manuscript for publication (if accepted). These individuals include editorial staff, corresponding authors, potential reviewers, actual reviewers, and editors. However, in suspected cases of misconduct, a manuscript may be revealed to members of FJST’s ethics committee and institutions/organizations that may require it for the resolution of the misconduct.

Peer review: The review process is an important aspect of the publication process of an article. It helps an editor in making decision on an article and also enables the author to improve the manuscript. FJST has in place a double blind review process.

The identity of author(s) is removed from the manuscript and shielded from the reviewers during the review process. The reviewer is left with only the manuscript without any information that might enable him/her uncovers the identity of the author(s).

Manuscripts are assigned to members of the editorial board of the journal or other competent reviewers from within and outside Nigeria. The review process is done using the Manuscript Management System. Reviewers make one of the following recommendations:

- Accept As Is
- Requires Minor Corrections
- Requires Moderate Revision
- Requires Major Revision
- Submit To Another Publication Such As
- Reject on grounds of (Please be specific)

A Review Certificate is issued to reviewers after the review of the manuscript. The review reports are sent to the authors. However, reviewers’ identity is removed from the review reports. The author(s) is left with only the review reports/recommendation without any information that might enable him/her uncovers the identity of the reviewers. A minimum of two review reports are required per manuscript.

On receipt of the author(s) revised manuscript, the original manuscript, the revised manuscript and the review reports are sent to the editor. The editor makes one of the following decisions:

1. Accept
2. A Review of the Manuscript
3. Reject

If a manuscript is “Accepted”, an Acceptance Certificate is issued to the author(s) and the manuscripts are processed for publication.

If a manuscript is rejected, the authors are informed of the decision and no further processing is done on the manuscript.

If a manuscript requires review or improvement, it is sent to the author(s) with the editor’s recommendation for further revision. The editor makes a final decision on the revised to “Accept” or “Reject” the manuscript.

Misconduct: Misconduct constitutes violation of this editorial policy or the publication ethics. Similarly, any other activities that portend/compromise the integrity of the research or publication process are potential misconducts.

Correction and retraction of articles: Corrections may be made to a published article with the authorization of the editorial board. The FJST can review and assess this editorial policy from time to time.

GUIDELINE TO AUTHORS

COPYRIGHT

Authors are advised to ensure that any article submitted to the FULafia Journal of Science and Technology (FJST) has never been submitted to any other journal. Papers will be subjected to editorial peer review process. By submitting a manuscript, the author agrees to transfer the copyright of the manuscript automatically to the FULafia Journal Science at the time of acceptance for publication. The decision of the editors on the acceptability of a paper or otherwise is final.

PREPARATION AND ARRANGEMENT OF MANUSCRIPTS

Manuscripts should be prepared in English language and should be clearly written. The subsections should include the Abstract, Introduction, Materials and Methods, Results and Discussion, Conclusion and Recommendations and References.

Manuscripts should be typed in word form or Latex format in Times New Roman 12 font size, double-spaced with margins of 4cm. A manuscript should be divided into cover page (title, names of author(s), author’s affiliation, and address for correspondence and reprints, including e-mail addresses), abstract and keywords, introduction, materials and methods, results and discussion, conclusion, acknowledgement (if any) and references. A maximum of 10 printed pages is allowed.

TITLE

Title of manuscript should not be ambiguous and must be concise and reflecting the content of the paper. A maximum of 20 words is recommended for the title.

ABSTRACT

A concise and factual abstract is required. The abstract should state briefly the purpose of the research, the principal results and major conclusions. The abstract should be structured with a minimum of 250 words and a maximum of 300 words. Abbreviations should be avoided and if used should be explained at first mention.

INTRODUCTION

Should contain the objectives of the work and provide an adequate background. Avoid a detailed literature review.

MATERIALS AND METHODS

Provide sufficient detail to allow the work to be reproduced. Methods already published should be indicated by a reference: only relevant modifications should be described.

RESULTS AND DISCUSSION

Results should be clear and concise. Discussion should explore the significance of the results of the work and this should not be repeated. Avoid extensive citations and discussion of published literature.

CONCLUSION

The main conclusions of the study may be presented in a short Conclusions section, which may stand alone or form a subsection of a Discussion or Results and Discussion section.

ACKNOWLEDGEMENT

Acknowledgements should be made in a separate section at the end of the article before the references. List here those individuals who funded or provided help during the research.

