

TARGET INFORMATION

1. Security classification: Unclassified

2. IP Address of the targeted system(s) IP:

Port:

 Static Dynamic

3. Serial number of system:

4. OS of the targeted system:

Version:

5. MAC Address of system NIC:

6. Fully Qualified Host Name of the targeted system
(i.e. www.greedy.army.mil):

7. How long has the system been online:

8. Date and/or level of Latest patch:

9. System Hardware: (i.e.
Sun/Compaq/Dell):

10. Is system a web server?

YES NO

 Publicly accessible?

YES NO

11. Is system a network server?

YES NO

12. How many clients on the network?

13. How many servers on the network?

14. Security mode of operation: (dedicated/system, high/multi-level/etc):

15. Other software installed on the system:

16. Unauthorized software installed on the system?

YES NO

 If yes, what type: (IRC, Napster etc?):

17. What AV product is installed on the system:

 Norton MacAfee Trend Micro None Other

18. What was the latest AV update:
19. Were there any alerts from the AV product? YES NO
- If yes, identify the alert/warning:
20. Accreditation date:
21. Trusted Host: (What systems trust this host?):
 IP address
 IP address
 IP address
 IP address
22. Is there an approved login warning banner? YES NO
23. Information contained on the system:
24. Information available on the network:
25. What was the system used for:
 (ie admin/ C2/logistics/DNS/etc)
26. Is there an Intrusion Detection Sensor monitoring this network? YES NO
- If yes, what type? (Real Secure/Shadow/NID/JID/snort/etc):
27. Are IDS logs available? YES NO
- Can they be provided/accessed: YES NO
28. Is there a firewall protecting this system? YES NO
- If yes, what type? (Sidewinder/Raptor/Gauntlet/etc):
29. Are firewall Logs available? YES NO
- Can they be provided/accessed: YES NO
30. When was intrusion detected?
31. Who discovered the intrusion?
32. How was intrusion detected? What suspicious activity caused or preceded the investigation?

33. What actions did the system administrator/security specialist take in this incident to date:

34. Has the site been blocked at the controllable security routers? YES NO

If yes, how:

35. How was the intruder able to access the system:

36. What was the exploit used if identified:

37. Level of access gained by the intruder? Root User

38. Was the system used to target another site? YES NO

Commercial/civilian IP:

Military IP:

39. Security status; Offline? YES NO

If no, why is the system still on line? (PDC/BDC/exchange server etc):

40. Has the system had a vulnerability assessment conducted in the past? YES NO

If yes, when:

By Whom:

41. Has the system been compromised previously? YES NO

If yes, when:

How:

42. Was the IP changed as a result of the previous compromise: YES NO

43. Have other systems on the network been compromised previously? YES NO

If yes, when:

44. Has the password file been accessed or copied? YES NO

If yes, when:

45. Has the system administrator changed root password for other systems? YES NO
- If yes, when:
46. Were files uploaded to the target system? YES NO
- If yes, what type:
- Names of files identified:
- Can the files be provided? YES NO
47. Were files downloaded from the target system? YES NO
- If yes, what type:
- Names of files identified:
- Can the files be provided? YES NO
48. Has the system been scanned after the backup was conducted? YES NO
49. Have the results been provided? YES NO
50. Counter measure installed on the system:
 (i.e. TCP wrappers/shadowed password files/etc)
51. Impact to Unit's mission:
52. Man-hours / People involved
 (investigation):
53. Man-hours / People involved (recovery):
54. Man-hours / People involved (lost productivity):
55. Any suspicious emails sent from the users account? YES NO
56. If Yes, what was the destination address? include copy: