Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

memorandum

TO: Earl R. Tech, ESS-10, MS D440

DATE: 11 July 1983

FROM: Steve Shaw

MAIL STOP/TELEPHONE: D440/7-4676

SYMBOL: ESS-10:87-83

SUBJECT: UNAUTHORIZED USER ON ESSDP1

We have been informed by OS-4 that on the night of June 28, 1983, an unauthorized user logged onto ESSDP1 via the DECNET non-privileged account.

An investigation of our accounting records shows that the user first attempted to log on via the DECNET privileged account. When that failed, an attempt was made to log on via the non-privileged account. That log on was terminated by our DECNET login.com which terminates all non-network log ons. Unfortunately, we did not have the account set up "captive" so the user was able to successfully log on on the third attempt by using the /NOCOMMAND qualifier.

In light of the above events, we have modified the DECNET accounts to be captive accounts (i.e, disable CONTROL-Y and disallow the use of the /NOCOMMAND log-in qualifier). These actions will prevent future unauthorized entry to our distributed processors via the method described above.

SS:jm

Cy: Steve Blair, ESS-10, MS D440
Charlene Douglass, OS-4, MS F679
ESS-10 Files

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

memorandum

TO: Earl Tech, ESS-10, MS D440

DATE: August 4, 1983

FROM: Steve Blair SB

MAIL STOP/TELEPHONE: D440/7-9211

SYMBOL: ESS-10:96-83

SUBJECT: UNAUTHORIZED USER ON ESSDP2

Following an unauthorized login to ESSDP1 on the night of June 28, 1983, Steve Shaw and I have completed a review of accounting records for both ESSDP1 and ESSDP2 for the month of June.

In addition to the previously known login, accounting records show an unauthorized interactive login to ESSDP2 on the night June 28, 1983. The login was via the DECNET non-priviledged account, and presumably was accomplished in the same fashion as the login to ESSDP1 earlier that night. While on ESSDP2, the user attempted to set host to ESSDP2 and log on the priviledged DECNET account, but failed.

Accounting records also reveal a login failure from machine G just after midnight on June 25, 1983.

SB:kjs

Cy: Steve Shaw, ESS-10, MS D440
Charlene Douglass, OD-4, MS F679
ESS-10 File

TIMES AND DATES OF INTRUSIONS

JUNE 17, Attempted but unsuccessful
J 23, 1983 at 00:56 MDT
Ju 24, 1983 at 00:13 MDT
June 24, 1983 at 23:33 MDT
June 25, 1983 at 00:09 MDT
June 28, 1983 at 21:36 MDT
June 28, 1983 at 22:15 MDT
June 29, 1983 at 00:08 MDT

ACCESS TECHNIQUES USED

TELENET was used to access Machine G on the ICN and DECNET was used to access the other VAX's after the passwords were obtained. Further investigation has determined one questionable access to the ADP STORES VAX from the Distributed Processor at Pacific Northwest Laboratories. This access is being investigated. Investigation found this access to probably be valid due to a program executing at Battelle designed to map the network from their DP.

MP access?

OPERATIONS PERFORMED ONCE ACCESS WAS OBTAINED

After access was granted into Machine G, the perpetrator created a command file that dumped the DECNET database containing passwords to his remote terminal. The NETPRIV account had the following privileges assigned to it: DIAGNOSE, TMPMBX, OPER, NETMBX. These priviliges allowed a dump of the database to the remote terminal. Access was then g d to the other VAX's in the OPEN partition by using the "SET H utility and the DECNET passwords. Continued investigation has revealed a 38 hour operation performed on the ADPDP2 VAX that is highly suspicious. The operation involved memo verification on that DP. Further investigation revealed the probability of a Los Alamos execution of a program that apparently started looping. The start time is still questionable.

change!?!

TYPE OF ACCESSIBLE INFORMATION

We have not proven yet that any information other than DECNET passwords was obtained but there was certainly the opportunity for access to several types of information including the following:

Mx G - databases including clerical communications information, source files for C-Div utilities, DECNET passwords, some ICN passwords and user numbers imbedded in the system, unclassified scientific computing, Mx G accounting files.

OFVAX - Laboratory clerical information (phone book), and the Laboratory Electronic Mail System.

ESS10 - unclassified scientific word processing, databases pertaining to NASA and military satellite information and the codes that process satellite information.

MP VAX - Data analysis and support information for Los Alamos M Physics Facility.

ADPDP2 VAX - Laboratory mail from the following divisions:
ADP, MAT, PA

STORES - Laboratory warehouse (stock) information.

*** It has been determined through further investigation that the intruder attempted to gain access to the ZIA DP but failed. Access was gained to the S1VAX through the GUEST account but the intruder did not linger on this machine. Access was also gained to the QDVAX and we are still investigating operations performed during intrusion. Access to the Battelle DP was attempted but unsuccessful. It was possible, however, to explore the system by simply being logged on to an account with no privileges. This feature was available on the entire network, so the intruders had the ability to explore the systems without actually doing anything else.
Accounting logs were lost from
the ADPDP3 DP that contained information relating to all the information services of the Laboratory. We are fairly certain that access was attempted and possibly gained to this DP due to the access patterns previously established.

DISRUPTION, DAMAGE, OR LOSS

At this time, we have , to our knowledge, experienced no loss of information. Alterations were made to privileges on some accounts and a new account established with the ability to set privileges for all accounts.
T isruption has been extensive, requiring, up to this t , and we are still investigating, approximately 3 to 4 man months of tracking time between the groups involved.

VALUE of TELENET TIME USED
As near as we can determine, the Telenet time involved cost the Laboratory at the most approximately $150.

COST OF FUTURE PREVENTION

About 10 hours of software changes were made to all the VAX's to prevent future access. Telenet changes were made at the cost of $100 per month for future access to telenet.

PERSONS WILLING TO TESTIFY

Charlene Douglass
P.O. Box 1061
Los Alamos, New Mexico 87544
Phone- 662-5565
BUS - 667-4844

John F. Davis
2848 A Walnut
Los Alamos, New Mexico 87544
Ph e 662-7890
B 667-4793