REFERENCES

References should be listed on a separate sheet and should be listed alphabetically without numbering at the end of the text. The APA reference system is adopted in this Journal. References should be arranged first alphabetically and then further sorted chronologically if necessary. More than one reference from the same author(s) in the same year must be identified by the letters “a”, “b”, “c”, etc., placed after the year of publication. For example, Kwon-Ndung *et al.*, 2009a, 2009b, 2009c).

All citations within the text should follow these formats:

1. Single author: the author's name (without initials) and the year of publication;
2. Two authors: both authors' names and the year of publication;
3. Three or more authors: first author's name followed by “*et al.*” and the year of publication.

Groups of references should be listed first alphabetically, then chronologically. Examples: “as reported (Kwon-Ndung, 2009a, 2009b, 2012; Salihu and Chuku, 2009). Nja (2014) recently reported”

Only published papers can be mentioned in the manuscript. Reference to a journal publication, books, chapters in a book, thesis etc should be listed as follows:

Journal Article:

Edache, J.A., Ehiobu, N.G and Njike, M.C. (2003). Performance of laying Japanese quail (*Cortunixcortuni japonica*) fed different levels of protein under Nigerian environment. *Journal of Agric Sci. &Tech.* 13(2):110-116

Book

Helleiner, G.K. 1966. Peasant agriculture, government and economic growth in Nigeria. Homewood, Illinois, Irwin Press.

Chapter in an edited book:

Jonathan, G. (1999). Agriculture and national development. In: Oduye, M.L. and Suswan, J.T. (Eds.), Politics and the agrarian revolution in Africa. Inter-Academy Publishers, Lagos, Pp. 324-334.

ILLUSTRATIONS

Tables

Number tables consecutively in accordance with their appearance in the text. Place footnotes to tables below the table body and indicate them with superscript lowercase letters. Avoid vertical rules. Be sparing in the use of tables and ensure that the data presented in tables do not duplicate results described elsewhere in the article.

Figures

All illustrations, whether diagrams or photographs, are referred to as Figures. If any figures appear in colour, please note that they will only appear in colour in the online version; in the printed version they will be in black and white. If the quality of the colour figure supplied is not suitable to be produced in colour, it will also be shown in black and white in the online version. Figures should ideally be black and white, not colour, and numbered sequentially. However, if colour is essential to the figure please send a good quality colour image. Please place them at the end of the article, rather than interspersed in text.

Please prepare all figures, especially line diagrams, to the highest possible standards. Bear in mind that lettering may be reduced in size by a factor of 2 or 3, and that fine lines may disappear.

Units of Measurement

FULafia Journal of Science and Technology follow the Système International (SI) for units of measurement. Similarly IUPAC and Authors and editors are, by general agreement, obliged to accept the rules governing biological nomenclature, as laid down in the International Code of Botanical Nomenclature, the International Code of Nomenclature of Bacteria, and the International Code of Zoological Nomenclature. All crops, plants, insects, birds, mammals, etc. should be identified by their scientific names when the English term is first used,

with the exception of common domestic animals.

Math formulae

Present simple formulae in the line of normal text where possible and use the solidus (/) instead of a horizontal line for small fractional terms, e.g., X/Y . In principle, variables are to be presented in italics. Powers of exponential are often more conveniently denoted by exp. Number consecutively any equations that have to be displayed separately from the text (if referred to explicitly in the text). Imperial units will be converted, except where conversion would affect the meaning of a statement, or imply a greater or lesser degree of accuracy.

SECTION A: AGRICULTURAL AND BIOLOGICAL SCIENCES

A mycological assessment of the air quality in flood-prone homes within Lafia Local Government Area of Nasarawa State.

Chuku, A., Arikpo, G., Obande, G. A., Akherenegbe, P., Uteh, P. U. and Namang, M.

Analysis of women participation in livestock production in Mangu Local Government Area of Plateau State, Nigeria

Onuke, E. G.; Ohen, S. B. and Shehu, N. D.

An assessment of earthworm population and soil factors in Amurum forest reserve of Jos, Plateau State, Nigeria.

Abiem, L., Shiwua, M. and Saha, S.

An epidemic of coccidiosis in chickens sold in Keffi central market, Nasarawa State, Nigeria. Yako, A. B. Nweze, C. C. Ogunnu, F. J. and Chessed G.

Effects of access to pasture and integration with rabbits on performance and carcass characteristics of broiler chicken.

Gambo D., Carew, S. N. and Winifred P. M.

Microspora infiltration of gastrointestinal epithelium among HIV/AIDS patients in Keffi, Nigeria.

Yako A. B. Nweze, C. C., Adebayo E. A., Chessed, G.

Morphometric indices and parasites of frozen *Clarias gariepinus* and *Oreochromis niloticus* sold in Jos metropolis, Plateau State.

Doe'ogot, N. L., Dakul, D. A., Pam, D. D., Ombugadu, A., Ayuba, S. O., Njila, H. L.

Nematicidal potential of extracts of neem (*Azadirachta indica*) and lemon grass

(*Cymbopogon citratus*) on root-knot nematodes (*Meloidogyne* spp) infecting sweet potato. Okechalu, O.

B. Dalong, S., Okechalu, A. A., and Oke, F. M.

Outcome of calcium and phosphorous mineral sources on performance, carcass and bones characteristics of broilers.

Ari, M. M., Gambo, D., Ali, S. E., Edwin, E. E., Aminu, R. A., Isa, J. M. and Yaduma, M.

Partial characterization of protease extracted from "Yatsin biri" ginger (*Zingiber officinale*) cultivar of northwestern Nigeria.

Murtala, Y., Babandi, A., Babagana, K., Alhassan, A. J. and Shehu, D.

Phenotypic variability of false sesame (*Ceratotheca sesamoides* End L.) treated with sodium azide. Aliyu, R. E., Aliyu, A. and Adamu, A. K.

Protein contents of maize varieties as influenced by nitrogen and micronutrients.

Olowookere, B. T., Uyovbisere, E. O., Malgwi, W. B. and Oyerinde, A. A.

Rot of seed potato (*Solanum tuberosum* L.) tubers as affected by storage conditions and storage duration in Jos, Plateau State, Nigeria.

Deshi, K. E., Nanbol, K. K., Shutt, V. M., Okechalu, B. O. and Ifenkwe, O. P.

Seasonal responses of two faunal taxa to fire treatments in Yankari Game Reserve, Nigeria. Mwansat, G. S., Da'an, S. A. & Nwabueze, E.

Some ethnobotanical uses of plant resources in Nasarawa State, Nigeria.

Terna, T. P., Kwon-Ndung, E. H., Akomolafe, G. F., Goler, E. E., Okogbaa, J. I., Waya, J. I., and Markus, M.

Utilization of tuber and sprout characteristics in delimiting accessions of "rizga" (*Plectranthus esculentus* N. E. Br.) in Jos, Nigeria.

Agyeno, O. E.

SECTION B: CHEMICAL SCIENCES

Preliminary assessment of heavy metals and water quality of selected wells in Talata Mafara, Zamfara State, Nigeria.

Zubairu, A. Y., Mukhtar, M., Sokoto, A. M., Zubairu, A. and Ladifa, H. M.

SECTION C: EARTH SCIENCES

Delineation of mineral potential zones over Keffi – Abuja Area in North-central, Nigeria using Aeromagnetic data.

Jiriko, A. K., Mohammed, M. A., Kalu, O., Udensi, E. E.

The application 3D seismic data interpretation to hydrocarbon prospect mapping in "Dede" field, Niger

Adeoye, T. O., Johnson, L. M. and Ologe, O. Delta.

SECTION D: ENVIRONMENTAL SCIENCES

Geospatial modeling of land use management for sustainable urban development in Karu, Nasarawa State, Nigeria.

Joshua, J. K., Jobin P. D. and Kuhiyop M. E.

SECTION E: PHYSICAL SCIENCES

Comparative study of the molecular dynamics of anthracene and one of its derivative (1-hydroxyanthracene) in gas phase and ethanol: rhf and dft study.

Umar, G., Chifu E. Ndikilar and John S. M.

Derivation of fitzhugh-nagumosystem.

Aku D. H., Alhamdu A. M. and Useni P. F.

On performance of some methods of detecting nonlinearity in stationary and non-stationary time series data.

Akeyede, I., and Oyeyemi, G. M.

Operating system security and penetration testing.

Adoga, H. U., Ezugwu, E. A. and Umar, M. B.